Westinghouse Non-Proprietary Class 3

WCAP-15830-NP
Revision 1

July 2007

Staggered Integrated Engineered Safety Features and Loss of Off-site Power Testing at CE NSSS Plants

WCAP-15830-NP, Revision 1

Staggered Integrated Engineered Safety Features and Loss of Off-site Power Testing at CE NSSS Plants

Developed under PWROG Program Task CEOG-2016, PA-OSC-288 and PA-OSC-367

July 2007

Joseph R. Congdon*
Plant Operations

David Finnicum*
Risk Applications & Methods II

John Duryea*
Plant Operations

**Electronically Approved Records are Authenticated in the Electronic Document Management System*

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

LEGAL NOTICE

This report was prepared as an account of work performed by Westinghouse Electric Company LLC. Neither Westinghouse Electric Company LLC, nor any person acting on its 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.

COPYRIGHT NOTICE

DISTRIBUTION NOTICE

This report was prepared for the PWR Owners Group. This Distribution Notice is intended to establish guidance for access to this information. This report (including proprietary and non-proprietary versions) is not to be provided to any individual or organization outside of the PWR Owners Group program participants without prior written approval of the PWR Owners Group Program Management Office. However, prior written approval is not required for program participants to provide copies of Class 3 Non-Proprietary reports to third parties that are supporting implementation at their plant, and for submittals to the NRC.

PWR Owners Group Project Plant Participation Table Member Participation* for PWROG Project CEOG Task 2016, PA-OSC-288 and PA-OSC-367			
Utility Member	**Plant Site(s)**	**Participant**	
		Yes	**No**
AmerenUE	Callaway (W)		X
American Electric Power	D.C. Cook 1&2 (W)		X
Arizona Public Service	Palo Verde Unit 1, 2, & 3 (CE)	X	
Constellation Energy Group	Calvert Cliffs 1 & 2 (CE)	X	
Constellation Energy Group	Ginna (W)		X
Dominion Connecticut	Millstone 2 (CE)	X	
Dominion Connecticut	Millstone 3 (W)		X
Dominion Kewaunee	Kewaunee (W)		X
Dominion VA	North Anna 1 & 2, Surry 1 & 2 (W)		X
Duke Energy	Catawba 1 & 2, McGuire 1 & 2 (W)		X
Duke Energy	Oconee 1, 2, & 3 (B&W)		X
Entergy Nuclear Northeast	Indian Point 2 & 3 (W)		X
Entergy Operations South	Arkansas 2, Waterford 3 (CE)	X	
Entergy Operations South	Arkansas 1 (B&W)		X
Exelon Generation Co. LLC	Braidwood 1 & 2, Byron 1 & 2 (W)		X
Exelon Generation Co. LLC	Three Mile Island 1 (B&W)		X
FirstEnergy Nuclear Operating Co.	Davis Besse (B&W)		X
FirstEnergy Nuclear Operating Co.	Beaver Valley 1 & 2 (W)		X
Florida Power & Light Group	St. Lucie 1 & 2 (CE)	X	
Florida Power & Light Group	Turkey Point 3 & 4, Seabrook (W)		X
Nuclear Management Company	Prairie Island 1 & 2, Point Beach 1 & 2 (W)		X
Entergy Operations	Palisades (CE)	X	
Omaha Public Power District	Fort Calhoun (CE)	X	
Pacific Gas & Electric	Diablo Canyon 1 & 2 (W)		X
Progress Energy	Robinson 2, Shearon Harris (W)		X
Progress Energy	Crystal River 3 (B&W)		X
PSEG – Nuclear	Salem 1 & 2 (W)		X
Southern California Edison	SONGS 2 & 3 (CE)		X
South Carolina Electric & Gas	V.C. Summer (W)		X
South Texas Project Nuclear Operating Co.	South Texas Project 1 & 2 (W)		X
Southern Nuclear Operating Co.	Farley 1 & 2, Vogtle 1 & 2 (W)		X

PWR Owners Group Project Plant Participation Table Member Participation* for PWROG Project CEOG Task 2016, PA-OSC-288 and PA-OSC-367			
Utility Member	**Plant Site(s)**	**Participant**	
		Yes	**No**
Tennessee Valley Authority	Sequoyah 1 & 2, Watts Bar (W)		X
TXU Power	Comanche Peak 1 & 2 (W)		X
Wolf Creek Nuclear Operating Co.	Wolf Creek (W)		X
British Energy	Sizewell B		X
Electrabel (Belgian Utilities)	Doel 1, 2 & 4, Tihange 1 & 3		X
Kansai Electric Co., LTD	Mihama 1, Ohi 1 & 2, Takahama 1 (W)		X
Korea Hydro & Nuclear Power Corp.	Kori 1, 2, 3 & 4 Yonggwang 1 & 2 (W)		X
Korea Hydro & Nuclear Power Corp.	Yonggwang 3, 4, 5 & 6 Ulchin 3, 4 & 5 (CE)		X
Nuklearna Electrarna KRSKO	Krsko (W)		X
Nordostschweizerische Kraftwerke AG (NOK)	Beznau 1 & 2 (W)		X
Ringhals AB	Ringhals 2, 3 & 4 (W)		X
Spanish Utilities	Asco 1 & 2, Vandellos 2, Almaraz 1 & 2 (W)		X
Taiwan Power Co.	Maanshan 1 & 2 (W)		X
Electricite de France	54 Units		X

*** This is a list of participants in this project as of the date the final deliverable was completed. On occasion, additional members will join a project. Please contact the PWROG Program Management Office to verify participation before sending documents to non-participants listed above.**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

AC	Alternating Current
AFAS	Auxiliary Feedwater Actuation Signal
ALARA	As Low As Reasonably Achievable
ANO-2	Arkansas Nuclear One Unit 2
ASME	American Society of Mechanical Engineers
CAFTA	Computer Aided Fault Tree Analysis
CC-1,2	Calvert Cliffs Units 1 & 2
CCF	Common Cause Failure
CCW	Component Cooling Water
CDF	Core Damage Frequency
CE	Combustion Engineering
CEOG	CE Owners Group
CIS	Containment Isolation Signal
CIAS	Containment Isolation Actuation Signal
CPHS	Containment Internal Pressure High Signal
CR	Condition Report
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
ER	Event Report
ESCS	Engineered Safeguards Control System
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FCS	Fort Calhoun Station
FMEA	Failure Mode Effects Analysis
F&O	Facts & Observations
FTS	Failure to Start
HEP	Human Error Probability
HPSI	High Pressure Safety Injection
ISI	In-Service Inspection
IESFT	Integrated Engineered Safety Features Test
IST	In-Service Testing
LAR	License Amendment Request
LCO	Limiting Condition for Operation
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
LPSI	Low Pressure Safety Injection
LTOP	Low Temperature Over Pressurization
MCC	Motor Control Center
MGL	Multiple Greek Letter
MOV	Motor Operated Valve
MP2	Millstone Point Unit 2

ACRONYMS (continued)

MSIS	Main Steam Isolation Signal
MTBF	Mean Time Between Failure
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OOS	Out of Service
OPLS	Off-site Power Low Signal
OPPD	Omaha Public Power District
PAL	Palisades
PPLS	Pressurizer Pressure Low-Low Signal
PRA	Probabilistic Risk Assessment
PVNGS	Palo Verde Nuclear Generation Station
PWR	Pressurized Water Reactor
PWROG	Pressurized Water Reactor Owners Group
RAS	Recirculation Actuation Signal
RCS	Reactor Coolant System
RG	Regulatory Guide
RPS	Reactor Protection System
RWST	Refueling Water Storage Tank
SDC	Shutdown Cooling
SGIS	Steam Generator Isolation Signal
SIAS	Safety Injection Actuation Signal
SR	Surveillance Requirement
SSC	Structures, Systems and Components
STLS	Borated Water Tank Level Low-Low Signal
STI	Surveillance Test Interval
SW	Service Water
TS	Technical Specification
UV	Under Voltage
UVR	Under Voltage Relay
VAC	Volt Alternating Current
VCT	Volume Control Tank
VIAS	Ventilation Isolation Actuation Signal
VR	Voltage Regulator
WSES-3	Waterford Steam Electric Station Unit 3

ABSTRACT

The purpose of this report is to develop a generic methodology that individual plants may use as a model to apply staggered integrated Engineered Safety Features and Loss of Off-site Power (ESF/LOOP) testing at their plant. Utilities desiring to adopt a staggered integrated ESF/LOOP test program must submit a plant specific risk analysis and defense-in-depth evaluation, plus request a change to the affected TS surveillance intervals.

This report documents the results of Pressurized Water Reactor Owners Group (PWROG) CEOG Task 2016, "Staggered Integrated ESF/LOOP Testing." The generic methodology described in this report is applicable to CE NSSS plants. CEOG Task 2016 used a risk-informed, performance based approach to demonstrate that changing the integrated ESF/LOOP test interval from once per cycle on a sequential basis to once every other cycle on a staggered test basis results in a negligible change in risk. Currently, integrated ESF/LOOP testing is performed on both ESF trains each refueling cycle. Using a staggered approach, one ESF train will be tested each refueling outage with each ESF train being tested once every other cycle.

The methodology described in this report is consistent with NEI 04-10, Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies (Reference 1). NEI 04-10 uses a risk-informed, performance-based approach to establish surveillance frequencies, consistent with the philosophy of NRC Regulatory Guide 1.174 (Reference 2). Sensitivity studies were performed on important PRA parameters. PRA technical adequacy is addressed through NRC Regulatory Guide (RG) 1.200 (Reference 3), which references the ASME PRA standard, RA-Sb-2005, (Reference 4) for internal events at power. External events and shutdown risk impact may be considered quantitatively or qualitatively.

The defense-in-depth analysis on selected generic Category A components showed that extending the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] months to every other refueling interval on a staggered basis [36] months will not increase the unavailability of one train of ESF equipment. In addition, the increase in ESF/LOOP test interval will not decrease the defense-in-depth of the emergency power distribution system as required by General Design Criterion (GDC) 17 and GDC 18 (Reference 5) or change the acceptance criteria of Regulatory Guide (RG) 1.9, (Reference 6) RG 1.108, (Reference 7) and IEEE standard Std 387 (Reference 8) since all required Emergency Diesel Generator (EDG) testing will still be verified and EDG operation during emergency conditions will not compromised.

Results show that changing the interval of integrated ESF/LOOP testing on a given ESF train from once per normal refueling cycle [18] months with sequential testing to once every other cycle [36] months with staggered test basis results in change a negligible change in plant risk.

1.0 INTRODUCTION

1.1 KEY SAFETY PRINCIPLES FOR CHANGING SURVEILLANCE TEST FREQUENCIES

Regulatory Guide (RG) 1.174 (Reference 2) identifies five key safety principles to be met for all risk-informed applications and to be explicitly addressed in risk-informed plant program change applications. These principles summarized in the remainder of this section along with how these principles are met.

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change.

10 CFR 50.36(c) provides that Technical Specifications will include items in the following categories:

> "(3) Surveillance Requirements. Surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met."

The staggered integrated Engineered Safety Features and Loss of Off-site Power (ESF/LOOP) test program extends the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] months to every other refueling interval on a staggered basis [36] months. This safety principle is met since the surveillance requirements normally addressed by the integrated test would not be changed and would remain in the Technical Specifications.

2. The proposed change is consistent with the defense-in-depth philosophy.

Consistency with the defense-in-depth philosophy is maintained if:

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

> The Surveillance Test Interval (STI) change has only a small-calculated impact on Core Damage Frequency (CDF) and Large Early Release Frequency (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 change. 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 to compensate for weaknesses in plant design is avoided.

> The plant design will not be changed to accommodate the STI extension. All safety systems, including the Engineered Safety Features Actuation System (ESFAS), will still function in the same manner with the same signals available to trip the reactor and initiate Engineered Safety Features (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 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

3. The proposed change maintains sufficient safety margins.

Conformance with this principle is assured with changes in surveillance test frequencies since the Structure, Systems and Components (SSC) design, operation, testing methods, and acceptance criteria specified in applicable Codes and Standards, or alternatives approved for use by the Nuclear Regulatory Commission (NRC), will continue to be met as described in the plant licensing basis (i.e., FSAR, or Technical Specifications Bases). Also, the safety analysis acceptance criteria in the utilities licensing basis (i.e., Final Safety Analysis Report (FSAR), supporting analyses) will continue to be met with the changes to surveillance frequencies.

4. When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.

In the methodology described in this report, the overall impact of the change is assessed and compared to the quantitative risk acceptance guidelines of RG 1.174, which is consistent with the intent of the Commission's Safety Goal Policy Statement. The effects on CDF and LERF are considered. The first effect involves the total or aggregate risk impact for all Probabilistic Risk Assessment (PRA) events for each individual surveillance frequency change. The second effect involves the cumulative risk impact from all surveillance frequency changes. More detail is provided in subsequent paragraphs that describe the generic methodology. The PRA used to support this change will, at a minimum, address CDF and

LERF for power operation. External event risk and shutdown considerations will be addressed through quantitative or qualitative means.

RG 1.200 addresses technical adequacy of PRA for risk-informed applications. This regulatory guide will be followed by utilities seeking to implement staggered integrated ESF/LOOP testing based on this report.

5. **The impact of the proposed change should be monitored using performance measurement strategies.**

A performance monitoring strategy will be developed by the applicant to provide confidence that the equipment performance is consistent with the considerations of the overall goals of RG 1.174, and is not degrading such that the analysis assumptions are no longer valid. For certain cases, existing performance monitoring required by the Maintenance Rule (Reference 9) may be adequate for SSCs whose surveillance frequencies are impacted by the staggered integrated ESF/LOOP test program. The output of the performance monitoring will be periodically re-assessed by the applicant and appropriate adjustments made to the surveillance frequencies.

1.2 PURPOSE

The objective of this report is to demonstrate that adopting a staggered test basis for Surveillance Requirements (SRs) typically addressed by Integrated ESF/LOOP testing results in a negligible change in plant risk. The staggered integrated ESF/LOOP test program proposes to extend the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] months to every other refueling interval on a staggered basis [36] months. The methodology uses a risk-informed, performance based approach and is consistent with the guidelines for evaluating changes to STIs contained in NEI 04-10 (Reference 1).

Seven Combustion Engineering NSSS utilities representing a total of twelve units participated in various elements of this project. 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. Entergy Nuclear North, 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 change will benefit the utilities in the following ways:

1. Reduce Human Performance challenges
2. Dose/radiation exposure reduction (ALARA)
3. Reduce Reactor Coolant System (RCS) mass addition challenges
4. Reduce safety equipment wear and tear
5. Reduce challenges to safety related equipment
6. Reduced outage time

1.3 APPROACH AND METHODOLOGY

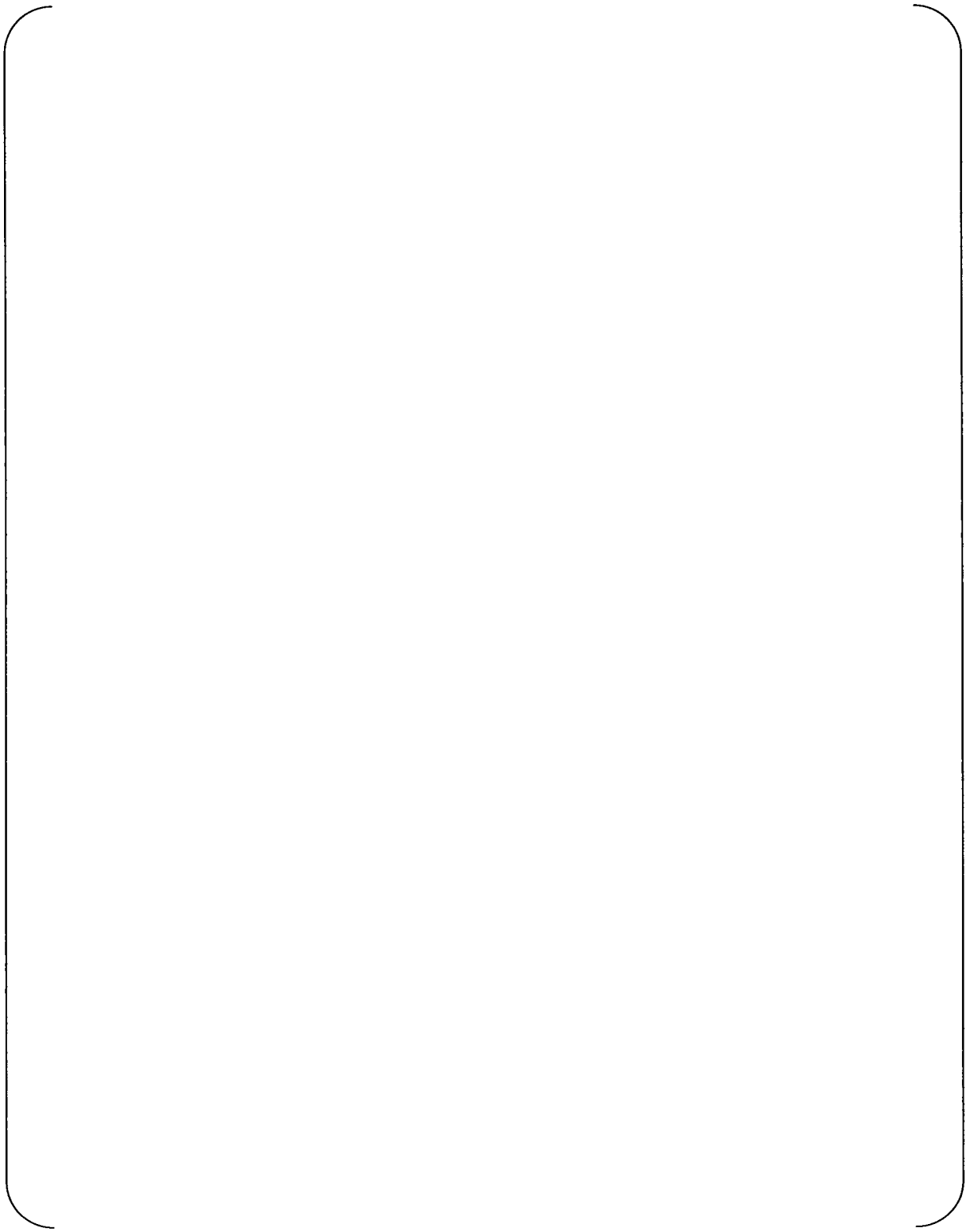
This methodology uses a risk-informed, performance based approach to demonstrate that any change in risk will be negligible if a staggered test basis is adopted for surveillance requirements normally addressed by the integrated ESF/LOOP test. The methodology is consistent with the philosophy of RG 1.174 (Reference 2) and NEI 04-10, Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies (Reference 1). Sensitivity studies were performed on important PRA parameters. PRA technical adequacy for the demonstration plants was partially addressed in this report to ensure the validity of the results in the demonstration appendices. PRA technical adequacy must be completely addressed at the time of License Amendment Request (LAR) submittal to show compliance with current RG 1.200 requirements (Reference 3).

The integrated ESF/LOOP 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/LOOP testing. For the components and functions tested only by the integrated ESF/LOOP 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 PRA review and analysis.

A deterministic evaluation was performed on generic components typically tested only by the integrated ESF/LOOP test. The evaluation basically consisted of a generic Failure Modes and Effect Analysis (FMEA). The purpose of the evaluation was to: (1) show that there are no non-constant failure rates and no Mean Time between Failure (MTBF) greater than test interval (36 months), (2) show that the change will not degrade the performance of either ESF or emergency power train and (3) confirm the overall conclusions of the risk analyses.

a,c

a,c



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/LOOP 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/LOOP testing include inadvertently transferring water to the containment sump, inadvertent transfers from the Boric Acid Storage Tanks (BAST) resulting in violating the minimum requirements, overflowing the Refueling Water Storage Tank (RWST), and exceeding the maximum overpressure in the Volume Control Tank (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/LOOP testing is the most complex test run during an outage. Testing on each channel takes approximately 24 hours to complete: eight hours to establish the equipment lineup, eight hours to run the test, and eight hours to restore. During the eight 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/LOOP 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 usually run the test on both trains.

During a typical refueling outage at a plant, there are extra personnel in the plant performing a variety of tasks. Many of the extra personnel may be contractors or technicians from other plants. Many systems and components are tagged Out-of-Service (OOS) to support outage maintenance activities. It is challenging for outage management and operations to coordinate and execute all the required work activities, surveillance testing, and post maintenance realignments. Reducing the amount of required testing and abnormal 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/LOOP 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.

The integrated ESF/LOOP 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 a stop watch or data recorder was not started 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/LOOP 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 change to reduce the amount of testing may result in savings in avoidable exposure. This would help the plant realize as low as reasonable achievable (ALARA) radiation exposure for the outage.

Reduction in RCS mass additions challenges

Integrated ESF/LOOP testing involves testing the response of an entire ESF train to various actuation signals, either with or without off-site 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 can inject water into the RCS if an isolation valve is misaligned or a check valve leaks-by during the test. 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/LOOP testing supports this objective.

Reduction in challenges to safety equipment and plant security

As mentioned previously, by reducing the amount of integrated ESF/LOOP 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/LOOP 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 address 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 during testing. However, for the reasons mentioned above, sometimes it is necessary to repeat a test for reasons that are relatively minor. It is this additional wear-and-tear on equipment that could be reduced by limiting the amount of integrated ESF/LOOP testing performed during an outage.

Also, by necessity during the integrated ESF/LOOP 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/LOOP 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, i.e., electrical shock, burns, injury to the eyes or injury from a fall. By reducing the amount of testing, the potential for personnel injury due to high-risk tasks will also be reduced.

Reduction in Operation and Maintenance costs

Integrated ESF/LOOP 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. 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/LOOP testing in the outage by one half, thousands of dollars in labor costs alone can be saved each outage.

2.2 TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS TYPICALLY ADDRESSED BY INTEGRATED ESF/LOOP TESTING AND WITHIN THE SCOPE OF THIS REPORT

Integrated ESF/LOOP testing is performed each refueling outage to satisfy numerous refueling interval Technical Specification (TS) surveillance requirements on engineered safeguards equipment including the Emergency Diesel Generators (EDG). Both engineered safeguard trains are tested each refueling interval, one train at a time. Plant specific Integrated ESF/LOOP test procedures explicitly list all surveillance requirements addressed by the procedures. There is considerable variation in integrated ESF/LOOP test procedures from one plant to the next. Integrated ESF/LOOP test procedures reviewed for this effort did however have certain objectives in common. The following is a summary of the surveillance requirements (per NUREG-1432, Reference 10) that are typically addressed by integrated ESF/LOOP testing. These results are consistent with Surveillance Requirements (SRs) typically addressed at custom TS plants as well.

2.2.1 Related Technical Specifications

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 off-site 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 ≥ [3740] V and ≤[4580] V
    3. Maintains steady state frequency ≥ [58.8] Hz and < [61.2] Hz, and
    4. Supplies permanently connected [and auto-connected] shutdown loads for ≥ [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 ≤ [10] seconds after auto-start and during tests, achieves voltage ≥ [3740] V and frequency of ≥ [58.8] Hz
b. Achieves steady state voltage ≥ [3740] V and ≤[4580] V and frequency ≥ [58.8] Hz and < [61.2] Hz
c. Operates for ≥ [5] minutes
d. Permanently connected loads remain energized from the off-site power system, and
e. Emergency loads are energized [or auto-connected through the automatic load sequencer] from the off-site power system.

SR 3.8.1.16 - Verify each EDG:

a. Synchronizes with off-site power source while loaded with emergency loads upon a simulated restoration of off-site power
b. Transfers loads to off-site power source, and

[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.

c. Returns to ready-to-load operation.

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

SR 3.8.1.19 - Verify on an actual or simulated loss of off-site 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 ≥ [3740] V and ≤[4580] V
4. Achieves steady state frequency ≥ [58.8] Hz and < [61.2] Hz, and
5. Supplies permanently connected [and auto-connected] shutdown loads for ≥ [5] minutes.

CE NSSS plants frequently coordinate other EDG surveillance testing with the integrated ESF test when appropriate. The type and nature of these tests varies greatly from one plant to another. 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 ≤ [10] seconds and achieves rated voltage and frequency when stated within 5 minutes of shutting down following ≥ [2] hours of operation.

- SR 3.8.1.17 - Verify, with an 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 off-site power.

Some utilities for CE NSSS plants use integrated ESF/LOOP testing to partially satisfy additional Technical Specification SRs or testing as 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 SRs provide examples that are typically partially addressed by the integrated ESF/LOOP 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

2.2.2 Related Technical Specifications Bases

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

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 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 Off-site Power

This surveillance demonstrates the "as designed operation" of the standby power sources during loss of the off-site source. The test verifies all actions encountered from the loss of off-site 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 Loss of Coolant Accident (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, HPSI 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 off-site electrical power system on an ESF signal without loss of off-site 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, HPSI 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 off-site power following Loss of Off-site power verification

This surveillance ensures that the manual synchronization and automatic load transfer from the EDG to the off-site source can be made and that the EDG can be returned to ready to load status when off-site power is restored. It also ensures that the auto-start logic is reset to allow the EDG to reload if a subsequent loss of off-site 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 off-site 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 Design Basis Accident (DBA) coincident with a loss of off-site 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 off-site 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.

2.2.3 Technical Specifications STIs within the Scope of this Topical Report

SR 3.3.5.2 - Channel Functional Test on ESFAS Manual Trip Channel
SR 3.8.1.11 - EDG start verification on Loss of Off-site Power
SR 3.8.1.12 - EDG start verification on ESF actuation
SR 3.8.1.16 - Restoration of off-site power following Loss of Off-site power verification
SR 3.8.1.19 - EDG start verification on Loss of Off-site Power with ESF actuation

Note: SR 3.8.1.18 - EDG Load sequencer interval verification testing is not explicitly included in the scope of the change addressed by this report. Sequencer design, calibration and functional testing is plant specific. However, sequencer testing may be included in the staggered integrated ESF/LOOP test program if it is found to be acceptable based on plant specific drift analysis. Additional plant specific evaluations would be required to justify the change.

2.3 INDUSTRY INITIATIVES AND REGULATORY GUIDELINES RELATED TO CHANGING TS SURVEILLANCE TEST INTERVALS

Several industry initiatives and regulatory guidelines are applicable to changing STIs including implementation of staggered integrated ESF/LOOP testing. These documents are identified in the remainder of this sub-section.

2.3.1 Regulatory Guidelines

Regulatory Guide 1.200, Revision 1, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," January 2007 (Reference 3)

NRC has developed RG 1.200 (Reference 3) to address PRA technical capability. RG 1.200 addresses the use of the ASME PRA standard (Reference 4) and the NEI peer review process (NEI 00-02, Reference 11) for evaluating PRA technical capability. RG 1.200 also provides attributes of importance for risk determinations relative to external events, seismic, internal fires, and shutdown. Plants implementing staggered integrated ESF/LOOP testing shall evaluate their PRAs in accordance with this regulatory guide. The RG specifically addresses the need to evaluate important assumptions that relate to key modeling uncertainties (such as common cause failure methods, success path determinations, human reliability assumptions, etc). Further, the RG addresses the need to evaluate parameter uncertainties and demonstrate that calculated risk metrics (i.e., CDF and LERF) represent mean values. The identified "Gaps" to Capability Category II requirements from the endorsed ASME PRA Standards in the RG and the identified key sources of uncertainty serve as inputs to identify appropriate sensitivity cases to be run.

Regulatory Guide 1.174, Revision 1, "An approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific changes to the Licensing Basis," November 2002 (Reference 2)

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, PRA 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 judgment on the complexity and difficulty of implementing the proposed licensing basis change to decide upon appropriate engineering analyses to support regulatory decision-making. 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 PRA 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 (i.e., QA program changes under 10 CFR 50.54(a)).

Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," August 1998 (Reference 12)

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 Surveillance Test Intervals (STIs) in order to assess the impact of such proposed changes on the risk associated with plant operation.

A typical approach to integrated decision-making 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 (i.e., topical reports), methods, codes and PRA 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 securing regulatory approval.

Regulatory Guide 1.9, Revision 3, "Selection, Design, Qualification and Testing of Emergency Diesel Generator Units used as Class 1E Onsite Electric Power Systems at Nuclear Power Plants, July 1993 (Reference 6).

This regulatory guide provides guidance acceptable to the NRC staff for complying with the Commission's requirements that diesel generator units intended for use a onsite emergency power sources in nuclear power plants to be selected with sufficient capacity, be qualified, and have the necessary reliability and availability for station blackout and design basis accidents.

Regulatory Guide 1.108, Revision 1, "Periodic Testing of Diesel Generator Units used as Onsite Electric Power Systems at Nuclear Power Plants," August 1977 (Reference 7).

This regulatory guide describes a method acceptable to the NRC staff for complying with the Commission's regulations with regard to periodic testing of diesel electric power units to ensure that the diesel electric power systems will meet their availability requirements.

General Design Criteria GDC 17 and GDC 18, 10CFR50, Appendix A (Reference 5)

Criterion 17, "Electric Power Systems," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10CFR Part 50 requires that onsite electric power systems have sufficient independence, capacity, redundancy and testability to perform their safety functions, assuming a single failure.

Criterion 18, "Inspection and Testing of Electric Power Systems," of Appendix A to 10CFR part 50 requires that electric power systems important to safety be designed to permit appropriate periodic inspection, and testing to assess the continuity of the systems and the condition of their components.

2.3.2 Industry Initiatives

TSTF-425, Revision 1, "Relocate Surveillance Frequencies to Licensee Control - RITSTF Initiative 5," (Reference 13)

Revision 1 of TSTF-425 expands the applicability of the change to all reactor types and references Revision 1 of NEI 04-10, "Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies, Industry Guidance Document." Revision 1 of NEI 04-10 was submitted by the Nuclear Energy Institute on April 19, 2007.

NEI 04-10, Revision 0, "Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies," July 2006 (Reference 1)

This document provides guidance for implementation of a generic Technical Specifications improvement that establishes licensee control of surveillance test frequencies for the majority of Technical Specifications surveillances. Existing specific surveillance frequencies are removed from Technical Specifications for the affected specifications, and placed under licensee control pursuant to this methodology. A paragraph is added to the Administrative Controls section referencing this methodology document, as approved by NRC, for control of surveillance frequencies. The surveillance test requirements (test methods) are not changed and remain in the Specifications.

This methodology uses a risk-informed, performance-based approach for establishment of surveillance frequencies, consistent with the philosophy of NRC RG 1.174. Probabilistic Risk Assessment (PRA) methods are used to determine the risk impact of the revised intervals. Sensitivity studies are performed on important PRA parameters. PRA technical adequacy is addressed through NRC RG 1.200, which references the ASME PRA Standard, RA-Sb-2005, for internal events at power. External events and shutdown risk impact may be considered quantitatively or qualitatively.

A multi-disciplinary plant decision-making panel is utilized to evaluate determinations of revised surveillance frequencies, based on operating experience, test history, manufacturers recommendations, codes and standards, and other factors, in conjunction with the risk insights from the PRA. Results and bases for the decision must be documented. The methodology includes guidance on determining the specific surveillance frequencies to which this process is applied; existing frequencies are retained if the process is not applied.

Process elements are included for determining the cumulative risk impact of the changes, updating the PRA, and for imposing corrective actions, if necessary, following implementation.

NEI 06-09, Revision 0, "Risk-Informed Technical Specifications Initiative 4B, Risk-Managed Technical Specifications (RMTS) Guidelines," November 2006 (Reference 14)

This document provides guidance for implementation of a generic Technical Specifications improvement that establishes a risk management approach for voluntary extensions of completion times for certain Limiting Conditions for Operation. This document provides the risk management methodology, and will be referenced through a paragraph added to the Administrative Controls section.

This methodology uses a risk-informed approach for establishment of extended completion times, and is consistent with the philosophy of NRC RG 1.174. Probabilistic Risk Assessment (PRA) methods are used to determine the risk impact of the revised completion times. PRA technical adequacy is addressed through NRC RG 1.200, which references the ASME PRA Standard, RA-S-2005b for internal events at power. Quantification of risk due to internal fire is also necessary for this application, through PRA or bounding methods.

Section 2.0 of the document provides requirements for implementation. Section 3.0 provides additional implementation guidance relative to these requirements. Section 4.0 presents attributes of the PRA and configuration risk assessment tools. The extension of completion time must take into account the configuration-specific risk, and is an extension of the methods used to comply with paragraph (a)(4) of

the Maintenance Rule, 10CFR50.65. Plants implementing this initiative are expected to use the same PRA analyses to support their Maintenance Rule (a)(4) programs. A deterministic backstop value is imposed to limit the completion time extension regardless of low risk impact. Results of implementation are monitored, and cumulative risk impacts are compared to specific risk criteria. Corrective actions are implemented should these criteria be exceeded.

2.3.3 Industry Standards and Guides

NUREG-0800, Standard Review Plan 19.1, "Determining The Technical Adequacy Of Probabilistic Risk Assessment Results For Risk-Informed Activities," June 2007, (Reference 15).

NUREG-0800, Standard Review Plan 19.2, "Review of Risk Information Used To Support Permanent Plant specific Changes To The Licensing Basis: General Guidance" June 2007, (Reference 16).

NUREG-0800, Standard Review Plan 16.1, "Risk-Informed Decisionmaking: Technical Specifications," March 2007, (Reference 17).

ASME RA-Sb-2005, "Addenda to ASME RA-S-2002 Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications", December 2005, (Reference 4).

ASME OM-S/G-2000, Standards and Guides for Operation and Maintenance of Nuclear Power Plants (Reference 18) - Part 15, Performance Testing of Emergency Core Cooling Systems in Pressurized Water Reactor Power Plants.

Part 15 of the ASME code establishes the requirements for in-service testing to assess the operational readiness of Emergency Core Cooling Systems (ECCS), including those systems required for long-term decay heat removal, used in Pressurized Water Reactors (PWRs). It establishes test methods, test intervals, parameters to be measures and evaluated, acceptance criteria, corrective actions, and records requirements for the purpose of assessing integrated system performance. In-service testing is required to be conducted at 5-year intervals, 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.

IEEE Std 387-1995, "IEEE Standard Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power." (Reference 8)

This standard describes the criteria for the application and testing of diesel generator units as Class 1E standby power supplies in nuclear power generating stations.

2.3.4 Related ESFAS CEOG Reports

CEN-327-A, RPS/ESFAS Extended Test Interval Evaluation (Reference 19)

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 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 CDF and system unavailability to demonstrate that the proposed changes did

not adversely increase the plant risk when compared with the current technical specifications requirements.

CEN-403, ESFAS Subgroup Relay Test Interval Extension (Reference 20)

This report justifies extending the ESFAS subgroup relay STI for Combustion Engineering (CE) Nuclear Steam Supply System (NSSS) plants. The study evaluated the performance of these relays in plants with CE designed NSSS from different perspectives. The original CEN-403 evaluated all relays generically, where as 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 refueling interval be extended to the refueling 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 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, Arkansas Nuclear One Unit 2 (ANO-2), and Palo Verde Nuclear Generating 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 at each plant. But the processing of the signals and the actuation of equipment is common to all the plants.

All ESFAS designs typically require two-out-of-four coincidence of like parameter signals to exceed a setpoint to initiate ESFAS. One measurement channel can be bypassed, leaving a two-out-of-three condition to initiate ESFAS. Also, all systems allow for one measurement channel to go into test, leaving a 1 out of 3 condition to initiate ESFAS.

The later vintage plant designs combined RPS and ESFAS measurement channels. The older plants designs 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 PRA models include this level of detail, they show a dependency between ESFAS and mitigating systems, i.e., ESFAS starts of a HPSI pump. It is customary to model the instrument loops 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. 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 (References 21, 22, 23, 24 and 25) for those plants that utilize a non-CE ESFAS design. Additional ESFAS system descriptions are 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 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 ESFAS design simply tests for two-out-of-four signals exceeding a setpoint value (or out-of-service) using electromechanical relays. Fort Calhoun is the first of the CE supplied NSSS plants to house the ESFAS in a specific control room cabinet. Although functionally very similar, Palisades does not have an ESFAS cabinet otherwise typical of a CE supplied NSSS 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.

Palisade's 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 CE supplied NSSS plant to compare analog sensor output versus a fixed signal using a separate bistable device.

At Palisades, there are multiple sets of actuation relays, i.e., a set of SIAS actuation relays derived from pressurizer low-pressure. At the Calvert Cliffs and Waterford 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 supplied NSSS 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 function as if a parameter exceeded a setpoint.

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

Four instrument loops 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-design 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. 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:

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 the channels while maintaining a two-out-of-three system. A plant specific description of each of the above signals is presented in the FSARs (References 26, 27 and 29) for those plants that utilize the CE ESFAS design. Additional ESFAS system description is provided in Appendix D for the Waterford Unit 3.

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

The Waterford ESFAS design is the most complex of the three systems but also the most flexible in terms of testing and maintenance. The Waterford ESFAS design splits the power supply into four trains with the coincidence logic 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 by 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 initiation 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 Alternating Current (AC) distribution bus.

The initiation 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 initiation 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 de-energizes the bistable output relay. The bistable output relay de-energizes the trip relays. 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 initiation 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 120 volt vital AC 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. The actuated components 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 pump motors.

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 actuation 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

The basic methodology uses a risk-informed approach, based on RG 1.174 (Reference 2) to demonstrate that any change in risk will be negligible when integrated ESF/LOOP surveillance testing is performed on a staggered basis. Currently, the integrated ESF/LOOP test is preformed on both ESF trains during normal refueling cycle to satisfy Technical Specifications (TSs) surveillance requirements.

This methodology uses a balanced approach between risk-informed and deterministic assessments to demonstrate that changing the integrated ESF/LOOP test interval between successive tests on a given ESF train from once every refueling interval [18] months to once every other refueling interval on a staggered basis [36] months results in a negligible change in risk. TS surveillance procedures for the participating plants were reviewed to identify overlap in component and functional testing. Each component tested by the integrated ESF/LOOP test was placed into a unique Category (A, B or C).

Category A components, those tested solely by the integrated ESF/LOOP test, were then analyzed in detail using a risk-informed approach. The associated risk model was adjusted as necessary. The change in risk was then recalculated and the results evaluated. A deterministic evaluation was also performed on the Category A components to confirm the conclusions of the risk analyses. Finally, the combined results (risk and deterministic) were evaluated using RG 1.174 criteria. The methodology includes performance of sensitivity studies on important PRA parameters. It does not completely address PRA quality issues for the demonstration plants. PRA technical adequacy (quality) will be addressed per NRC RG 1.200 requirements through a plant-specific submittal.

The methodology is consistent with NEI 04-10, Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies (Reference 1). NEI 04-10 uses a risk-informed, performance-based approach to establish surveillance frequencies, consistent with the philosophy of NRC RG 1.174.

The STI changes described in this report only apply to plants with an 18 month refueling cycle. The methodology may also be applied to 24 month refueling cycle plants, but only after additional analyses are performed to evaluate the associated STI changes.

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

Changes in the test interval for the integrated ESF/LOOP 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/LOOP test. Plant PRA 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 PRA model. Where this was not possible, the appropriate event frequencies (i.e., STIs) in the PRA model were revised to account for the 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 change in the integrated ESF/LOOP test interval on risk was assessed by comparing the risk measures (CDF and LERF) for the existing and staggered testing schemes. The risk measures for the existing testing schemes were determined by analyses using base PRA models at the demonstration plants. Quantification of the revised PRA model, reflecting the extended test interval and revised test scheme, determined the risk measures for the proposed staggered testing scheme.

The effect of a staggered surveillance schedule on plant risk is negligible because the integrated ESF/LOOP test is not the primary or sole operability test for the majority of the components tested by this test. Operability and reliability of these components is demonstrated by other surveillance tests that are performed on the same or a more frequent basis since there is considerable overlap between other TS required tests and the integrated ESF/LOOP test. Also, for those components tested only by the integrated ESF/LOOP, a risk informed and deterministic analyses of these components will show that the overall change in plant risk is acceptable.

4.2 PROCEDURE REVIEW PROCESS

4.2.1 Functions Tested by the Integrated ESF/LOOP Test

The integrated ESF/LOOP test procedure is typically divided into two parts, the Loss of Off-site Power and the Loss of Off-site Power with a concurrent LOCA. Although details vary from plant to plant, the test is usually initiated by simulating a loss of off-site power on the selected emergency bus, and either simulating or manually actuating SIAS on the associated ESF train. Integrated ESF and LOOP testing may be performed at any time during the outage when the plant is shutdown.

Test procedures were reviewed for the lead plant and seven (7) demonstration plants. The purpose of the review was to identify all of the components and functions tested by the integrated ESF/LOOP test. The functions are plant specific. They are usually clearly stated in the objectives or acceptance criteria of the procedure or bases document.

The objectives of the integrated test typically verify the following:

- EDG automatic start on Under Voltage (UV) and SIAS
- Automatic load shedding
- EDG energizing emergency bus and automatic sequencing of loads onto EDG
- Permanent loads energized
- SIAS actuation
- Return to normal off-site power test

Table 4.2-1 shows a comparison of the functions commonly tested by the integrated ESF/LOOP test at each plant in order to illustrate the variety of test schemes used by the CE supplied NSSS plants. The shaded areas for Table 4.2-1 show the functions selected to be included in the review process. Note that EDG testing as related to LOOP events (with or without ESF actuation), automatic start verification, load shedding and sequencing are included.

4.2.2 Diesel Generator Testing Included in the Integrated ESF/LOOP Test

Some utilities include additional EDG testing in the integrated ESF/LOOP test in order to minimize EDG cycling. 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 but may be addressed on a plant specific basis.

4.2.3 Review and Overlap with Other ESF Surveillance Tests

Once the integrated ESF/LOOP 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/LOOP test. An overlapping test is defined as one that tests the same component and function as the integrated ESF/LOOP test at the same or greater frequency. Examples of overlapping tests are the quarterly ISI/IST valve and pump tests; and quarterly ESFAS logic and relay testing.

Table 4.2-1
Functions Addressed by Integrated ESF/LOOP Test [(1)]

a,c

Objective	PV-1,2,3	CC-1,2	MP-2	SL-1,2	FCS	PAL	ANO-2	WSES-3

Table 4.2.2
Emergency Diesel Generator Testing Included in the Integrated Safeguards Tests
(not specifically addressed in this report)

a,c

Function	PV-1,2,3	CC-1,2	MP-2	SL-1,2	FCS	PAL	ANO-2	WSES-3

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/LOOP test. The matrix also includes other TS surveillance tests that tested the same component or function. In addition to the matrix, simplified schematics were created to illustrate the overlap in testing. These schematics are not intended to provide engineering and system design detail. Figures 4.2-1 through 4.2-8 illustrate the overlap in ESF testing at Fort Calhoun Station (Lead Plant). Similar plant-specific schematics for the most significant tests are included in the appendices for the other demonstration plants. Quarterly pump and valve operability tests are not included because they are too numerous.

The schematics 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 4.2-1 through 4.2-6 address testing associated with SIAS, CIAS, CSAS, RAS, SGIS and VIAS actuations. Figure 4.2-7 covers EDG load sequencers. Figure 4.2-8 covers under voltage sensing (OPLS). 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/LOOP test. This information was used to categorize each component in one of three basic categories (A, B or C).

Figure 4.2-1
SIAS Surveillance Procedures – Ft. Calhoun

a,c

Figure 4.2-2
CIAS Surveillance Procedures – Ft. Calhoun

a,c

Figure 4.2-3
CSAS Surveillance Procedures – Ft. Calhoun

a,c

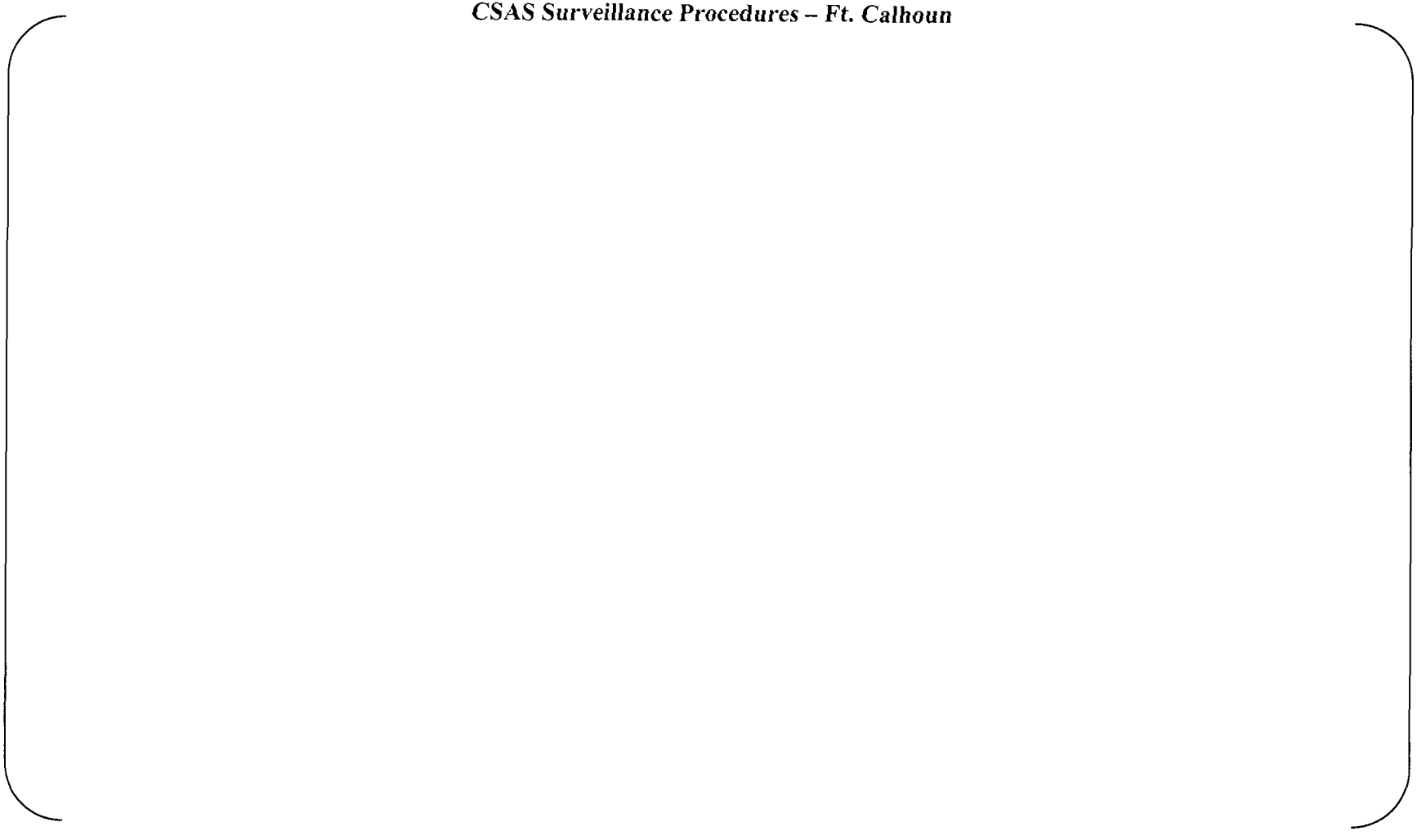


Figure 4.2-4
RAS Surveillance Procedures – Ft. Calhoun

a.c

Figure 4.2-5
SGIS Surveillance Procedures – Ft. Calhoun

a.c

Figure 4.2-6
VIAS Surveillance Procedures – Ft. Calhoun

a.c

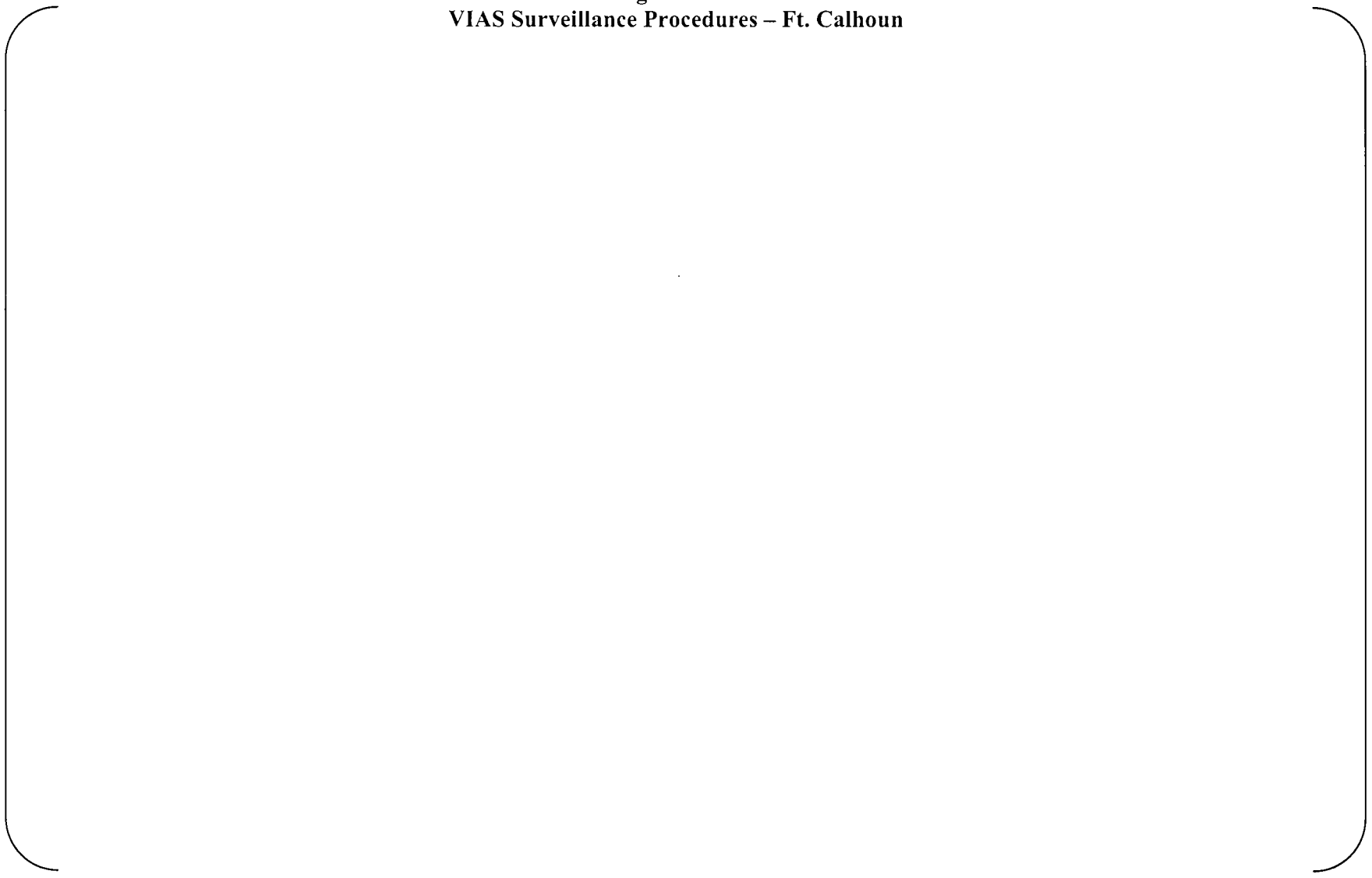


Figure 4.2-7
Sequences Surveillance Procedures – Ft. Calhoun

a,c

Figure 4.2-8
OPLS Surveillance Procedures – Ft. Calhoun

a,c

4.3 COMPONENT SCREENING AND CATEGORIZATION PROCESS

4.3.1 Category Definitions

In this phase of the evaluation, the list of category A and B components generated in Section 4.2 was further divided into sub-categories A-1, A-2 A-3, A-4 and B. This was accomplished using surveillance procedures, the list of basic events from the Fort Calhoun PRA, FCS Generic Letter 96-01 evaluations and responses, as well as selected plant drawings (primarily electrical one-lines and P&IDs). The sub-categories were developed to facilitate evaluating the Category A components and to make recommendations for calculating the change in risk.

a,c

The component/function categorization is discussed more in the following paragraphs.

The FCS categorization is based on both the plant-specific procedure review described earlier in this report, and a review of the plant PRA model. The three basic categories are defined as follows:

a,c

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

a,c

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

a,c

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

a,c

4.3.2 Classification Results

Table 4.3.2-1 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 PRA model may address these functions differently, resulting in two subcategories for the single component.

Table 4.3.2-1
Summary of Classification Results by Unit [1]

a.c

Category	Evaluation Summary	Number of Components / Functions							
		ANO-2	PV-1,2,3	CC-1,2	SL-1,2	MP-2 [3]	FCS [5]	PAL	WSES-3 [2]

4.4 GUIDELINES FOR PLANT SPECIFIC PRA MODEL ADJUSTMENTS AND REQUANTIFICATION

This categorization promotes uniformity among plant specific PRA evaluations by providing a process to determine the change in risk when performing integrated ESF/LOOP surveillance tests on a staggered test basis. The following two factors are crucial to the establishment of the risk quantification methodology:

1. Standby Failure Rate Model

   The assumption behind stand-by time dependent events is that at the conclusion of each test, the tested component is as good as new. Below is the equation for the average unavailability for the Standby Failure Rate Model:

$$Q = \frac{\lambda \tau}{2} \qquad \text{(Eqn. 4.4-1)}$$

   where λ is the standby failure rate; Q is the average unavailability or probability of failure on demand given random demands and test interval τ.

   From the above equation, the doubling of the test interval, τ, results in the doubling of the average unavailability Q.

2. Treatment of Common Cause Failures

   Common Cause Failure (CCF) must be considered when evaluating implementation of a staggered integrated ESF/LOOP test basis. CCF represents redundant components failing for the same reason(s) and are linked to the same coupling mechanism.

   The two main methods for treating CCF are the Alpha Model and the Multiple Greek Letter (MGL) approach. (See NUREG/CR-5485, Reference 30.) For a two train system, the Beta-factor technique is used to model common cause failures. In this approach, a basic event is inserted into the PRA model to represent the simultaneous failure of each redundant component due to the unspecified common cause. The probability of the common cause failure is quantified by a fraction, β, of the total failure probability for one of the individual components. As shown in Equation A.61 in Section A.3 of Reference 30, the β factor for sequential testing is twice the β factor for staggered testing for a given test interval, or:

$$\beta_S = 1/2\ \beta_{NS} \qquad \text{(Eqn 4.4-2)}$$

   Where β_S is the β factor for staggered testing and β_{NS} is the β factor for non-staggered or sequential testing.

   If the integrated ESF test interval is modified from once per refueling cycle to every other refueling cycle and sequential testing remains, the average CCF unavailability for an applicable component doubles. Since the integrated ESF test is being analyzed using a doubled test interval with staggered testing of the two trains, the CCF unavailability for the staggered test interval is one-half of the CCF unavailability for sequential testing. As a result, the net impact on CCF unavailability of doubling the test interval and also changing from sequential to staggered testing is that the CCF unavailability will remain unchanged. This can be represented as:

$$\beta_{NS,E} = 2 * \beta_{NS,B} \qquad \text{(Eqn. 4.4-3)}$$

Where $\beta_{NS,B}$ is the β factor for the base test interval with non-staggered testing and, $\beta_{NS,E}$ is the β factor for the extended test interval with non-staggered testing.

Based on Equation 4.4-2:

$$\beta_{S,E} = \beta_{NS,B} \quad \text{(Eqn. 4.4-4)}$$

Or, based on Equation 4.4-3:

$$\beta_{S,E} = \frac{1}{2} (2 * \beta_{NS,B}) \quad \text{(Eqn. 4.4-5)}$$

Which reduces to:

$$\beta_{S,E} = \beta_{NS,B} \quad \text{(Eqn. 4.4-6)}$$

4.4.1 Modifying the PRA Model for the New Baseline Case with Category A-3 and A-4 Components

[a.c

]

4.4.1.1 Incorporating Category A-3 Components into the New Baseline PRA Model

[a.c

]

4.4.1.2 Integrating Category A-4 Components into the New Baseline PRA Model

[ ] a,c

4.4.1.3 Requantify Base Model

[ ] a,c

4.4.2 Procedure for Requantifying the Baseline PRA Model for the Extended Staggered Test Interval

[ ] a,c

4.4.2.1 Category A-1

[ ] a,c

a,c

4.4.2.2 Category A-2

a,c

4.4.2.3 Category A-3

a,c

a,c

4.4.2.4 Category A-4

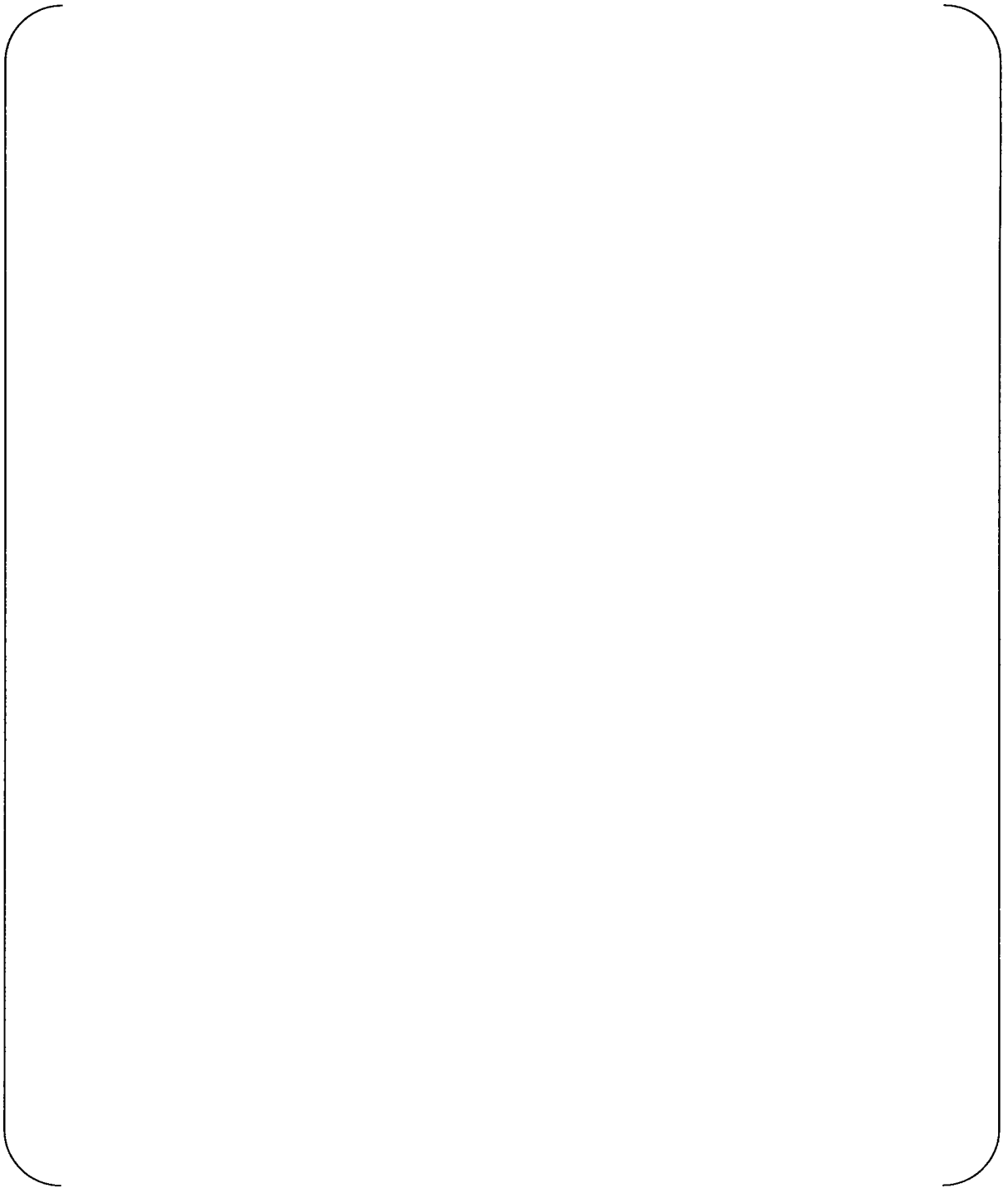
a,c

4.4.3 Category B

a,c

a,c

a,c



4.5 LOAD SHED AND BREAKER MODELING ISSUES AND CONSIDERATIONS

4.5.1 Breaker Modeling Issues

The circuit breakers of concern can be divided into two main groups for evaluation of the modeling issues; safety-related breakers and non-safety related breakers. The following subsections discuss the modeling issues for these breakers and any associated subgroups.

4.5.2 Safety-related Breakers

The safety-related circuit breakers provide power to safety-related loads on the 4.16kV vital buses and 480 Volt Alternating Current (VAC) vital buses. These breakers are further categorized into four groups based on the circuit interruption requirements covered by the integrated ESF/LOOP test.

First, there is a set of circuit breakers that are always connected to the bus, these are termed Group 1 breakers. These breakers are always closed and remain closed on a loss of off-site power. In general these breakers have no protective features that might have the potential to open the breakers following a loss of off-site power because they remain closed on a loss of off-site power. For a number of plants, the integrated ESF/LOOP test confirms that these breakers remain closed. These provide power to small standby loads which, in general, are turned on and off by other controls in the circuit (i.e., a MOV which is controlled by a position switch or control logic used to open or close the valve). The primary safety function of this type of breaker is to remain closed/maintain continuity. In a typical PRA, these breakers are either subsumed within the component to which they provide power (i.e., a MOV) or the model includes a basic event representing "transfer open" of the breaker. Typically, the components to which these breakers provide power are covered by tests that are more frequent than once per refueling cycle. A standby failure of one of these breakers would be immediately obvious during any test of the powered component, so the performance of these breakers is effectively covered by the tests of the powered components. Therefore, this type of breaker was classified as a Category B component, a component for which one or more failure modes are tested only during the integrated ESF/LOOP test but for which there are sufficient bases to justify no additional modeling or changes to the component unavailability.

The second set of safety-related breakers provides power to large standby safety-related rotating loads such as the HPSI or LPSI pumps; these are termed Group 2 breakers. These breakers close to the bus to start and run the loads and are opened to stop the loads. The loads are normally in standby with breakers open and they will receive a close signal from the appropriate ESFAS. They will also receive an open signal on loss of off-site power via an undervoltage relay. (Note: Some breakers automatically trip free when the bus to which they are connected becomes de-energized. Such breakers do not have undervoltage relays as such.) Normally, a PRA will directly model failure of these breakers to close to start the pumps although occasionally they will be subsumed into the related element for failure of the pump to start. Both the "open" and "close" function of the breaker is tested each time the associated pump is tested. However, operation of the undervoltage relay appears not to be tested by any test other than the integrated engineered safety features test. (Note: The "trip free" on loss of power capability of breakers without undervoltage relays is also not covered by any other test.) Failure of the undervoltage relay to open the breaker (or failure of the breaker to open) would only be of concern given a loss of off-site power if the associated equipment was running. In this case, the load would then still be connected to the bus when the EDG starts to pickup the bus. The safety-related loads are typically loaded in blocks with all equipment in a given block loaded simultaneously. The first load block contains the most important equipment; the second load block contains the next most important equipment and so on. The amount of equipment in a given load block is determined by total startup (or inrush) current of the equipment compared to the remaining load capability of the associated EDG given the loads already

connected to the EDG. The sum of the startup currents for the equipment in the first load Block is typically very close to the maximum capacity of the EDG because this equipment is needed for immediate response to design basis accidents. Therefore, if one of the breakers for equipment in the first load block were to fail to open on a loss of off-site power, the EDG would not trip on overload because the startup current for that piece of equipment would already be within the load capacity for the first load block. However, if one of the breakers for equipment in the second or subsequent load block were to fail to open on a loss of off-site power, the EDG may not have sufficient capacity to pickup that load in conjunction with the loads in the first load Block. In this case there is a potential that the EDG would trip on overload and would continue to trip on overload every time the loads were resequenced onto the bus. This would be modeled as failure of the EDG. The potential for failure of the EDG due to excess load is a function of several factors. The first factor is the number of loads in the second and subsequent load blocks that would exceed any EDG load capacity remaining after the first load block is loaded. The second factor is the likelihood that the specific loads would be connected to the bus prior to a loss of off-site power. Many of the loads in the second and subsequent load "Blocks" are standby loads that are not typically energized (connected to the bus). If the loads are not energized prior to the loss of off-site power, the breaker will be in the open position and can not "fail to open" following the loss of off-site power. The potential for failure of the EDG due to excess load associated with a standby load is directly proportional to the fraction of time that the load may be energized during normal operation and the probability of failure of the breaker or its associated load shed device.

The third factor is to determine what loads would be required for a given challenge. The load groups are established based on the loads required for the worst case design basis accident (i.e., a large break LOCA). However, the more likely challenges such as a loss of feedwater do not require all of the equipment in the first load block". Thus, for many challenges coupled with a loss of off-site power, all loads in the first load block would be shed, but not all of the loads would be reconnected to the bus and draw current. This would increase the EDG load margin available to handle load shed failures for loads in the second and subsequent load "blocks".

Most PRAs do not model failure of the EDG due to excess load associated with failing to shed safety-related breakers. A complete treatment of the Group 2 breakers would add significant complexity to the models. A simplified and conservative approach would be to model failure of a EDG due to excess load for each safety-related breaker in the second and subsequent load blocks. Should this prove to have a large impact on CDF and ΔCDF, a more complete model can be developed to eliminate conservatism associated with the issues discussed above. Note also that for some plants, the EDG generator output breaker is interlocked such that failure to shed any of the loads on the safety bus would prevent closing the EDG generator output breaker on to the safety-related bus. For these cases, only failure of the EDG generator output breaker needs to be modeled to address failure to shed the loads.

A third set of safety-related breakers provide power to normally operating loads that are turned on and off by closing or opening the associated breaker; these are termed Group 3 breakers. These loads may be continuously operating or they may be operated cyclically in conjunction with redundant/parallel components. The breakers for these components will typically receive a confirmatory close signal on the appropriate engineered safety features actuation signal. They will also receive an open signal on loss of off-site power via an undervoltage relay. Some breakers automatically trip free when the bus to which they are connected becomes de-energized; such breakers do not have undervoltage relays. Normally, a PRA will directly model a "transfer open" failure of these breakers and a failure to close to start the standby pump. Occasionally these failure modes will be subsumed into the related elements for failure of the pump to run or to start. Both the "open" and "close" function of the breaker is tested each time the associated pump is tested. However, operation of the undervoltage relay appears not to be tested by any test other than the integrated ESF/LOOP test. (Note: The "trip free" on loss of power capability of breakers without undervoltage relays is also not covered by any other test.) Failure of the undervoltage relay to open the breaker (or failure of the breaker to open) would only be of concern given a loss of off-

site power if the associated equipment was running. Group 3 breakers should be treated like the Group 2 breakers discussed above because they are equivalent, except that they will be connected to the bus a larger fraction of the time than the Group 2 breakers.

The fourth set of safety-related breakers is those that provide power to safety-related loads that are not immediately required to mitigate an initiating event; these are termed Group 4 breakers. While the breakers may be equivalent to a Group 2 or Group 3 breaker, the key feature of these breakers is that they have an associated permissive signal. These loads will be shed on a loss of off-site power. On restoration of power to the associated safety-related bus, a timeout relay will be energized. When the timeout relay times out, a permissive contact will permit manual re-energization of the load. If the breaker were equivalent to a Group 2 or Group 3 breaker where the loss of off-site power results in opening of the breaker if it is closed, the associated load will not be on the bus when it is re-energized unless there is also a failure of the permissive and a human action to connect the load to the bus. If the load were required, failure of the permissive should be modeled as a way of losing power to the load. However, failures leading to extra loads on the bus that might result in EDG failure need not be modeled because of the low probability for the scenario due to the number of independent failures involved.

4.5.3 Non-Safety Related Breakers

The initial evaluation of equipment tested by the integrated ESF/LOOP test showed that many plants power some non-safety related loads from the safety buses. On a loss of off-site power, these loads are shed from the safety-related buses. The integrated ESF/LOOP test verifies that these non-safety related loads are shed on a loss of off-site power. In some cases the load shed occurs on an undervoltage signal, in other cases the breakers automatically trip free when the bus to which they are connected becomes de-energized. The integrated ESF/LOOP test is the only test that confirms this function. Other plants are configured such that the non-safety related loads are powered from non-safety related buses which are connected to the associated safety-related buses via tie breakers. Upon a loss of off-site power, the tie breakers open to separate the non-safety related loads from the safety-related buses.

Because the loads are not safety-related and not risk significant, they are not included in the plant PRA models and, consequentially, neither are the breakers. The primary concern with these breakers is that if they are not shed from the safety-related buses upon loss of off-site power, the EDG may not have sufficient capacity to pick up any additional loads from the non-safety related loads in conjunction with the safety-related loads in the first load block. In this case, there is a potential that the EDG would trip on overload and would continue to trip on overload every time the loads were resequenced on to the bus. This would be modeled as failure of the EDG.

As discussed above for the Group 2 safety-related breakers, the potential for failure of the EDG due to overload as a result of failure of the non-safety related loads to shed is a function of several factors. Addressing all of the pertinent factors would add significant complexity to the model. A simplified and conservative approach would be to model failure of a EDG due to excess load if any of the non-safety related loads fails to shed. Should this prove to have a large impact on CDF and ΔCDF, a more complete model can be developed to eliminate conservatism associated with the issues discussed above. Note also that for some plants, the non-safety related loads and safety-related loads are on separated buses with a tie breaker between the safety-related and non-safety related buses. Upon a loss of off-site power, the non-safety related loads are shed by opening the tie breaker. For this type of configuration, only the tie breaker needs to be modeled.

For plants that do not segregate safety-related and non-safety related loads, not all of the non-safety related loads would be continuously energized. If the non-safety related load is not operating at the time of a loss of off-site power, the load breaker would not be connected to the bus and thus would not have to be shed. Likewise, small non-safety related loads like valves would only place a load on the bus when the valve is changing position. Even if the load shed breakers for this type of load fail to open, it is unlikely that the valves will be changing position following a loss of off-site power, so they would not place a load on the bus. When setting up the model to reflect failure of the EDG generator due to failure to shed non-safety related loads, the small, short duration loads such as valves can be disregarded. For the loads that are not continuously energized, failure of the breaker to open and shed the load should be modified to address the fraction of time that the load would actually be energized.

5.0 DEFENSE-IN-DEPTH AND SAFETY HAZARD EVALUATION

In 1995, the U.S. Nuclear Regulatory Commission issued a Policy Statement endorsing the use of probabilistic risk analysis in all regulatory matters. That Policy states that the use of PRA technology should be increased to the extent supported by the state-of-the-art in PRA methods and data, and in a manner that complements the NRC's deterministic approach.

With the subsequent issuance of risk-informed regulatory guidance, the NRC has cautiously but conclusively transitioned from a deterministic-based regulatory methodology with its dependence on qualitative engineering judgment to a risk-informed methodology when evaluating the impact of plant operation on the health and safety of the public. Paramount among the risk-informed guidance issued by the staff is RG 1.174 since it forms the basis for increased use of PRA technology when used in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy. The transition to a risk-based regulatory environment has been further emphasized by the issuance of RG 1.200 that is intended to reflect and endorse guidance provided by standards-setting and nuclear industry organizations along with describing an acceptable approach for determining the technical adequacy of results obtained from probabilistic risk assessments.

Consistent with RG 1.174, the philosophy of defense-in-depth is maintained when a reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation; system redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties; defense against potential common cause failure is preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. Further, avoiding over-reliance on programmatic activities to compensate for weaknesses in plant design, ensuring the independence of barriers is not degraded, and preserving the defenses against human errors helps maintain the intent of the General Design Criteria in Appendix A to 10 CFR Part 50.

5.1 DETERMINISTIC ASSESSMENT

The fundamental principles of event prevention, detection and mitigation remain the pillars of nuclear plant safety. Supporting these pillars are the design philosophies of defense-in-depth, safety margin, redundancy and diversity. Each of these deterministic design basis philosophies is considered and shown to be accommodated when implementing a staggered integrated ESF/LOOP testing program and thereby comply fully with the staff's regulatory requirements.

A deterministic analysis is needed to reinforce the conclusions of the corresponding risk-informed analysis performed to support the change in testing interval and to provide the necessary balance between risk and deterministic arguments required by RG 1.174. Each defense-in-depth analysis consists of two parts; a Failure Modes and Effects Analysis (FMEA) and a Significant Hazards Analysis of systems and equipment that is tested solely by the integrated ESF/LOOP tests.

5.2 SURVEILLANCE TESTING

Extensive surveillance activities including calibration and operability tests are performed in the course of a fuel cycle or during a refueling outage, with the ESF initiation system and portions of the actuation system functionally tested at intervals that typically vary from [92] days to [18] months. In addition,

safety related equipment is included in plant specific maintenance programs designed to identify and eliminate the impact of time dependent failure modes.

These surveillance tests are independent of the integrated ESF/LOOP tests, thus further analysis of the ESF initiation system is not required since it is not affected by a change in the integrated ESF/LOOP test interval. Surveillance tests also assure that a change in ESF train unavailability will be identified, should such occur as a result of adopting a staggered test interval.

5.2.1 Emergency Diesel Generator Surveillance Testing

The focus of this deterministic analysis is Emergency Diesel Generator (EDG) surveillance tests. Many of the required refueling interval EDG surveillance tests are performed in conjunction with integrated ESF/LOOP testing in order to minimize equipment degradation due to testing. The extent of this integration and coordination is plant specific and dependent on EDG designs.

Review of the EDG electrical surveillance requirements as described in the Standard Technical Specifications (NUREG-1432) and the demonstration plant integrated ESF/LOOP test procedures indicates that all or part of the following surveillance tests are typically performed in conjunction with the integrated ESF/LOOP testing.

SR 3.8.1.9 verifies the operability of EDG Voltage Regulator (VR) and governor.

SR 3.8.1.10 verifies the operability of EDG VR and governor to maintain EDG speed.

SR 3.8.1.11 verifies operability of Under Voltage Relays (UVR) 27 with auxiliary relays, safeguard bus breaker trip circuits, EDG start control circuits, EDG breaker, EDG voltage regulator, EDG excitation and field circuits, EDG governor, EDG load sequencer and slave relays.

SR 3.8.1.12 same as SR 3.8.1.11 plus the SIAS actuation relays.

SR 3.8.1.13 verifies automatic EDG trips are bypassed on ESF bus UV with or without a SIAS. It also tests EDG breaker control circuits and UVR 27 with auxiliary relays.

SR 3.8.1.14 verifies the operability of EDG VR, EDG governor and EDG fuel transfer system. It also verifies all other electrical and mechanical EDG components are capable of continuous high load operation.

SR 3.8.1.15 verifies operability of, EDG breaker control circuits, safety injection actuation signal presence at EDG breaker control circuits following a hot restart.

SR 3.8.1.16 verifies operation of EDG synchronization check relays, voltage regulator and governor.

SR 3.8.1.17 verifies test mode override in the presence of a safety injection actuation signal at the EDG control circuits and response of emergency loads.

SR 3.8.1.18 verifies the time intervals of the safety injection and shutdown load sequencers.

5.2.2 Major EDG Components with Specific Testing Requirements

Various surveillance tests validate the operability of key EDG related systems and components. These components and their testing requirements include:

- UVR 27 and auxiliary relays,
- Safeguard buses feeder circuit breakers,
- EDG control circuits,

- EDG load sequencer and load feeder breakers,
- SI and shutdown sequencers,
- ESFAS subgroup relays,
- EDG voltage regulator, EDG governor, EDG exciter,
- EDG synchronization relays.

UVR 27 relays are functionally tested every 92 days per SR 3.3.6.2, and are calibrated and functionally tested every 18 months per SR 3.3.6.3. The testing intervals for UVR 27 and the auxiliary relays will not change with the change in the integrated ESF/LOOP test interval. Therefore, extending the integrated ESF/LOOP test interval will not affect the reliability of the UVR 27 and auxiliary relays.

Safeguard bus and feeder circuit breakers (other than the EDG output breakers) are activated by the UVR 27 relays and automatic load sequencer. These circuits are functionally tested and calibrated in accordance with their respective requirements under TS 3.3.5 and 3.3.6. Breakers are also maintained in accordance with vendor recommendations and plant procedures to ensure reliability. These test and maintenance intervals are not affected by extending the ESF/LOOP test interval.

EDG control circuits are functionally tested each month per SRs 3.8.1.2 and 3.8.1.3 through manual start/stop of the EDG using a local or remote test switch. The circuits are provided with permissive contacts from UVR 27 and safety injection actuation signals to start EDG from both or either signal and to selectively bypass EDG protective circuits as warranted. Therefore, all portions of the control circuit, with the exception of the UVR 27 and SIAS contacts (tested separately) and contacts for bypassing automatic trips are tested every month and are not affected by extending the test interval for the integrated ESF/LOOP test.

EDG breakers are functionally tested during the monthly surveillance test (SR 3.8.1.3). The breaker control circuit is provided with permissive contacts from UVR 27 and ESFAS signals to ensure that the circuits will close/open the breaker when required. ESFAS signal initiation and UVR 27 are calibrated and functionally tested each refueling interval (18 months). Breaker maintenance is performed in accordance with vendor recommendations and plant procedures.

EDG safety injection and shutdown load sequencers are calibrated and functionally tested every 18 months per SR 3.8.1.18. This calibration and test frequency is not affected by a change in the integrated ESF/LOOP test frequency. The ability to functionally test load sequencers during normal operation varies from plant to plant but most designs permit thorough functional testing of all components excluding final output relays. In order to include sequencer calibration in the staggered integrated ESF/LOOP test scheme, utilities would be required to show that there are no sequencer components subject to time-dependent failures or eliminate the time dependent failure mode and include the failure mode in the plant risk model. Assuming the sequencer timers are calibrated and functionally tested every refueling outage by SR 3.8.1.18, independent of the integrated ESF/LOOP test, extending the integrated ESF/LOOP test interval for other refueling interval surveillance requirements has no affect on sequencer operability nor does it change its unavailability.

ESFAS subgroup relays are functionally tested every 92 days by SR 3.3.5.1. Subgroup relay operability is verified every 184 days by SR 3.3.6.2. Manual trip channels are functionally tested every refueling outage by SRs 3.3.6.1 and 3.3.6.2. Channel calibration, performed every 18 months, includes associated relays if they require calibration. ESFAS response time is verified according to the SR 3.3.5.4. Therefore, the operability and proper functioning of these relays is verified by surveillance requirements other than the integrated ESF/LOOP test. Any failure of these relays discovered during the integrated

ESF/LOOP test would be considered a random failure. Extending the integrated ESF/LOOP surveillance test interval is not expected to increase the failure probability of these relays.

This review found that EDG components discussed above are not affected adversely by an extension of the integrated ESF/LOOP test interval. This results since component functions are verified by other required technical specification surveillances that are independent of the integrated ESF/LOOP testing.

5.2.2.1 EDG Components Tested by Comprehensive EDG testing

Functional testing of the EDG voltage regulator and exciter, governor, breaker synchronization check relays and fuel transfer system is verified during comprehensive surveillance tests. Required testing of these EDG components and functions, as shown in Table 5.2-1, may be combined with the integrated ESF/LOOP test.

Table 5.2-1
EDG Surveillance Testing
Correlation of Test Performed with Component/Function Tested

Type of Test	Component/Function tested
Start and stop test	SI signal, UVR signals, Governor
Load test in parallel mode	Voltage regulator, governor
LOOP test	Voltage regulator, governor
SI actuation signal test	SI signal
LOOP with SIAS test	Voltage regulator, governor, SI signal
Single load rejection test	Voltage regulator, governor
Endurance test	All EDG systems
Synchronization test	Governor, synchronous check relay
Hot restart test	Governor

5.2.2.2 EDG Voltage Regulator and Exciter

Voltage regulators maintain a constant generator output voltage and control the reactive volt-amperes output from the generator when it is tested in parallel with the grid. The excitation system controls generator output voltage by regulating the amount of current delivered to the generator field. The voltage regulator senses generator output voltage and compares a rectified sample of that voltage to a reference voltage; differences result in generation of an error signal. This error signal is amplified by a differential amplifier to control how early or late the silicon controlled rectifiers are fired. EDG excitation and regulation circuits may vary depending on the specific design, but the basic operation of the voltage regulator is the same for all designs.

Monthly tests are performed with the EDG operating in parallel with off-site power. EDG endurance testing in the emergency mode is performed with a simulated LOOP. Although the voltage regulator is challenged differently depending on the mode of operation, the governor functions are basically the same in either mode. Each test challenges the voltage regulator in different ways; some by verifying the time it takes an EDG to reach the rated voltage, others by verifying stability, and some by verifying that the voltage regulator can respond to a load change.

Voltage regulator response is different when the EDG is operating in parallel with the off-site power than when operating under LOOP conditions. The voltage regulator maintains a constant generator terminal voltage for emergency operation while controlling the generator volt-amp reactive output when it is

operating in parallel with off-site power. Operation of the voltage regulator along with the governor is more dynamic when EDG is in the LOOP mode of operation. Voltage regulator operation during the EDG startup is about the same under both modes of operation. However, when loading the EDG according to sequenced timing, the operation of the voltage regulator becomes critical. It must ensure that voltage will recover quickly and remain constant by using voltage feedback circuits to generate the error signals and subsequently increase the silicon controlled rectifier rate of firing and increase excitation field current. The time required to detect the voltage feed back to increase the excitation currents is critical to ensure that EDG voltage will remain within the operating limits. During EDG monthly test, the EDG is paralleled with the off-site power and loads are added individually. Voltage is set according to the operating procedure and the volt-amp reactive is maintained by the voltage regulator. The circuit that maintains the volt-amp reactive is part of the circuit that must monitor the EDG output voltage, current, and power factor to ensure proper EDG output. If the voltage regulator can maintain and respond to the grid volt-amp reactive requirements, then it can respond to the change in voltage.

EDG endurance testing will not identify a weakness or degradation in the voltage regulator when EDG output is increased from 100% to 110% for two hours (SR 3.8.1.14) during the monthly surveillance test. The voltage regulator will either fail completely or result in an output voltage swing that provides an unsteady volt-amp reactive output. There are no components within the voltage regulator circuits that are tested only when EDG output power is increased to either 100 or 110% of the rated value.

The most common symptom of a voltage regulator problem is variation in voltage or cycling of the reactive volt-amp output. EDG voltage regulator problems may become evident through:

1. Collapse of the EDG output voltage after field flashing due to a blown potential transformer fuse or an open circuit voltage regulator potentiometer resulting in no firing pulses being applied to the silicon controlled rectifier firing circuits, or
2. Voltage high and uncontrollable at the voltage regulator circuits as a result of:
    - Low or no voltage from the voltage sensing circuits,
    - Voltage adjusting pot is shorted or misadjusted prior to EDG start,
    - Faulty K type relays, or
    - Shorted silicon control rectifier.

None of the above voltage regulator failures can be attributed to a failure that is time dependent. Random component failure and human error are the most common contributors to a voltage regulator failure or malfunction. Voltage regulator circuits are de-energized while the EDG is in a standby condition, thus these circuits are, in general, not susceptible to failure. However, circuits are sensitive to the stresses caused by the number of start and stops imposed by testing.

5.2.2.3 EDG Governor

Governor performance is defined by its ability to minimize bus frequency transients during the required loading sequences. The governor has the ability to maintain stable frequency under a variety of conditions. Typical causes of governor failure could be summarized as follows:

- Contaminated lubricating oil,
- Binding of fuel rack and other governor linkages,
- Lack of proper maintenance on the governor internal parts resulting in servomechanism wear, buildup of dirt or formation of rust.

The above failure mechanisms would normally be detected during routine monthly tests. The governor control circuits operate in different modes during routine and LOOP testing. During routine tests when the generator is operating parallel to off-site power, the governor operates in the droop mode to maintain stable power output. During LOOP testing, the governor operates in the isochronous mode to maintain constant frequency. Time response is important as step loads are applied. Governor time response problems are generally a result of hydraulic or mechanical problems. Routine maintenance programs for the EDG governors are plant specific. There are no parts of the governor control circuits and hydraulic system that depend solely on the integrated ESF/LOOP test to verify functionality or prove operability.

5.2.2.4 EDG Fuel Transfer System

SR 3.8.1.6 verifies that the fuel oil transfer system operates automatically to transfer oil from storage tank to the day tank and the engine mounted tank. SR 3.8.1.4 verifies that each day tank and engine mounted tank contains the minimum required volume of diesel fuel. Proper operation of the fuel transfer system is verified each time the EDG is operated. The integrated ESF/LOOP test is not the sole test used to verify functionality or prove operability of the fuel transfer system.

5.2.2.5 EDG breaker synchronization check relays

The EDG must also synchronize with the off-site power source and transfer loads from the EDG back to the off-site power following off-site power restoration after a LOOP per SR 3.8.1.16. This requires the governor to change from the isochronous to the droop mode. There is no historical evidence that the components or circuits involved in this switch are subject to time-dependent failure.

SR 3.8.1.3 requires EDG synchronization with off-site power for one hour or more of operation. The synchronization relays are tested every time the EDG is synchronized with off-site power. SR 3.8.1.16, the transfer of emergency loads from the EDG back to off-site power, requires synchronization of off-site power with the EDG. The operation of the synchronization relay is essentially the same in both situations. Therefore, the integrated ESF/LOOP test, including SR 3.8.1.16, is not the sole test used to verify functionality or prove operability of the synchronization check relays.

5.3 ESFAS DEFENSE IN DEPTH ANALYSIS

An integrated test is performed on each ESF train to confirm that systems and equipment will perform their required function when initiated by a safety injection signal, with or without a LOOP, thereby maintaining the defense in depth philosophy. The objectives of a defense-in-depth evaluation are to show that there are no time-dependent failure modes and to support the conclusion of the risk-informed analysis that extending the surveillance interval for the integrated ESF and LOOP tests results in a negligible change in plant risk.

The defense-in-depth analysis for extending a technical specification surveillance test interval requires analysis of time-dependent failure modes. This is done by performing a FMEA on each component to identify:

- If the performed surveillance test covers all failure modes,
- If any of the identified failure modes are time dependent, meaning that the rate of change varies with time (i.e., heat exchanger fouling, time delay relay drift, etc.),
- If other plant activities, such as maintenance program or surveillance testing have identified a time dependent failure mechanism,

- If a preventive maintenance program has been established to assure that the components hazard rate remains constant,
- If the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact,
- If any aspect of implementing an increased surveillance interval would introduce a potential for common-cause failures.

A primary purpose of the plant maintenance program is to assure that time dependent failure modes are identified, the associated degradation is removed, and that the component is maintained to required standards. If any time-dependent failure mode is identified, the utility must implement a preventive maintenance program to remove the time-dependent mode and to assure that the component failure rate remains acceptable. Any identified time-dependent failure mode must also be included the plant risk model. The impact of the increased surveillance interval must also be monitored using performance measurement strategies.

5.3.1 Failure Modes and Effects Analysis

Utilities must perform plant-specific FMEAs to show that an increase in the integrated ESF/LOOP surveillance test interval does not degrade the performance of the ESF system and does not invalidate any assumptions in the plant licensing basis. The FMEA should also show that a staggered test interval does not adversely impact the required refueling test interval for types B and C containment penetrations currently covered by Appendix J testing requirements.

Each Categories A-1 through A-4 component that is tested solely by the integrated ESF/LOOP tests ultimately requires a plant-specific FMEA evaluation considering:

- Failure modes,
- Failure mechanisms (cause),
- Failure effects and consequences, and
- Safety significance and impact on margin of safety.

5.3.2 Significant Hazards Evaluation

A significant hazards evaluation is performed by analyzing the impact of the failure modes identified by the FMEA on the overall performance of an ESF train in response to an actuation signal and analyzing how the operation of the ESF train, that has not been tested during the refueling outage, will be impacted if a time dependent failure occurs. The significant hazards evaluation must consider the effect of the failure mode on ESF actuation, whether the effect of a failure on the ESFAS could create a significant increase in the probability or consequences of an accident previously evaluated, create the possibility of a new or different kind of accident from any accident previously evaluated, or if the failure could result in a significant reduction in a margin of safety.

The operability of the ESFAS instrumentation and interlocks must ensure that when a monitored parameter reaches its setpoint, an appropriate level of reliability of ESF instrumentation with sufficient redundancy is maintained to perform its intended function. The operability of the ESF system is required to provide the overall reliability, redundancy and diversity assumed available in the plant design for protection and mitigation of accident and transient conditions. For the above reasons, it is important that a safety evaluation be performed that considers each relevant failure mode against the possible impact on ESF system capability to perform its intended function. Also, the evaluation must confirm that at no time

is the defense-in-depth of the ESF system compromised and that it will function as described in the plant licensing bases.

5.3.3 Sample FMEA and Significant Hazards Analysis

Each utility pursuing a staggered integrated ESF/LOOP testing interval must identify and evaluate their plant-specific group of Category A components that are tested solely by the integrated ESF/LOOP test. After completing the FMEA, the identified failure mode(s) for each Category A component also requires a significant hazards evaluation to confirm there is no reduction in the plant safety margin.

The generic FMEA and Significant Hazards Analyses that follow illustrate the deterministic evaluation needed to support the plant specific risk analyses. This evaluation focuses on Technical Specification surveillance requirement 3.8.1.11 contained in NUREG-1432 which verifies operability of undervoltage relay 27 with auxiliary relays, safeguard bus breaker trip circuits, and the EDG start control circuit, breaker, voltage regulator, governor and load sequencer. For demonstration purposes, the following Category A components are assumed to be tested solely by the integrated ESF/LOOP test:

- Under voltage relay 27,
- ESFAS and subgroup actuation relays,
- EDG and load circuit breakers,
- Safety injection and EDG load sequencers,
- EDG control circuits.

5.3.3.1 Under Voltage Relay 27

- **Failure Modes and Effects Analysis**

Under Voltage Relays (UVR 27) are continuously energized and are, therefore, subject to accelerated coil insulation aging. The failure rate of UVR 27 may increase if service conditions result in an elevated coil temperature over an extended time period. In addition, some UVRs may experience degradation of coil wire insulation over time if they are continuously energized with a higher than rated voltage. These under voltage relays are typically located within the associated switchgear room/cabinet and are not exposed to a harsh environment. In general, the concern for relay failure due to accelerated coil insulation aging has been resolved by improvements in the plant maintenance programs and by controlling environmental conditions in areas where these relays are located. The FMEA for Under Voltage Relay 27 is summarized in Table 5.3-1.

Table 5.3-1
Under Voltage Relay 27
Failure Modes with Possible Impact on ESFAS

Failure Mode	Failure mechanism (cause of failure)	Failure effects	Consequences
Relay fails to drop out.	Relay pickup spring adjusted incorrectly (plant maintenance program inadequacy). Relay plunger binding due to insufficient spring force (inadequacy in plant maintenance program or inadequate control of operating environment).	UV logics are usually designed with one or two relays per phase. Two out of three relays must drop out to perform designed functions. Failure of one relay to drop out when required will not prevent the actuation of the UV logic if the relays on the other two phases drop out.	UV relays are calibrated and functionally tested according to the plant TS requirements independent of integrated ESF/LOOP test interval. Therefore extending the integrated ESF/LOOP test interval will not increase the hazard rate of this failure mode.
Relay contacts fused, or fail to make.	Contact surface tension (plant maintenance program inadequacy). Contact surface contamination (plant maintenance program inadequacy). Incorrect contact rating (incorrect component selection).	Insufficient tension between two contacts Contacts are normally open (deenergized). Therefore, contact fusing is very unlikely. Contacts close after the relay drops out following a loss of power.	Same as above.
Relay coil fails short or open (coil wire insulation failure; a random failure that will not change with time).	Either is as a result of random failure due to the insulation wire failure, or age related to continuous operation.	If relay is energized, it will drop out; if not energized, it will fail to pickup when needed. (Extreme design condition that a secondary UVR will be energized with the first line primary UVR).	UV relays are calibrated and functionally tested according to the plant TS requirements independent of integrated ESF/LOOP test interval. UV relay failures have no impact on the risk increase resulting from the change in the integrated ESF / LOOP test interval since UV relay failure modes are not time dependent. Failure functional consequence is same as above. This failure mode has no safety significance since it will be detected and alarmed in the control room during the plant operation.

- **Significant Hazards Evaluation**

Technical specifications require the UVR 27 and associated relays to be calibrated and functionally tested each refueling outage, independent of the integrated ESF/LOOP test. Operation of the UVR27 is also channel checked daily and functionally tested every 92 days. Safety bus arrangements typically incorporate either one UVR27 relay per phase or one relay between two phases.

The FMEA shown in Table 5.3-1 identified three potential failure modes; failure to drop out, relay contact failure, and coil failure, for the UVR 27 relay. Data provided by utilities for the purpose of this analysis confirmed that the dominant failure mode for UVR 27 relays has been a random failure with a constant hazard rate. Also, a few UVR 27 failures were related to human error or inadequate maintenance which could indicate a possible common cause failure mode. However, common cause issues were addressed by a plant specific UVR calibration program which calibrates and functionally tests each UVR 27 relay during the outage.

Implementing a staggered integrated ESF/LOOP test interval has no effect on either the configuration of the plant or the manner in which it is operated. Loss of one or a set of UVR27 relays on the safety bus does not create the possibility of a new or different accident from any accident previously evaluated nor does it involve a significant increase in the probability or consequences of an accident previously evaluated since failure of one under voltage relay at the safety bus does not prevent EDG start.

The functional test interval for UVR 27 will not change with an increase in the integrated ESF/LOOP test interval thereby assuring that the margin to safety is not significantly different from the original. Therefore, implementation of staggered integrated ESF/LOOP test interval for UVR 27 relays does not involve a significant reduction in a margin of safety.

5.3.3.2 ESFAS Actuation/Subgroup Relays

- **Failure Modes and Effects Analysis**

Engineered safety feature actuation systems, either relay-based or solid state, employ subgroup relays to actuate ESF related system and equipment. The subgroup relays actuate timers which generate time-sequenced start signals to load ESF pumps and other loads onto its assigned power distribution buses. Typically, subgroup relays actuate other interposing relays that initiate startup of the required equipment.

ESFAS actuation/subgroup relays are customarily located within a mild environment and are normally deenergized, thus these relays are not susceptible to thermal aging. While most relay designs do not require routine maintenance, operability is assured through functional testing, i.e., pickup and dropout tests, of ESFAS actuation/subgroup relays that are performed every 92 days with channel operational testing performed every 184 days. ESFAS actuation/subgroup relays are tested with a plant protection signal only during the integrated ESF/LOOP test. The FMEA for ESFAS/subgroup relays is summarized in Table 5.3-2.

Table 5.3-2
ESFAS / Subgroup Relays
Failure Modes with Possible Impact on ESFAS

Failure Mode	Failure Mechanism (cause of failure)	Failure Effect	Consequences
Coil failure (short or open)	Manufacturing defect (random failure) Coil insulation/wire breakdown (only if normally energized). ESF actuation relays are normally deenergized.	Relay fails to energize. (If normally energized, fails open.)	Functions are not performed. Functions status change, can cause spurious operation. Delay in ESFAS actuation. No ESF actuation. Random failure modes. Hazard rate will not change with increase in integrated ESF/LOOP test interval.
Contact fused	Contact surface tension (plant maintenance program inadequacy) Contact surface contamination (plant maintenance program inadequacy) Incorrect contact rating (incorrect component selection)	Insufficient tension between two contacts Contacts are normally de-energized therefore, contact fusing is very unlikely.	Same as above.
Mechanical binding or failure	Maladjustment, manufacturing defects mechanical cycling	Fails to perform its intended function	Same as above.

- **Significant Hazards Evaluation**

The safety significance of ESFAS actuation/subgroup relay failure on one train of ESF system and equipment operability is dependent on the plant-specific ESF system design. Actuation relays are normally deenergized and are energized on receipt of an ESF actuation signal. The failure modes and effects analysis identified three potential failure modes, coil failure, fused relay contacts, or mechanical binding, applicable to the ESF actuation/subgroup relays.

Based on a review of the historical operating data, ESF actuation/subgroup relay failure modes, as noted in Table 5.3-2 , are not time dependent. The type of failures identified shows that the relay failure rate does not change with time since these relays operate in a de-energized, standby state. However, a random relay failure could impact the operation of a train of ESF equipment at any time regardless of the integrated ESF/LOOP test interval.

Implementing a staggered integrated ESF/LOOP test interval has no effect on either the configuration of the plant or the manner in which it is operated. Loss of one ESF actuation relay does not create the possibility of a new or different accident from any accident previously evaluated nor does it involve a significant increase in the probability or consequences of an accident previously evaluated since failure of one actuation relay does not prevent initiation of ESF systems.

The functional test interval for the ESF actuation/subgroup relays will not change with an increase in the integrated ESF/LOOP test interval testing thereby assuring that the margin to safety is not significantly different from the original. Therefore, since there are no failure modes associated with ESF actuation relays that will be affected by an increase in the duration of the integrated ESF/LOOP test interval, implementing a staggered test interval for the integrated ESF actuation/subgroup relays does not create a significant reduction in the plant's margin of safety and does not create a substantial safety hazard.

5.3.3.3 EDG and Load Circuit Breakers

- **Failure Modes and Effects Analysis**

The FEMA for the EDG and load circuit breakers is summarized in Table 5.3-3. The circuit breaker failure mode can be summarized as fail to open and fail to close on demand. Circuit breaker operation is controlled by sets of contactors within the breaker control circuit; these contactors receive command signals from associated relays. Failure to provide any of the command signals will interfere with proper operation of breaker. For example, an UVR27 signal is generated by degraded or low voltage on the bus and initiates a breaker opening signal to isolate the faulted section of the distribution system.

Breaker opening requires that the normal and alternate feeder breakers must open, the associated EDG must start, and the EDG output breaker must close in approximately 10 seconds after the EDG is ready to load. All of these actions are required to be tested according to the plant specific technical specification requirements.

If an EDG circuit breaker fails to close as a result of a breaker failure, that safety bus will not be energized and the associated ESF train will not be available. Conversely, the EDG Group 1 loading would increase if a loaded feeder breaker fails to open as the result of a breaker failure. The EDG response to a larger-than-design loading demand varies with the size of the electrical load placed on the EDG and the ability of the EDG to accommodate such load.

Table 5.3-3
EDG and Load Circuit Breakers
Failure Modes with Possible Impact on ESFAS

Failure Mode	Failure mechanism (cause of failure)	Failure effects	Consequences
Breaker fails to close.	Mechanical binding. Closing coil in failed state. No closing signal provided to the breaker closing circuit (failure of UVR contact in breaker control circuit). Failure of the SI or load sequencer to provide close signal to the breaker (failure of SI contact in breaker control circuit).	Load will not be powered. Safeguard bus will not be powered.	Could cause loss of one train of safeguard bus. Breaker failure to open or close is typically alarmed in the control room and operators have the means to close the breaker manually if necessary. PRA model includes the failure of breaker to close or to open to determine the risk impact on the plant (very minimal). Plant risk impact much smaller than impact of breaker failing to close.
Breaker fails to open.	Mechanical binding. Opening coil in failed state. All of the above failures are as result of random failure that has no correlations with ESF test interval.	Unwanted loads will be energized. Possible overloading of the EDG.	Possible tripping of EDG due to overload and consequential loss of one ESF train. No time dependent failure modes. The failure modes have no correlation with ESF test interval. Therefore extending the integrated ESF/LOOP test interval will not increase the hazard rate of this failure mode.

- **Significant Hazards Evaluation**

The following hazards evaluation of the safeguard switchgear breakers, including EDG breakers, illustrates the impact of breaker failure on one train of ESF system and equipment operability. Each utility must perform a plant specific hazards evaluation based on the breaker type and manufacturer used at their facility.

The failure modes for a circuit breaker are a failure to open and to close as required. Safety related circuit breakers require periodic testing to verify proper operation. Most safety related loads such as pumps, chillers and unit coolers require in-service functional testing which is typically performed during normal plant operation. This testing requires cycling the component circuit breaker. Failure of a breaker is not time dependent since they are tested during normal operations at intervals less than the refueling cycle. However, some plant designs incorporate normally closed switchgear feeder breakers that power safeguard buses. Such safeguard buses are powered directly from a dedicated off-site power source through breakers that are not cycled (opened) during routine plant operation. In this case, the breaker trip function can only be tested during a refueling outage by the integrated ESF/LOOP test.

The safety significance of a specific breaker failure is dependent on the specific plant design, breaker safety function, and type of load that receives power through the breaker. Failure of an EDG output breaker could cause loss of one train of engineered safety features equipment if the operator fails, or is unable, to close the breaker manually. Implementing a staggered integrated ESF/LOOP test interval has no effect on either the configuration of the plant or the manner in which it is operated since loss of one train of EDG and ESFAS is an analyzed design basis event.

Risk models show that a loss of one train of EDG and ESFAS will reduce the margin of safety. However, these types of failures are random and can occur under any postulated scenario, and are not related to the integrated ESF/LOOP test interval. Loss of one EDG and ESFAS load circuit breaker does not create the possibility of a new or different accident from any accident previously evaluated. Further, such loss does not involve a significant increase in the probability or consequences of an accident previously evaluated since failure of one circuit breaker does not prevent actuation of the opposite ESF train

The impact on EDG loading caused by failure of a feeder circuit breaker to open on demand will depend on the additional load imposed on the EDG. The single largest load normally imposed on an EDG is typically that of a service water pump. Failure of a service water pump breaker to open on demand could cause an EDG to trip on overload when such pump load is combined with normal operating loads. This type of breaker failure is independent and not a function of the integrated ESF/LOOP test interval since it could occur under other plant accident scenarios. The consequence of a failure to load shed and loading the EDG with additional loads could trip EDG and cause a loss of one ESF train. This scenario is an analyzed plant scenario and is independent of the integrated ESF/LOOP test interval.

The functional test interval for the EDG and load circuit breakers will not change with an increase in the integrated ESF/LOOP test interval testing thereby assuring that the margin to safety is not significantly different from the original. Therefore, since there are no failure modes associated with the EDG and load circuit breakers that will be affected by an increase in the duration of the integrated ESF/LOOP test interval, implementing a staggered test interval for the integrated EDG and load circuit breakers does not create a significant reduction in the plant's margin of safety and does not create a substantial safety hazard.

5.3.3.4 Safety Injection and EDG Load Sequencers

- **Failure Modes and Effects Analysis**

The purpose of the safety injection and EDG load sequencers is to energize ESF components according to preset timing sequences to ensure that motor inrush currents do not overwhelm diesel generator operation. Load sequencers are calibrated and functionally tested during each refueling outage with sequencer operation verified every 31 days. Testing each refueling outage also verifies automatic lockout actuation for these sequencers.

The increase in the integrated ESF/LOOP test interval from every outage to every other outage will have no affect on the availability of sequencers. The calibration and functional testing of the individual sequencers remain unchanged and is performed each refueling interval. A sequencer component failure would be considered a random failure, since the interval between the calibration and functional testing remains unchanged.

The FEMA shown in Table 5.3-4 has identified three potential sequencer failure modes that should be considered; these are failure of the sequencer to energize, failure to energize at the correct time, and insufficient sequencer output. These failure modes are independent of the integrated ESF/LOOP test

interval since the sequencer functionality test and calibration are performed independent of the integrated ESF/LOOP test interval. Sequencer failure or delay in the sequencer operation would be detected and corrected within the sequencer surveillance and calibration interval (one refueling cycle), and not by the integrated ESF/LOOP test.

Table 5.3-4
Safety Injection and EDG Load Sequencer
Failure Modes with Possible Impact on ESFAS

Failure Mode	Failure Mechanism (cause of failure)	Failure Effect	Consequences
Sequencer fails to energize.	Either solid state circuits or electro mechanical relay failure (random failure).	Sequencer fails to initiate loading of the required group two loads.	One train ESF fails to energize associated components.
Sequencer energizes but not at the correct interval.	Timing relays at fault.	EDG may be loaded outside of sequencing order.	May cause energized loads to dropout, caused by EDG lump sum loading. Larger than expected voltage drop.
Sequencer output is not sufficient.	Some relays may failed to energize (random failure).	Partial loading failure.	Some of the components may fail to energize, causing a partial ESF train failure.

- **Significant Hazards Analysis**

Failure of a sequencer to initiate loading of one train of ESF system/equipment or failure to energize loads at the correct interval is an analyzed event since it could occur at any time and is independent of the integrated ESF/LOOP test interval. The same is true for the situation where a sequencer may have insufficient output and failure of an output relay results in partial loading of ESF equipment. These potential failure modes are not time dependent since sequencers are functionally tested every 31 days, with calibration and functionally testing performed every refueling interval. Each utility must confirm that a sequencer failure does not create a substantial safety hazard by performing an evaluation based on the specific sequencer design at their facility.

An increase in the integrated ESF/LOOP test interval from every outage on a sequential basis to every other outage on a staggered basis will have no affect on the availability of sequencers. The calibration and functional testing of the individual sequencers remain unchanged and is performed each refueling interval. A sequencer component failure would be considered a random failure, since the interval between the calibration and functional testing remains unchanged.

Risk models show that a loss of one EDG train would reduce the margin of safety. However, sequencer failures are random and can occur under any postulated scenario since such failure is not related to the integrated ESF/LOOP test interval. Loss of one safety injection or EDG load sequencer does not create the possibility of a new or different accident from any accident previously evaluated. Further, loss of a sequencer does not involve a significant increase in the probability or consequences of an accident previously evaluated since failure of one sequencer does not prevent actuation of the opposite ESF train.

The functional test interval for the safety injection and EDG load sequencers will not change with an increase in the integrated ESF/LOOP test interval testing thereby assuring that the margin to safety is not

significantly different from the original. Therefore, since there are no failure modes associated with the safety injection and EDG load sequencers that will be adversely affected by an increase in the duration of the integrated ESF/LOOP test interval, implementing a staggered test interval for the safety injection and EDG load sequencers does not create a significant reduction in the plant's margin of safety and does not create a substantial safety hazard.

5.3.3.5 EDG Control Circuits

- **Failure Modes and Effects Analysis**

Monthly surveillance testing of a diesel generator involves three control circuit functions; EDG start/stop using manual control, EDG start from a safety injection signal with or without off-site power, and EDG start from an undervoltage signal with or without a safety injection signal. Operation of the EDG start control circuit function is not affected by adopting a staggered integrated ESF/LOOP test interval since functional testing intervals for UVR27 circuits, safety injection signal initiation, and EDG start/stop control circuits will remain unchanged. Implementing a staggered integrated ESF/LOOP test interval has no effect on either the configuration of the plant or the manner in which it is operated since loss of one EDG train is an analyzed design basis event.

Initiation of the safety injection signal is verified every 92 days according to the plant technical specification requirements. Channel operational tests are performed every 184 days. Manual actuation of the logic circuits is verified during surveillance activities each refueling outage.

The consequence of a failure in the EDG starting control circuit includes failure to start, failure to reach the required Revolution per Minute (RPM), or failure of the generator field to flash. The most common EDG failures are fail to start and fail to field flash as summarized in the FMEA provided in Table 5.3-5. Field flashing circuits are incorporated into the generator design and are not affected by the EDG control circuit. The same control circuit is used when starting the EDG with undervoltage or safety injection initiation signals during the integrated ESF/LOOP test. Therefore, failure of the EDG control circuit is unrelated to and independent of the integrated ESF/LOOP test interval.

Table 5.3-5
EDG Control Circuit
Failure Modes with Possible Impact on ESFAS

Failure Mode	Failure Mechanism (cause of failure)	Failure Effect	Consequences
Control circuits fail to energize air start solenoid valves.	Solenoid failure, air start system failures random.	EDG fails to start.	Loss of one train of EDG. Operator will actuate manual EDG air start valves once the EDG malfunction is diagnosed.
Control circuits fail to flash field.	DC power system failure, failed field flash circuit, EDG failed to reach appropriate RPM (speed contacts failure).	EDG fails to achieve its rated RPM or voltage and will trip.	Loss of one train of EDG.

- **Significant Hazards Analysis**

EDG control circuit designs vary according to the manufacturer and plant specific application. Control circuits are tested monthly when the EDG is manually started. Any single failure within the control circuits that could prevent EDG start and loading is an analyzed scenario. Such failures would be due to a random failure within the control circuits, other component failures or improper maintenance activities.

Evaluation of typical EDG control circuits indicates that there are no specific components or circuits that are only tested during an integrated ESF/LOOP test. The only circuit that is tested during the integrated ESF/LOOP test is deactivating the shutdown emergency start circuit which is bypassed when the safety injection signal is present. Testing this function is performed by using a number of K type relays. Utilities are required to show how their surveillance program verifies the operability of these relays since relay types vary from one plant to other. There is no historical evidence that components associated with bypassing automatic trips are subject to any time-dependent failures.

Risk models show that loss of one EDG train will reduce the margin of safety. However, failure of an EDG is random, can occur under any postulated scenario, and is not related to the integrated ESF/LOOP test interval. Loss of one EDG does not create the possibility of a new or different accident from any accident previously evaluated. Further, such loss does not involve a significant increase in the probability or consequences of an accident previously evaluated since failure of one EDG does not prevent actuation of the opposite ESF train.

EDG functional testing will not change with an increase in the integrated ESF/LOOP test interval thereby assuring that the margin to safety is not significantly different from the original. Therefore, since there is no failure mode associated with the EDG that will be affected by an increase in the duration of the integrated ESF/LOOP test interval, implementing a staggered integrated ESF/LOOP test interval does not create a significant reduction in the plant's margin of safety and does not create a substantial safety hazard.

5.4 DETERMINISTIC EVALUATION SUMMARY

5.4.1 Defense-in-Depth Summary

This deterministic evaluation shows that the elements of defense-in-depth are preserved when implementing a staggered integrated ESF/LOOP test interval. These elements include:

- A reasonable balance among preventing core damage, preventing containment failure, and consequence mitigation is preserved,
- Programmatic activities are not relied upon to compensate for weaknesses in plant design,
- System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system,
- Defenses against potential CCFs are maintained, and the potential for introduction of new CCF mechanisms have been assessed,
- Independence of barriers is not degraded, and
- Defenses against human errors are maintained.

A reasonable balance among preventing core damage, preventing containment failure, and consequence mitigation is preserved since the staggered test interval has a negligible impact on CDF and LERF and 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 remains unchanged. Consequence mitigation remains unaffected by staggering the surveillance interval. Further, no new accident or transient is introduced by extending the surveillance interval and the likelihood of an accident or transient is not impacted. Conversely, a staggered test interval may reduce the likelihood of a test-induced transient or accident.

The plant design will not be changed to accommodate a staggered integrated ESF/LOOP test interval. All safety systems, including the ESFAS, will 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 insignificant (see Table 6.0-1) and additional control processes are not required to compensate for any risk increase. Thus implementing a staggered test interval does not rely on programmatic activities to compensate for weaknesses in plant design.

System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system. There is no impact on the redundancy, independence, or diversity of the ESFAS or of the ability of the plant to respond to events. The ESFAS is comprised of diverse and redundant sub-systems and remains unchanged. There is no change to the signals available to trip the reactor or initiate an ESFAS actuation.

Defenses against potential CCFs are maintained and the potential for introduction of new CCFs mechanisms have been assessed. The staggered surveillance test interval is not sufficiently long to expect new CCFs mechanisms to arise. In addition, the operating environment for these components remains unchanged; therefore no new CCFs 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.

Defense in depth barriers are not degraded since the barriers protecting the public and the independence of these barriers are maintained. It is not expected that a 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 when operating on a staggered surveillance test interval.

Defenses against human errors are maintained since no new operator actions related to the staggered test interval are required. No additional operating or maintenance procedures are introduced or have to be revised, except to note the new test frequency, when implementing a staggered test interval and no new at-power test or maintenance activities are required.

5.4.2 EDG Component Deterministic Summary

This generic defense-in-depth evaluation of the EDG system and equipment and other time sensitive control circuits within the ESF actuation system did not identify any components with a failure rate that would be adversely affected by an increase in the integrated ESF/LOOP test interval. The analysis found that the failure rate of ESF equipment and control circuits is unrelated to the integrated ESF/LOOP surveillance test interval.

If a similar plant specific analysis of a Category A component was to identify any time dependent failure mode, each failure mode must then be evaluated to ensure that surveillance requirements, calibration, functional testing and an operability determination are performed at a time interval of less than one refueling cycle. If a time dependent failure mode is found in a Category A component tested solely by the integrated ESF/LOOP test, then the following must be performed to evaluate the acceptability of increasing the integrated ESF/LOOP surveillance test interval:

1. Ensure a preventive maintenance program is established to remove the time dependent failure mode and to assure that the components hazard rate remains constant,
2. Ensure that the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact.

This defense-in-depth analysis of the selected Category A components found that extending the integrated ESF/LOOP testing to every other refueling interval on a staggered basis would not increase the unavailability of one train of ESF. In addition, the increase in ESF/LOOP test interval does not adversely impact the defense-in-depth of the emergency power distribution system as required by General Design Criteria 17 and 18. The increase in the integrated ESF/LOOP test interval will not change the acceptance guidelines of RGs 1.9 or 1.108 or IEEE Standard 387 since all required EDG testing will still be verified and EDG operation during emergency conditions is not compromised.

6.0 ASSESSMENT OF DEMONSTRATION PLANT RISK FACTORS

In WCAP-15830-P, Revision 0, four plants completed a plant specific risk analysis to determine the impact of extending the integrated ESF/LOOP test interval from once per refueling cycle on a sequential basis to once every other refueling cycle on a staggered basis. Updated risk analysis for two demonstration plants (Fort Calhoun and Waterford Unit 3) are provided in this report.

All risk analysis will be revised and updated to RG 1.200 requirements to support plant specific implementation of staggered surveillance intervals for integrated ESF/LOOP testing. The results of the analyses are summarized in Table 6.0-1 with updated information provided for Fort Calhoun and Waterford Unit 3. ANO-2 did not perform a risk analysis because all components covered by integrated ESF/LOOP testing are also tested by other required tests that have a test frequency of once per cycle or more frequently.

a,c

Table 6.0-1
Results from Sequential to Staggered Integrated ESF/LOOP Testing

	CDF			LERF		

6.1 Process Summary

6.1.1 Categorization of Components

a,c

a,c

The effect of failure to load shed on the EDGs was evaluated, to investigate:

1. The impact of all components that are designated to load shed on LOOP.
2. The consequences, i.e., the ability of the EDG to maintain rated voltage and frequency, and any effects on the components supplied by the associated EDG.
3. Prioritize components failing to load shed.

The results of the analysis were used to adjust the event frequencies and/or modify the risk model as appropriate to ensure that load shed failures were addressed.

6.1.2 Base Case Modification

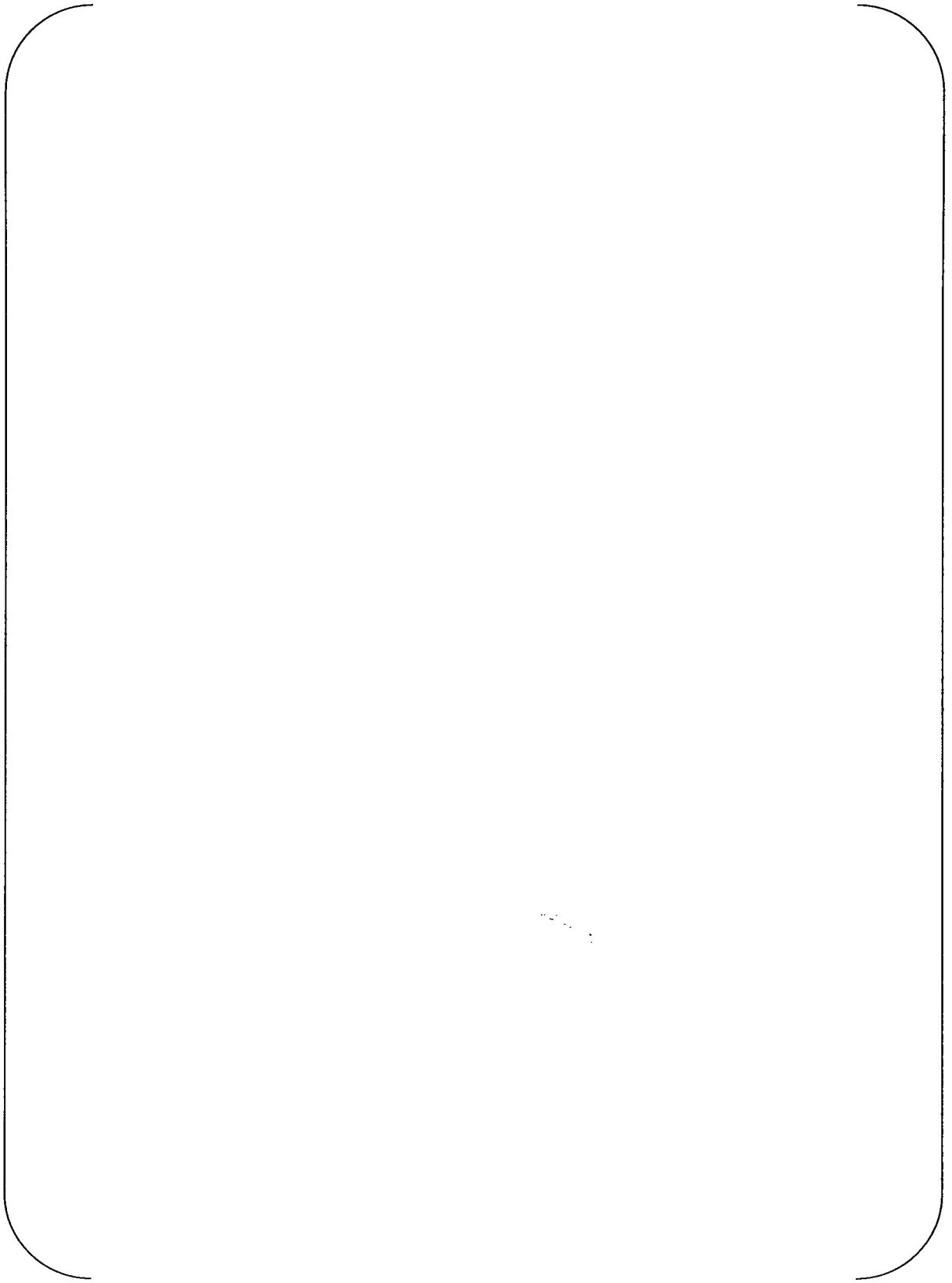
a,c

[ ] a,c

6.1.3 Analyses to Evaluate Impact of Surveillance Test Interval

[ ] a,c

a,c



a,c

6.2 EVALUATION OF RESULTS

6.2.1 Acceptance Criteria

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

6.2.2 Scope of PRAs

In WCAP-15830-P, Revision 0, four plants completed a plant specific risk analysis. For these four plants, the demonstration risk evaluations used PRA models with scopes varying from site to site. The Calvert Cliffs PRA was a Level 2 at-power that included internal events (including flood) and external events. The external events that were included are fire, seismic and high wind (hurricane and tornado). Fort Calhoun's PRA scope considered seismic, internal events and flood. Palisades and Waterford considered internal events only in their respective PRA scopes. Waterford is located in a very low seismic region, so the lack of a seismic model does not significantly impact their results.

Fort Calhoun and Waterford updated their PRA to support this revision of WCAP-15830-P. As part of there update, Fort Calhoun added Category A-3 components to the base model. The Waterford update addressed findings from their peer review and incorporated a simplified NUREG/CR-6595 (Reference 32) LERF model.

6.2.3 Factors Affecting Results

a,c

6.2.4 Shutdown Risk Assessment

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

6.2.5 PRA Detail Needed for Change

The PRA explicitly models the functions associated with ESFAS. Calvert Cliffs units 1 and 2 are the only demonstration plants in which all unit-to-unit interactions have been considered. Common cause has been addressed earlier in Section 4.4.

6.2.6 Sensitivity Studies

a,c

a,c

6.2.7 Unavailability Impacts

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

In addition, all the components tested by the integrated ESF/LOOP test must be available, or nominally available if placed into a special testing configuration. Since any equipment tested by the integrated ESF/LOOP test must be available to conduct the integrated ESF/LOOP test, such testing does not impact unavailability.

7. 0 OPERATING EXPERIENCE REVIEW AND ANALYSES

7.1 ANALYSES OF FAILURES AND ISSUES DISCOVERED DURING INTEGRATED ESF/LOOP TESTING

a,c

Table 7.1-1
Integrated ESF/LOOP Test Performance Summary

a,c

Units (6)	Study Time Period (Yr.)	Number of Integrated ESF/LOOP Tests Performed in Study Period	Number of CRs/ ERs Reviewed	Group			
				I	II	III	IV

7.2 Analyses of Equipment Failures Discovered during Integrated ESF/LOOP Testing

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

To simplify the analyses and focus just on functions usually verified by the integrated ESF/LOOP test, the following functions were analyzed (refer to Table 7.2-1): (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/LOOP test has been instrumental in discovering only a very few significant equipment failures.

Table 7.2-1
Verifications vs. Failures

a,c

Function	Total Number of Verifications	Number of Group I Equipment Failures per Function	Number of Group II Equipment Failures per Function

8.0 RESULTS AND CONCLUSIONS

8.1 RISK INFORMED EVALUATION

In WCAP-15830-P, Revision 0, four plants completed a plant specific risk analysis to determine the impact of extending the integrated ESF/LOOP test interval from once per refueling cycle on a sequential basis to once every other refueling cycle on a staggered basis. Updated risk analysis for two demonstration plants (Fort Calhoun and Waterford Unit 3) are provided in this report.

The calculated ΔCDFs at the demonstration plants varied from [ ]^{a,c} per year to [ ]^{a,c} per year (refer to Table 6.0-1). The ΔLERFs at these plants varied from [ ]^{a,c} per year to [ ]^{a,c} per year. ANO-2 had no components for which the integrated ESF/LOOP test was the sole test of operability, therefore that plant had no change in CDF or LERF associated with the change to the integrated ESF/LOOP test interval. The acceptance guidelines for proposed changes as provided in RG 1.174 consider CDF changes and LERF changes of 1.0E-06 per year to 1.0E-07 per year, 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 interval of integrated ESF/LOOP testing on a given ESF train from once per normal refueling cycle [18] months with sequential testing to once every other cycle [36] months with staggered test basis results in very small risk changes. Therefore the changes are acceptable from a risk perspective.

8.2 OVERALL EVALUATION

Implementation of the method described in this report is plant specific. This report provides the generic methodology to be followed and plant specific analyses required. Utilities desiring to adopt a staggered test basis for the integrated ESF/LOOP test must first perform the required plant specific risk analyses and defense-in-depth evaluation and then submit a request to change the affected TS surveillance intervals.

The overall conclusion, based on risk analysis for the demonstration plants and the generic deterministic evaluation of typical Category A components, is that changing the interval of integrated ESF/LOOP testing on a given ESF train from once per normal refueling cycle [18] months with sequential testing to once every other refueling cycle [36] months with staggered test basis results in very small risk changes that are within the acceptance criterion of RG 1.174.

9.0 ADDITIONAL IMPLEMENTATION GUIDANCE

The following activities must be addressed by each utility in their request to extend the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] months to every other refueling interval on a staggered basis [36] months:

1. Ensure that they have an administrative program in place to trend, monitor and evaluate failures of all components tested solely by the integrated ESF/LOOP test.

2. Ensure that all components tested solely by the integrated ESF/LOOP test are categorized Risk Significant as defined by the Maintenance Rule.

3. Perform the following actions if a component that is tested solely by the integrated ESF/LOOP test fails during performance of the integrated ESF/LOOP test: (This guidance applies only to equipment failures, not test or human performance related failures.)

    - Category A component failures:
        - Initiate failure analyses to determine failure mode and time dependency in accordance with (IAW) plant Corrective Action Program,
        - Using existing plant Maintenance Rule procedures, evaluate the failure to determine if it is potentially a common-mode failure. If it is determined to be a potential common-mode failure, immediately test the same component/function in the opposite train (IAW plant specific test procedures),
            - If there is no way to individually test the opposite train component, then perform a full IESF test on the opposite train during the current outage,
        - Correct the failure and perform a component specific test (IAW plant specific test procedures).
            - If there is no way to individually test the repaired component, then perform a full IESF retest on the affected train,
        - Procedures for re-running TS surveillance tests are plant specific

    - Non-Category A component failures:
        - Initiate failure analyses to determine failure mode, IAW plant Corrective Action Program,
        - Using existing plant Maintenance Rule procedures, evaluate the failure to determine if it is potentially a common-mode failure. If it is determined to be a potential common-mode failure, immediately test same component/function in opposite train to demonstrate availability,
        - Correct failure and perform component specific test on affected train to demonstrate availability.

4. The utility's administrative program to trend, monitor and evaluate failures of all components tested solely by the integrated ESF/LOOP test should include provisions for evaluating failures of Category A components and for implementing additional testing for any of the Category A components that show evidence of increasing failure rates for the extended test interval.

5. Each utility must document that the safety analysis acceptance-criteria as stated in the updated Final Safety Analysis Report are not impacted by this extended staggered interval test change.

The utilities should document that diversity with regard to signals, which provide reactor trip and actuation of engineered safety features, will also be maintained and that the 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.

6. Each utility must modify their plant specific PRAs to include:
   - PRAs must be modified to include the Category A-3 and Category A-4 components and the base model will need to be requantified,
   - The common cause failure models for the Category A components will need to be adjusted as follows;
     - For Alpha PRA model, use the staggered test interval equations to calculate Common Cause unavailability,
     - For full Multiple Greek Letter (MGL) PRA model, use equivalent equations or use Alpha model equations and then convert back to MGL,
     - For Simplified MGL PRA model with modules, replace modules with basic event with probability calculated separately using the appropriate equations.

7. Each utility will need to provide specific evidence that their PRA meets RG 1.200 and is compliant with the ASME PRA standard, RA-Sb-2005, with respect to key areas of technical adequacy for the application. RG 1.200 references the ASME PRA standard, RA-Sb-2005, for internal events at power. External events and shutdown risk impact may be considered quantitatively or qualitatively. The required documentation includes:
   - Summary of results of NEI 00-02 peer review,
   - Summary of results of gap analysis per RG 1.200, Appendix B,
   - Status of all "A" and "B" Facts & Observations (F&Os),
   - For any open "A" or "B" F&Os from either the NEI 00-02 peer review or any subsequent reviews or self-assessments, an assessment of potential impact of the unresolved issue on the application.

8. The key areas of technical adequacy for this application include
   - Accident Sequence analysis, with particular emphasis on AS-A10, AS-B1, AS-B2, and AS-B5,
   - Systems Analysis, with particular emphasis on SY-A8, SY-A11, SY-A12, SY-A13, SY-18a, SY-B1, SY-B3, SY-B4, SY-B10, SY-B11, SY-B14 and SY-B15,
   - Data Analysis, with particular emphasis on DA-A1, DA-A1a, DA-A2, DA-A3, DA-B1, all of DA-C and all of DA-D. (Note: for DA-D5, the plant must meet CC-II or better for this application.),
   - Quantification with particular emphasis on QU-A2b, QU-D and QU-E,
   - Large Early Release Frequency.

(Note: All of the supporting requirements in the ASME PRA standard are important to establishing the technical adequacy of a PRA for an application. The requirements called out above are those that focus on the level of detail needed to support this application.)

9. Utilities will have to evaluate changes in both CDF and LERF, and provide a numerical uncertainty analysis for CDF and LERF. This uncertainty analysis covers the numerical uncertainty in the failure rates. (Note: MTBF is essentially the inverse of the failure rate.)
   - LERF will be based on a simplified LERF model (per NUREG/CR-6595) (Reference 32).

10. Each utility must perform a sensitivity analysis to evaluate the potential impact of aging-related increases in the average failure rate after 24 months. Details of how to perform the sensitivity is described in Section B4.2.2 of this report. (Note: another sensitivity study to evaluate the potential impact of use of a combined binomial/standby failure rate model for demand failures was treated qualitatively in Section 6.2.6.)

11. Utilities must show that the changes will not invalidate any assumptions in the plant licensing basis. Check for prohibitive commitments. Some of the commitments to maintain a certain surveillance test interval may have been made in relation to certain other plant issues. As part of this step, such commitments are identified and then examined to determine if they can be changed. If there are no such commitments, then the STI change process continues. If the are commitments, then each commitment must be evaluated and changed as per NEI 99-04 guidance (Reference 33).

12. ASME RA-Sb-2005, Item 5.2 (d) (Reference 4), requires re-evaluation of past risk informed applications when the PRA is modified. If a plant identifies any Category A-3 or Category A-4 components, these components need to be incorporated into the base model. After incorporating these changes, the plant needs to perform a qualitative review of past Risk-Informed applications to determine if the changes might impact the conclusions for these applications. If there is any indication that the incorporation of the Categories A-3 and A-4 components might affect the results of a previous risk-informed application, the plant should requantify the risk calculations for the application to confirm that the results are still acceptable.

13. Utilities must show process elements for determining the cumulative risk impact of the changes, updating the PRA, and for imposing corrective actions, if necessary, following implementation per NEI 04-10 (Reference 1).

14. A multi-disciplinary plant decision-making panel should be utilized to evaluate the impact of revised surveillance frequencies, based on operating experience, test history, manufacturer's recommendations, codes and standards, and other factors, in conjunction with the risk insights from the PRA. Results and bases for the decision must be documented in the plant-specific application, per NEI 04-10.

15. A reliability review (based on operations and maintenance history) must be performed on the Category A components per NEI 04-10.

10.0 REFERENCES

1. NEI 04-10, Revision 0, "Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies," July 2006.
2. 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.
3. Regulatory Guide 1.200, Revision 1, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," January 2007.
4. ASME RA-Sb-2005, "Addenda to ASME RA-S-2002 Standard For Probabilistic Risk Assessment For Nuclear Power Plant Applications," December 2005.
5. General Design Criteria GDC 17 and CDC 18, 10CFR50, Appendix A
6. Regulatory Guide 1.9, Revision 3, "Selection, Design, Qualification and Testing of Emergency Diesel Generator Units used as Class 1E Onsite Electric Power Systems at Nuclear Power Plants, July 1993.
7. Regulatory Guide 1.108, Revision 1, "Periodic Testing of Diesel Generator Units used as Onsite Electric Power Systems at Nuclear Power Plants," August 1977.
8. IEEE Std 387-1995, "IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power".
9. Maintenance Rule, 10CFR50.65.
10. NUREG-1432, Revision 03, "CE Improved Standard Technical Specifications," March 3, 2004.
11. NEI 00-02, "Probabilistic Risk Assessment (PRA) Peer Review Process Guidance," Revision A3, March 2000.
12. Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," August 1998.
13. TSTF-425, Revision 1, "Relocate Surveillance Frequencies to Licensee Control".
14. NEI 06-09, Revision 0, "Risk-Informed Technical Specifications Initiative 4B, Risk-Managed Technical Specifications (RMTS) Guidelines," November 2006.
15. NUREG-0800, Standard Review Plan 19.1, "Determining The Technical Adequacy Of Probabilistic Risk Assessment Results For Risk-Informed Activities," June 2007.
16. NUREG-0800, Standard Review Plan 19.2, "Review of Risk Information Used to Support Permanent Plant Specific Changes to the Licensing Basis: General Guidance," June 2007.
17. NUREG-0800, Standard Review Plan 16.1, "Risk-Informed Decisionmaking: Technical Specifications," March 2007.
18. ASME OM-S/G-2000, Part 15, "Performance Testing of Emergency Core Cooling Systems in Pressurized Water Reactor Power Plants".
19. CEN-327-A, Revision 000, "RPS/ESFAS Extended Test Interval Evaluation," May 1986.
20. CEN-403, Revision 000, "ESFAS Subgroup Relay Test Interval Extension," July 1991.
21. Calvert Cliffs Units 1 and 2 Final Safety Analysis Report, Revision 38, September 2006.
22. Millstone Unit 2 Final Safety Analysis Report, Change Number 61, June 2002.

23. St. Lucie Units 1 and 2 Final Safety Analysis Report, Amendment 21 and Amendment 17, December 2005.

24. Fort Calhoun Final Safety Analysis Report, Revision 21, August 9, 2005.

25. Palisades Final Safety Analysis Report, Revision 26, April 2007.

26. Waterford Unit 3 Final Safety Analysis Report, Revision 15, June 2007.

27. Arkansas One Unit 2 Final Safety Analysis Report, Amendment 20, April 2007.

28. Not used.

29. Palo Verde Nuclear Generating Station Units 1, 2 and 3 Final Safety Analysis Report, Revision 14, June 2007.

30. NUREG/CR-5485, "Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment," November 1998.

31. NUREG/CR-5497, Common Cause Failure Parameter Estimations, October 1998.

32. NUREG/CR-6595, Revision 1, "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," October 2004.

33. NEI 99-04

34. WCAP-16341-P, "Simplified Level 2 Modeling Guidelines," November 2005.

APPENDIX A

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

This Appendix is Intentionally Blank

APPENDIX B

APPLICATION OF WCAP-15830-NP TO FORT CALHOUN STATION UNIT 1

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

B1.0 ABSTRACT

This report documents the results of Pressurized Water Reactor Owners Group (PWROG) CEOG Task 2016, Staggered Integrated ESF/LOOP Testing. CEOG Task 2016 used a risk-informed, performance-based approach to demonstrate that changing the integrated ESF/LOOP test from once per cycle on a sequential basis to once every other cycle on a staggered test basis results in a negligible change in risk. Currently, integrated ESF/LOOP testing is performed on both ESF trains each refueling cycle. Using a staggered approach, one ESF train will be tested each refueling outage with each ESF train being tested once every other cycle.

The methodology described in this report is consistent with NEI 04-10, Risk-Informed Technical Specifications Initiative 5b, "Risk-Informed Method for Control of Surveillance Frequencies". NEI 04-10 uses a risk-informed, performance-based approach to establish surveillance frequencies, consistent with the philosophy of NRC Regulatory Guide (RG) 1.174. Sensitivity studies were performed on important PRA parameters. PRA technical adequacy is addressed through NRC Regulatory Guide 1.200, which references the ASME PRA standard, RA-S-2005b, for internal events at power. External events and shutdown risk impact may be considered quantitatively or qualitatively.

This Appendix demonstrates the application of a staggered integrated ESF/LOOP testing at Fort Calhoun Station (FCS) Unit 1. It describes the major elements of the process including the following: procedure review, component categorization, component evaluation and risk analysis. The deterministic assessment of Category A components based on Section 5.0 of the generic process is not included in this demonstration, but will be address in a plant-specific submittal. The Technical Specification Surveillance Requirements addressed by the integrated ESF/LOOP test are listed in Table B2.3a.

The following is a summary of the method employed to determine the impact of extending the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] to every other refueling interval on a staggered basis [36] months. The first part consisted of a review of FCS procedures in conjunction with the component test matrix development (see Section B3.0). The second part consisted of the categorization of components and functions tested by the integrated ESF/LOOP test. The third part included the preliminary PRA review and Category "A" component sub-categorization. The fourth part of the method was the finalization of the PRA review and categorization. The PRA model was updated to explicitly reflect the [18] month test interval and included incorporation of the Category A-3 and Category A-4 components into the model. The PRA model reflecting the [18] month test interval was quantified. The model was then quantified a second time using the failure rates corresponding to a [36] month test interval in order to quantify the difference between the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) corresponds to the change in risk for the staggered STI. The fifth part, the Defense-in-Depth Evaluation, was not completed for this demonstration. The applicant must include the complete evaluation in the plant specific application. The last part is an overall assessment of the acceptability of the change.

The risk contribution associated with extending the current FCS [18] month test interval to a [36] month test interval on a staggered basis has been quantitatively evaluated using the current FCS PRA model. The calculated increase in Core Damage Frequency (ΔCDF) due to increasing the STI from an [18] months interval to a 36 month staggered test interval with one train tested each reviewing outage is [36] per year. The estimated change in Large Early Release Frequency (ΔLERF) is [ ]^{a,c} per year. This change in risk is within the RG 1.174 (Reference 2) criteria of 1E-06 per year for the ΔCDF and 1E-07 per year for the ΔLERF.

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

B2.0 BACKGROUND

The Engineered Safety Features system functions are controlled by the Engineered Safeguards Controls System (SSCS). Engineered Safeguards Equipment includes Engineered Safety Features Systems, Essential Auxiliary Support Systems and Engineered Safeguards Controls and Instrumentation. A non-CE designed ESCS 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 and 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 the minimum set of safeguards equipment.

The following is a brief description of the 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 affect 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 the consequences of a design basis event such as, a loss of coolant incident, a 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. The FCS 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. Non-essential equipment loads are then re-connected automatically or 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 4.16kV and 480-volts loads 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 a minimum initial delay.

The load connection sequence is the same whether off-site normal or on-site emergency power supply is used. When an 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 directly-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 an event 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.

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 to start and align equipment required to mitigate design basis events. A critical aspect of the ESCS design is to address 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 under-voltage relay protection scheme, which ensures 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 under-voltage 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 under-voltage 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 under-voltage 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 under-voltage 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 under-voltage relays will load shed the large 480V loads. The OPLS signal also directly (not through an under-voltage 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 the Technical Specification Surveillance Requirements that apply to integrated ESF/LOOP testing at FCS.

Table B2.3a
Existing Surveillance Test Intervals

SR	SR Description	Interval
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, Item 19	Verify manual Recirculation Actuation.	18 months
T.S.3.1, Table 3-2, Item 20(b)	Verify Recirculation Actuation Logic.	18 months
T.S.3.1 Table 3-2, Item 22	Verify manual Emergency Off-site Power Low Trip Actuation	18 months
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	18 months

Table B2.3a Existing Surveillance Test Intervals		
SR	**SR Description**	**Interval**
	perform its intended functions.	
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	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
T.S.3.8	Verify the ability of the main steam isolation valves to close upon signal.	18 months

B2.4 CHANGES TO TECHNICAL SPECIFICATIONS

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

Table B2.4a
Surveillance Test Interval Changes

SR	SR Description	Interval
T.S.3.1, Table 3-2, Item 3b	Verify Safety Injection Actuation Logic.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 5b	Verify Containment Spray Actuation Logic.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 8a	Verify Isolation Valve Closure.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 8b	Verify manual Containment Isolation Actuation.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 9	Verify manual Containment Spray Actuation.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 19	Verify manual Recirculation Actuation.	18 months on a Staggered Basis
T.S.3.1, Table 3-2, Item 20(b)	Verify Recirculation Actuation Logic.	18 months on a Staggered Basis
T.S.3.1 Table 3-2, Item 22	Verify manual Emergency Off-site Power Low Trip Actuation	18 months on a Staggered Basis
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 Basis
T.S.3.2, Table 3-5, Item 14	Verify Pressurizer Heater control circuit operation for post-accident use.	18 months on a Staggered Basis
T.S.3.6 (1)	Verify that the Safety Injection system will respond promptly and perform its intended functions.	18 months on a Staggered Basis
T.S.3.6 (2)	Verify that the Containment Spray system will respond promptly and perform its intended functions.	18 months on a Staggered Basis
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 Basis
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 Basis
T.S.3.8	Verify the ability of the main steam isolation valves to close upon signal.	18 months on a Staggered Basis

B3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

B3.1 METHOD DISCUSSION

B3.1.1 Integrated ESF/LOOP 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/LOOP 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/LOOP 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/LOOP test procedures to other surveillances that test the same components and functions.

The database contains references to the integrated ESF/LOOP test and other tests, as well as a preliminary PRA evaluation and assessment. The preliminary PRA assessment performed by Westinghouse provided

the foundation for the plant specific PRA calculation performed by FCS in 2002. The FCS PRA model was updated in 2007 and is referred to as Revision 8.

Table B3.1a defines the procedure review portion of the database used to develop the matrix. PRA 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	Associated Surveillance test
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/LOOP test.
Integrated test Summary	Summarizes the functions tested by the integrated test procedures for each component.
Cat	Component Categories A, B or C. Categories are defined and explained below. The initial PRA 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/LOOP 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/LOOP test on the same or more frequent basis. 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 of the candidate 'other test' procedures provided, Westinghouse made an assessment as to whether or not the integrated ESF/LOOP test was the sole/primary test for each component. An initial categorization of the components was then made. The Categories are defined as follows:

a,c

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

B3.2 Input

Westinghouse used electronic copies of current TS surveillance procedures provide by FCS to perform the review and develop the matrix database (refer to Table B3.1a for an explanation of the key fields in the database). Table B3.2a provides a list of the surveillance procedures included in the review, including the integrated ESF/LOOP procedures:

Table B3.2a
ESF Surveillance Test Procedures

Procedure Number	Procedure Title	Interval
OP-ST-ESF-0002, R39	EDG No. 1 and No. 2 Auto Operation	Once every 18 months
OP-ST-ESF-0011, R31	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, R22	Engineered Safety Features Off-Site Power Low Signal (OPLS) Functional Test	Once every 18 months
EM-ST-ESF-0001, R8	Quarterly Engineered Safety Features Offsite Power Low Signal (OPLS) Sensor Check	Once every quarter
EM-ST-RC-0001, R10	Pressurizer Heaters Control Circuit Operational Test	Once every 18 months
IC-ST-AFW-0001, R13	Auto Initiation of Auxiliary Feedwater Functional Check of Initiation Circuits	Once every 92 days
IC-ST-ESF-0001, R10	Functional Test Of Pressurizer Pressure Low Signal (PPLS) Actuation and Blocking Logic	Once every 18 months
IC-ST-ESF-0002, R912	Logic Channel Test of Containment Pressure High Signal (CPHS)	Once every 18 months
IC-ST-ESF-0003, R6	Functional Test of Steam Generator Low Pressure Signal (SGLS)	Once every 18 months
IC-ST-ESF-0004, R5	Channel Functional Test of Containment Pressure High Signal (CPHS) Switches	Once every 92 days
IC-ST-ESF-0005, R6	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, R14	Emergency EDG Endurance Functional Test	Once every 18 months
OP-ST-AFW-0004, R22	Auxiliary Feedwater Pump FW-10 Operability Test	Once every 18 months
OP-ST-AFW-0006, R7	AFW Operability Verification from AI-179	Once every 18 months
OP-ST-DG-0001, R53	EDG 1 Check	Once every month
OP-ST-DG-0002, R51	EDG 2 Check	Once every month
OP-ST-ESF-0001, R30	Diesel Auto Start Initiating Circuit Check	Once every Startup
EM-ST-ESF-0002, R1	13.8 KV Emergency Power Periodic Test	Once every 18 months

Table B3.2a ESF Surveillance Test Procedures		
Procedure Number	**Procedure Title**	**Interval**
OP-ST-ESF-0009, R48	Channel A Safety Injection, Containment Spray And Recirculation Actuation Signal Test	Once every 92 days
OP-ST-ESF-0010, R48	Channel B Safety Injection, Containment Spray And Recirculation Actuation Signal Test	Once every 92 days
OP-ST-ESF-0015, R22	480 Volt Load Shed and Engineered Safeguards Actuation Signal Retest	Once every 18 months
OP-ST-ESF-0022, R23	S1-2 Automatic Load Sequencer Test	Once every 92 days
OP-ST-ESF-0023, R23	S2-2 Automatic Load Sequencer Test	Once every 92 days
OP-ST-CH-3003, R43	Chemical & Volume Control System Pump/Check Valve Inservice Test	Once every 92 days
OP-ST-CH-3005, R14	Chemical And Volume Control System (CVCS) Category A and B Valve Exercise Test	Once every 18 months
OP-ST-RW-3002, R10	Raw Water System Category A and B Valve Exercise Test	Once every 92 days
OP-ST-CCW-3001, R9	Component Cooling Category B Valve Exercise Test	Once every 92 days
OP-ST-BD-3000, R9	Blowdown System Category A & B Valve Exercise Test	Once every 92 days
OP-ST-DW-3001, R10	Demineralized Water/Deaerated Water System Category A Valve Exercise Test	Once every 92 days
OP-ST-CA-3001, R10	Compressed Air Category A Inservice Valve Exercise Test	Once every 92 days
OP-ST-SL-3002, R15	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, R30	AC-10B Raw Water Pump Quarterly Inservice Test	Once every 92 days
OP-ST-RW-3021, R30	AC-10C Raw Water Pump Quarterly Inservice Test	Once every 92 days
OP-ST-RW-3031, R30	AC-10D RAW Water Pump Quarterly Inservice Test	Once every 92 days
OP-ST-CCW-3002, R19	AC-3A: Component Cooling Water Pump Inservice Test	Once every 92 days
OP-ST-CCW-3012, R16	AC-3B: Component Cooling Water Pump Inservice Test	Once every 92 days
OP-ST-CCW-3022, R16	AC-3C: Component Cooling Water Pump Inservice Test	Once every 92 days
OP-ST-AFW-0007, R3	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, R123a	Feedwater System Category A and B Valve Exercise Test	Once every 18 months

Table B3.2a ESF Surveillance Test Procedures		
Procedure Number	**Procedure Title**	**Interval**
OP-ST-SI-3001, R32	Safety Injection System Category A and B Valve Exercise Test	Once every 92 days
OP-ST-SI-3002, R25	Safety Injection System Category A, B and C Valve Exercise Test	Once every 92 days
OP-ST-CCW-3004, R18	Component Cooling Category A and B Valve Exercise Test	Once every 18 months
OP-ST-WDL-3001, R17	Waste Disposal System Category A and B Valve Exercise Test	Once every 92 days
OP-ST-VA-3001A, R5	Ventilating Air System Quarterly Category A Valve Exercise Test	Once every 92 days
OP-ST-SI-3022, R3a	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 Actuation	Once every 18 months
OP-ST-SHIFT-0001, R79	Operating Technical Specification Required Shift Surveillance	Once every day
IC-ST-AFW-0006, R1	Auto Initiation of Auxiliary Feedwater Functional Check of Logic Matrices	Once every 18 months
OP-ST-AFW-3010, R1	Auxiliary Feedwater System Quarterly Category A and B Valve Exercise Test	Once every 92 days
OP-ST-ESF-0018, R8	Engineered Safeguards Actuation Signal Retest	Once every 18 months
OP-ST-SI-3015, R0	Containment Sump Recirc Valves Exercise And Position Verification Test	Once every 18 months
OP-ST-SI-3021, R5	Room 21 Safety Injection/Containment Spray Pumps and Valve Exercise In-service Test	Once every 18 months
OP-ST-VX-3028, R0	Auxiliary Feedwater System Remote Position Indicator Verification Surveillance Test	Once every 18 months
Various – (Procedure reference listed were used in the database)	ISI/IST Equipment Test Surveillance's and PMS	Various - (STI listed were used in the database)

B3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in Section 4.0 of the main report. Table B3.3a provides a numerical summary of the classification results specifically for Fort Calhoun Station.

Table B3.3a
Categorization Summary for Fort Calhoun Station

a,c

Category	Number of Components

Figures B3.3-1 through B3.3-8 illustrates where there is overlap in integrated ESF/LOOP testing. 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. Figures 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

a,c

Figure B3.3-2
CIAS Surveillance Procedures - Fort Calhoun Station

a,c

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

a,c

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

a.c

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

a,c

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

a,c

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

a,c

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

a.c

B4.0 PROBABILISTIC RISK ASSESSMENT OF THE CHANGE IN STI

Westinghouse performed a preliminary categorization and assessment of components tested by the integrated ESF/LOOP test functions for FCS. FCS used the preliminary assessment as a foundation and starting point to perform the PRA analysis described in this Appendix. 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 or solely by the integrated ESF/LOOP testing.

The FCS PRA Master List of basic events was reviewed to determine if and how the model addresses each 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 change in the integrated ESF/LOOP surveillance test interval. Actual changes to the model were initially performed by FCS. Westinghouse performed the requantification of the model using Revision 8 of the FCS internal events PRA model for this report. The remainder of Section B4.0 is derived from the risk analyses.

B4.1 MODEL ANALYSIS

This analysis evaluates the risk impact of extending the test interval from once per refueling cycle on a sequential basis to once every other fueling 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 PRA. (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 train being tested every 18 months.)

The conclusions drawn in this appendix are applicable only to FCS. These conclusions are a strong function of the FCS PRA 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 PRA 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 logic to capture 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 under-voltage relay, which in turn energizes the trip coil. (The main under-voltage 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 under-voltage 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 under-voltage 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 under-voltage 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 under-voltage relay that energizes the main under-voltage 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 the relay contacts open. Opening the normally-closed 161/4.16kV circuit breaker completes the backup loss of voltage trip circuit and allows an under-voltage relay to be energized. The OPLS and the AC circuit breaker relays are in parallel with the under-voltage relay that energizes the main under-voltage relays which creates 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. Therefore, a total of five different relays or contacts must fail to prevent load shedding.

There is only one main under-voltage 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 under-voltage relay. The third and forth main failures are the lockout relays from the AC circuit breakers. The last failure that would have to occur is the under-voltage relay between the main under-voltage 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 devices for the 4.16kV loads are the trip coils and the circuit breakers. Many redundant signals are available to initiate load shed, thus it is unlikely that the two main under-voltage relays (the main one and the backup) would fail. The circuit breakers and their associated trip coils are contained in the FCS PRA Model.

480V Load Shedding

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

Load shed occurs through under-voltage 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 under-voltage relays are the only way that the single 480V loads can be automatically load shed. There are four under-voltage relays in series so if one fails, the components on that bus will not be load shed. 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 under-voltage 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 failed under-voltage relays on different buses. Particular loading

combinations are required 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 based on the total amount of horsepower required for steady-state operation, as opposed to the in-rush starting loads. Only the normally running components were considered because they would be picked up as dead load if load shedding were to fail. The horsepower required for each bus was obtained, then compared with the bus on DG-1 that had the highest horsepower requirements (for DG-1, bus 1B3B requires 650hp for all normally running components). Evaluations confirmed that the EDG could handle one failed bus since 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. Normally running components were modeled if the two buses added up to 650hp or more. The same philosophy applied for DG-2. More than two buses were not modeled because it would require three or more failed relays. 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 for the FCS PRA. Having a double bus failure is effectively improbable in a PRA sense, even when considering common-cause, and therefore was not modeled.

The MCCs on the nine buses could also fail to load shed. Failure of a single MCC to load shed, along with failure of an additional 480V load to load shed, could cause failure of an EDG. This is 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 could cause the MCC not to load shed. The motor contactors for many of the MCC loads "drop out" when power is removed. However, there are 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 a dead load. 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, normally-running components on the MCCs that are supposed to be load shed were identified. 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. Finally, 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 failed to load shed and if the combined horsepower would fail the EDG, then the relays for the MCC are in the FCS PRA 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

FCS documentation shows 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 that, if not load shed could cause failure of the EDG. Also, MCCs-3A4,-3C3 and -3B2, if not load shed, could cause EDG failure to due to overload.

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 under-voltage 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 AND'ing 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 PRA-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 over-speed trip would have to combine with an actual non-emergency EDG 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 [ ]^{a,c} with a condition causing a non-emergency EDG trip [,]^{a,c} is usually not modeled since realistic sequences involving emergency-mode operation of the EDG 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 [ ]^{a,c}.

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 PRA.

The spent fuel storage pool cannot contribute a meaningful heat load to 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.

This analysis assumed that the current ESCS relay surveillance test interval is [18] months for all relays and the revised test interval is [36] months with one train being tested every [18] months. This assumption maximizes the estimated ΔCDF and ΔLERF.

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 testing FCS ESCS relays on a staggered test schedule. RG 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.

B4.2 SCOPE OF FCS PRA

The FCS PRA is an at-power, internal and external events PRA. 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 logic that captures LERF cutsets. The Level 2 portion of the FCS PRA model is based on the Simplified Level 2 Modeling Guidelines documented in WCAP-16341-P (Reference 34). 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 PRA 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 PRA. Common cause basic events have been directly incorporated into the fault tree models, and represent the failure of all components with in defined group by a specified failure mode, for example if i.e., all safety injection pumps fail to start on demand due to common causes. This approach is used throughout the FCS PRA. Other key common cause impacts related to the EDGs are 125VDC batteries, CCW pumps, RW 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, which is three to four orders of magnitude below the most significant sequences identified in the analysis.

B4.2.2 Sensitivity Study

A notable assumption that is made in a PRA model is that all components in the plant have a constant failure rate during their scheduled testing cycle. All Category A components considered in this evaluation for FCS are on an 18 month sequential testing cycle (sequential meaning both trains of equipment are tested on the same schedule). An integrated ESF/LOOP test interval of 36 months for these components will increase their exposure time beyond what they have experienced in the past The generic Failure Modes and Effects Analyses (FMEA) discussed in Section 5.3 indicates that there are no failure modes/mechanisms that are likely to experience aging degradation over the 36 month test interval. However, the likelihood that failures due to aging will occur was evaluated with a sensitivity study that approximates the impact of aging for components tested on a 36 month staggered testing cycle.

The affect of aging can be approximated using insights from the product hazard rate Bath-Tub Curve, illustrated in Figure B4.2.2-1. As mentioned above, PRA models assume that the components in the plant are on the flat portion of this curve. However this assumption has only been shown to be valid for the first 24 months of a test interval (based on the 24 month testing cycle used at Calvert Cliffs). For this sensitivity studies this assumption is revised to reflect a constant hazard rate for the first 24 months of the test interval; after that the hazard rate is adjusted as the component enters the increasing hazard rate portion of the Bath-Tub Curve.

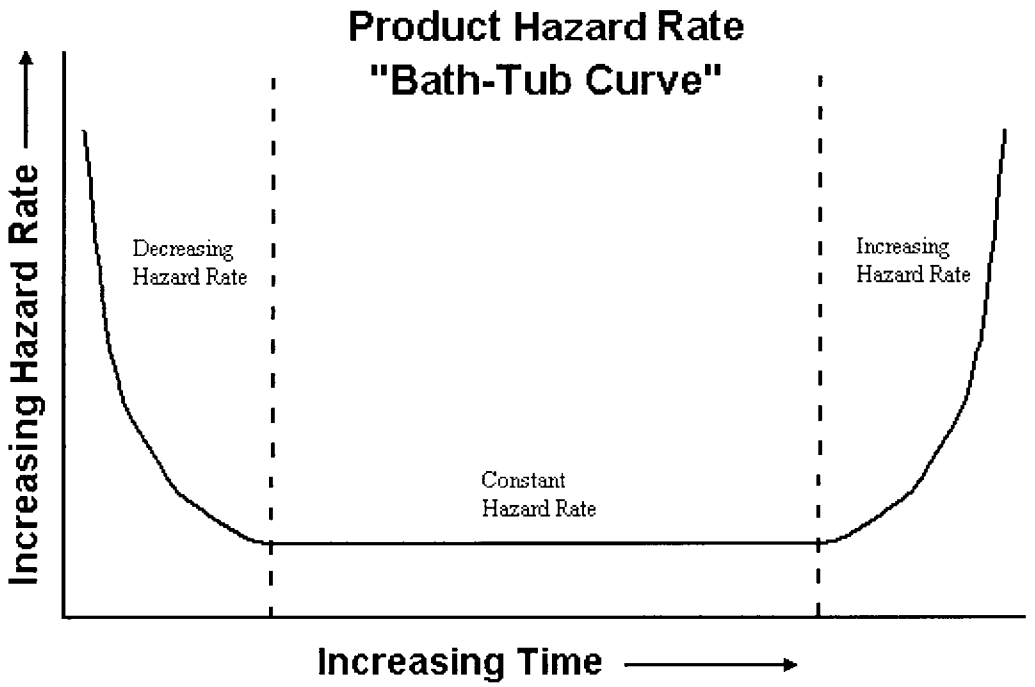


Figure B4.2.2-1: Graphical Representation of the Component Hazard Rate "Bath-Tub Curve"

To estimate the impact of aging related failures, the failure rate of a given component can be increased during the final 12 months of the testing interval. Figure B4.2.2-2 shows the failure rates increase that were considered for this study. As shown, the nominal component failure rate (the component hazard rate multiplied by time) is assumed constant for the first 24 months. After 24 months, the failure rate doubles during the next 6 months and for the final 6 months of the testing cycle the failure rate is assumed to be six times its nominal value.

a,c

Figure B4.2.2-2: Probability of Failure for the Sensitivity Evaluation

The information shown in Figure B4.2.2-2 cannot simply be applied to a basic event in a PRA model. The events in a PRA consider the average unavailability of a component which can be calculated as:

$$\overline{U} = \int_0^{\tau} \left(\frac{\lambda \, t}{\tau} dt \right) = \frac{\lambda \, \tau}{2}$$

where, $\overline{U}$ is the Average Unavailability
λ is the failure rate
τ is the testing interval, and
t is time

From this equation the average unavailability of the following cases can be calculated:

- 18 month testing cycle at a constant failure rate:

$$\overline{U} = \int_0^{18}\left(\frac{\lambda t}{18}dt\right) = 9\lambda$$

- 36 month testing cycle at a constant failure rate:

$$\overline{U} = \int_0^{36}\left(\frac{\lambda t}{36}dt\right) = 18\lambda$$

This shows that increasing the testing interval by a factor of 2 results in an average unavailability two times the original unavailability. This is consistent with the factor of 2 that was used to evaluate the impact of doubling the testing interval.

- 36 month testing cycle for the sensitivity case with the variable failure rate represented in Figure B4.2.2-2:

a,c

B4.3 QUALITY OF FCS PRA

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

- Formal qualification program for the PRA staff
- Use of procedures to control PRA processes
- Independent reviews (checks) of PRA documents
- Comprehensive PRA Configuration Control Program
  - Quarterly plant change monitoring program
  - Process to control PRA 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 PRA Technical Positions
- Commitment of continuous quality improvement

Considering the scope (internal and external events), level of detail and processes, the FCS PRA is sufficient to support a technically defensible and realistic evaluation of the risk associated with extending the surveillance interval for the integrated ESF and loop tests.

B4.4 PRA SOFTWARE

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

B4.4.1 CAFTA

CAFTA is a commercial product developed and maintained by the Electric Power Research Institute for performing risk and reliability analyses. 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 the 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,c

Risk Metric	Base Value (per year)	Changed STI Value (per year)	Change in Risk (per year)

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 change in the integrated ESF/LOOP testing strategy. The base situation is having the integrated ESF/LOOP test performed once per normal refueling cycle ([18] months) on a sequential basis. The frequency of [18] months on a staggered test basis results in an interval between successive tests of a given ESF train of [36] months.

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

B5.0 DEFENSE-IN-DEPTH AND SAFETY MARGIN EVALUATION

The objective of the defense-in-depth evaluation is to show that there are no time dependent failure modes for the Category A components and to support the conclusion of the risk analyses that extending the Surveillance Test Interval (STI) for the integrated ESF/LOOP test results in only minor changes in plant risk. The change in the plant risk is evaluated deterministically by performing plant specific Failure Modes and Effect Analysis (FMEA) and a significant hazards evaluation on systems and equipment that is tested solely by the integrated ESF/LOOP test. The analysis addressed the following areas:

- Failure Mode,
- Failure Mechanism (cause),
- Failure Effects and Consequences
- Safety Significance and impact on margin of safety

The evaluation determined whether or not there are time dependent failure modes. If any time-dependent failure modes are identified, the plant must ensure that a preventive maintenance program is established to remove the time dependent failure mode and to assure that the component's hazard rate remains constant. In addition, the time dependent failure mode must be included the plant risk model.

To maintain plant defense-in-depth as described in the plant licensing basis, the licensee must ensure that there will be no significant increase in unavailability for a single ESF train if the extension in integrated ESF/LOOP testing is doubled, i.e., changed to every other refueling outage. The deterministic analysis provides the necessary balance between risk and deterministic arguments required by RG 1.174.

B5.1 Failure Modes and Effects Analysis

The defense-in-depth analysis for extending a STI requires analysis of time-dependent failure modes to identify any of the following:

- If the performed surveillance test covers all failure modes,
- If any of the identified failure modes are time dependent, meaning that the rate of change varies with time (i.e., heat exchanger fouling, time delay relay drift and unit coolers performance degrading),
- If other plant activities, such as maintenance program or surveillance testing have identified a time dependent failure mechanism,
- If a preventive maintenance program has been established to assure that the components hazard rate remains constant,
- If the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact.
- If any aspect of implementing an increased surveillance interval would introduce a potential for common cause failures.

B5.2 Significant Hazards Evaluation

The operability of the ESCS instrumentation and interlocks must ensure that when parameters monitored by each channel or combination thereof reaches its setpoint, an appropriate level of reliability of ESF instrumentation with sufficient redundancy is maintained to perform its intended functions. The operability of the ESF system is required to provide the overall reliability, redundancy, and diversity assumed available in the plant design for protection and mitigation of accident and transient conditions. For the above reasons, it is important that a safety evaluation be performed that considers each relevant failure mode against the possible impact on the ESF system capability to perform its intended functions.

Also, the evaluation must consider that at no time is the defense-in-depth of ESF system compromised, and it will function as described in the plant licensing bases.

The significant hazard analysis should include the following:

- Consequences of the identified failure mode,
- Safety significance of the failure mode,
- Effect of the failure mode on ESF actuation,
- Does the effect of the failure on ESCS creates the possibility of a new different kind of accident from any accident previously evaluated,
- Does the change in safety significance involve a significant reduction in a margin of safety?

B5.3 FCS Category A Components

An assessment of Category A ESF components will be submitted with the FCS License Amendment Request to implement staggered integrated ESF/LOOP testing at FCS. This assessment will support RG 1.174 and consider relevant safety margins and defense–in-depth attributes including consideration of success criteria as well as equipment functionality, reliability, and availability. The analysis will be based on the methodology shown in Section 5.0 of this report and will incorporate the actual design, construction, operation and maintenance practices in effect at FCS. The following is a list of example Category A components installed at FCS that will be included in the assessment.

- Under Voltage Relay 27, Manufactured by General Electric International Inc., Model: 12HFA51A42F
- Auxiliary Relay 74, Manufactured by General Electric International Inc., Model: 12HFA151A2F
- Sequencer Supervisory Relay 86, Manufactured by General Electric International Inc., Model: 12HGA17C52G
- Sequencer Auto Start and Lockout Relay 86, Manufactured by General Electric International Inc., Model: 12HEA61C241X2
- Load Shed Relay 94, Manufactured by General Electric International Inc., Model: 12HFA151A2H
- 1A3 4160V Supply Breaker 1A33
- MCC 480V 4A3 Supply Breaker 1B4A-7
- CH-4A, Boric Acid Pump
- HCV-268, Boric Acid Pomp Header To Charging Pump

B6.0 OVERALL CONCLUSION

Results of the FCS risk analysis show that the change in CDF and LERF are insignificant and fall well within the acceptance criteria of RG 1.174. These results support implementing a staggered test basis for the integrated ESF/LOOP tests at FCS. An overall evaluation of the acceptability of this change, taking into consideration the deterministic assessment of the Category A components, will be included in the plant specific application.

APPENDIX C

APPLICATION OF WCAP-15830-NP TO PALISADES NUCLEAR POWER PLANT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

C1.0 ABSTRACT

Pressurized Water Reactor Owners Group (PWROG) CEOG Task 2016, "Staggered Integrated ESF and LOOP Testing" used a risk-Informed and performance based approach to demonstrate that changing the integrated Engineered Safety Features (ESF) and Loss of Off-site Power (LOOP) test from once per refueling cycle on a sequential basis to once every other refueling cycle on a staggered test basis results in a negligible change in risk. Currently, the integrated ESF testing is performed on both safeguards and emergency power trains each refueling interval. Using a staggered approach, only one train would be tested each refueling outage. The basis for this change is the fact that the integrated ESF/LOOP test is not the primary or sole operability test for most of the components tested. Other TS required surveillance procedures are performed on many of these components and functions on the same or more frequent basis. Therefore, considerable overlap exists between the integrated ESF test and other testing.

The approach used to demonstrate that the changes to the integrated ESF/LOOP test interval are acceptable is summarized as follows. First, a base case Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) were calculated using the plant-specific Probabilistic Risk Assessment (PRA) model. The failure probabilities for the components/functions that are tested only by the integrated ESF/LOOP test were then adjusted to reflect the increase in the test interval for the individual trains. The overall risk associated with the change was recalculated, and compared to the base case risk. In some cases, it was possible to develop a reasonable deterministic basis to demonstrate that the component failure mode addressed by the integrated ESF/LOOP test was not risk-significant. These components were exempt from further PRA review and analysis.

The methodology is consistent with NEI 04-10, Risk-Informed Technical Specifications Initiative 5b, "Risk-Informed Method for Control of Surveillance Frequencies." NEI 04-10 uses a risk-informed, performance-based approach to establish the surveillance frequency, which is consistent with the philosophy of NRC RG 1.174. PRA methods were used to determine the risk impact of the revised intervals. Sensitivity studies were performed on important PRA parameters to evaluate the robustness of the risk evaluations. PRA technical adequacy is addressed through NRC RG 1.200, which references the ASME PRA Standard, RA-Sb-2005, for at-power, internal events. External events and shutdown are not considered for this evaluation.

This Appendix demonstrates the application of a staggered integrated ESF/LOOP testing at Palisades and is unchanged from Revision 0 of this report. It describes in detail the major elements of the process including: procedure review, component categorization, component evaluation and risk analyses. The deterministic assessment of Category A components (Section 5.0 of the generic process) is not included this Appendix, but will be addressed in a plant-specific submittal. The Palisades Technical Specification Surveillance Requirements addressed by the Integrated ESF Test are listed in Table C2.3a.

The following is a summary of the method employed to determine the impact of extending the interval between successive integrated ESF/LOOP tests on a given train from every refueling interval [18] months to every other refueling interval on a staggered basis [36] months. The first part consisted of a review of Palisades procedures in conjunction with the component test matrix development (see Section C3.0). The second part consisted of the categorization of components and functions tested by the integrated ESF/LOOP test. The third part included the preliminary PRA review and Category A component sub-categorization. The fourth part of the method was the finalization of the PRA review and categorization. The PRA model was updated to explicitly reflect the staggered [18] month test interval and included incorporation of the Category A-3 and Category A-4 components into the model. The PRA model reflecting the [18] month test interval was quantified. The model was then quantified a second time using

the failure rates corresponding to a 36 month test interval in order to quantify the difference between the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) corresponding to the change in risk for the staggered STI. The fifth part, the Defense-in-Depth Evaluation, was not completed for this demonstration. The applicant must include the complete evaluation in the plant specific submittal. The last part is an overall assessment of the acceptability of the change.

The risk contribution associated with extending the current Palisades 18 month test interval to a 36 month test interval on a staggered basis, a STI of 36 months, was quantitatively evaluated using the Palisades PRA model described in Revision 0 of this report. The safety significance is based on the increase in 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. The risk analysis presented in this Appendix was not updated due to resource limitations and the abbreviated completion schedule. Palisades will perform all the necessary updates and required analysis to support their plant-specific application at a latter date.

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 mitigate 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 automatically actuate safeguards and essential support systems. 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 Y10; Channel B from Panel Y20. Instrument Channel C has odd numbered devices and Instrument 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.

Load sequencers will be initiated, if a SIS is accompanied by a loss of offsite power. There are two 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 during 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 containment isolation control system is on a two-channel design 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. Two high-radiation or two high-pressure signals are required to initiate containment isolation. This prevents spurious signals from causing containment isolation.

Coincidence 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 in-containment monitors will also close all containment isolation valves not required for engineered safeguards when locked in by the respective refueling monitor key switches.

Coincidence 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.

A containment high-pressure signal will initiate SIS and start containment spray. The 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.

A containment high pressure 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 are also closed on a high pressure signal.

C2.2 PALISADES CONFIGURATION

The ESF functions to start and align equipment required to mitigate design basis events. A critical aspect of the Engineered Safeguards Control System (ESCS) design is to address 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. Reliable onsite power is provided by duplicate EDGs, where each EDG provides power to the minimum necessary safeguards equipment.

Both 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 exhauster, two starting circuits and a load sequencer. Supply of electric power for this system is obtained from the EDG they are supporting. Each EDG is located in a separate room 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.

C2.2.3 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 trip set point is selected 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/LOOP 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 TS Table 3.3.4-1)	18 months
S.R.3.3.5.1	Verify a CHANNEL FUNCTIONAL TEST on each EDG-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

Table C2.3a Existing Surveillance Test Intervals		
SR	**SR Description**	**Frequency**
S.R.3.8.1.7	Verify on an actual or simulated loss of offsite power signal, a. De-energization of emergency buses b. Load shedding from emergency buses c. DG auto starts from Standby condition and: 1. Energizes auto- connected emergency loads through automatic load sequencer 2. Supplies permanently connected and auto connected loads for > 5 minutes.	18 months
S.R.3.8.1.9	Verify each EDG: 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: 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 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 TS 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 EDG-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

Table C2.4a Proposed Surveillance Test Intervals		
SR	**SR Description**	**Frequency**
		Basis
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, a. De-energization of emergency buses b. Load shedding from emergency buses c. DG auto starts from Standby condition and: 1. Energizes auto- connected emergency loads through automatic load sequencer 2. 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: 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 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: 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 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 on a Staggered Test Basis

C3.0 TEST MATRIX AND COMPONENT CATEGORIZATION

C3.1 METHOD DISCUSSION

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

Integrated ESF/LOOP 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/LOOP 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/LOOP Testing Matrix was prepared by Westinghouse for Palisades as part of CEOG Task 2016, Staggered Integrated ESF/LOOP 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/LOOP 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 PRA 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 PRA 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/LOOP 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/LOOP test.
Summary of functions tested by Integrated ESF/LOOP test	Summarizes the functions tested by the integrated ESF/LOOP 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 Categories A, B or C. Categories are defined and explained below. The initial PRA assessment further divides Category A components into Categories 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 .
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/LOOP test (RT-8C and RT-8D).

The matrix was developed as follows: First, Palisades 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 RT-8C and RT-8D were identified, other related TS surveillance tests were reviewed to determine if they tested any of the same components tested by the integrated ESF/LOOP 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/LOOP test was the sole/primary test for each component. An initial categorization of the components was then made. These categories are defined as follows:

[redacted] a,c

The Category A and B components then became the focus and were reviewed further to determine the PRA impact. The PRA 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. Table C3.2a provides a list of the surveillance procedures included in the review, including the integrated ESF/LOOP procedures.

Table C3.2a
ESF Surveillance Test Procedure

Procedure Number	Procedure Title	Interval
RT-8C, Revision 22	Engineered safeguards System – Left Channel	Once every 18 months
RT-8D, Revision 23	Engineered safeguards System – Right Channel	Once every 18 months
QO-1, Revision 54	The Safety Injection System	Once every quarter
QO-5, Revision 73	Valve Test Procedure	Once every quarter
RE-137, Revision 2	Calibration of Bus IC Undervoltage and Time Delay Relays	Once every 18 months
RE-138, Revision 2	Calibration of Bus ID Undervoltage and Time Delay Relays	Once every 18 months
RE-139-1, Revision 3	Test Starting Time of DG 1-1	Once every 18 months
RE-139-2, Revision 3	Test Starting Time of DG 1-2	Once every 18 months
RI-6B, Revision 8	Containment Pressure Channel Calibration	Once every 18 months
RI-7, Revision 12	Low Pressure SIS Initiation Logic Channel Calibration	Once every 18 months
RO-97, Revision 13	Auxiliary Feedwater Automatic Initiation Test	Once every 18 months
RT-129, Revision 6	Functional Test of Bus 1C Undervoltage Relays.	Once every 18 months
RT-130, Revision 6	Functional Test of Bus 1D Undervoltage Relays	Once every 18 months
QO-6, Revision 40	Cold Shutdown Valve Tests	Once every 18 months
MO-7A-1, Revision 65	EDG 1-1	Once every month
MO-7A-2, Revision 61	EDG 1-2	Once every month
RO-12, Revision 31	Containment High Pressure and Spray System Tests	Once every 18 months
RO-28, Revision 25	Control Room/Technical Suppler Center Ventilation	Once every 18 months

C3.3 EVALUATION, ANALYSES AND RESULTS

The component categorization process is described in Section 4.0. Table C3.3a provides a numerical summary of the classification results specifically for Palisades.

Table C3.3a
Categorization Summary

a,c

Category	Number of Components

Figures C3-1, C3-2 and C3-3 illustrate where there is overlap in the integrated ESF/LOOP testing at Palisades. They are simplified illustrations and therefore depict only an approximation of overlap. They are not intended to provide engineering and system design details. 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

a,c

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

a.c

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

a,c

C4.0 PROBABILISTIC ASSESSMENT OF A STAGGERED STI RISK

The analysis for Palisades has not been updated due to resource limitations and the abbreviated completion schedule. Palisades will perform all required updates and additional analysis to support their plant-specific application at a later date.

Westinghouse performed a preliminary categorization and assessment of components tested by the Integrated ESF/LOOP test functions for Palisades. Palisades used the preliminary assessment as a foundation and starting point to perform the PRA analysis described in this Appendix. The categorization began with the testing matrix described in Section C3.0. The matrix was used to identify components whose reliability was to be demonstrated primarily or solely by the integrated ESF/LOOP test.

The Palisades PRA 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/LOOP test frequency. The actual changes to the model and the requantification of the model were performed by Palisades. The remainder of this section is derived from the risk analyses performed by Palisades as proof-of-principle.

This analysis evaluates the risk significance of extending the interval between performing the integrated ESF/LOOP testing implemented by Surveillance Tests RT-8C and RT-8D. The test interval would be changed from requiring both tests each refueling outage to conducting one test each refueling outage on a staggered basis. In addition, this analysis evaluates the capability and quality of the Palisades PRA 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 Modes 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 change in STI does not directly impact the frequency of events that dominate LERF. Also, the needed change does 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 (i.e., containment spray).

Methodology

The current Palisades PRA 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 resolved as part of the evaluation of the test interval extension to assure that modeling issues that could impact the results have been addressed. 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 [ ]^{a,c} 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 based 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., ΔCDF) that would result from the test interval extension. The ΔCDF was determined to establish the risk significance category of the proposed change.

C4.1 MODEL ANALYSIS

A review of the current Palisades PRA 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 PRA 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 model analysis found that a significant contribution (>95%) to the ΔCDF was the result of an assumption in the current PRA 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 the loss of instrumentation and the operator's inability to accurately control secondary cooling. However, the significant contributors to the ΔCDF 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 for 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 created 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 PRA model is [ ]^{a,c} per year. 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 [ ]^{a,c} to [ ]^{a,c} and relay basic events from [ ]^{a,c} per year. The CDF for these changes was [ ]^{a,c} per year.

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 [ ], seven (7) were added to the right [ ] 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 were developed strictly on the test interval calculation. The probabilities of those components that would be affected by

the extension of the test interval were doubled in a separate calculation. The sum of the probabilities of failures of the breakers and the sum of the probabilities for the relays for each channel were assigned to the surrogate events.

CASE 1: New Base Case

This case represents the development of the new baseline risk based on changes necessary to evaluate the test interval extension. The data changes for this case are listed below.

P-CBMA-152-106 was changed from [ ]^{a,c}
P-CBMA-152-202 was changed from [ ]^{a,c}
R-REMB-194-108 was changed from [ ]^{a,c}
R-REMB-194-211 was changed from [ ]^{a,c}
P-CBCC-SG-MA was added with a probability of [ ]^{a,c}
R-RECC-LOADSHED was added with a probability of [ ]^{a,c}
An operator action was added with a screening Human Error Probability (HEP) value of 0.1

The CDF for this case is [ ]^{a,c} per year. This CDF is the new baseline for determining the ΔCDF due to the test interval extension. This case adjusts the model to account for changes that need to be made to the model prior to evaluating the new test interval.

CASE 2: Test Interval Impact

For the second case, the basic event probabilities for the components affected by the extension of test interval were doubled. The changes to the model for this case are listed below.

P-CBMA-152-106 was changed from [ ]^{a,c}
P-CBMA-152-202 was changed from [ ]^{a,c}
R-REMB-194-108 was changed from [ ]^{a,c}
R-REMB-194-211 was changed from [ ]^{a,c}
P-CBCC-SG-MA was changed to [ ]^{a,c}
R-RECC-LOADSHED was changed to [ ]^{a,c}

The CDF for this case is [ ]^{a,c} per year. This CDF is the updated value resulting from the test interval extension.

The ΔCDF is the difference between the Case 2 CDF and the new base line CDF calculated in Case 1 or [ ]^{a,c} per year.

CASE 3: Risk Informed Impact

There are a few of the breakers that were assigned failure probabilities as a function of the RT-8C/RT-8D test interval and subsequently doubled, for which there is information that would support a more frequent detection interval for verifying the breaker open function. While these components are not tested by another surveillance test the breakers are for normally operating equipment that is part of a regular train rotation or infrequently changed for maintenance. If the failure probability of these breakers were recalculated based on the rotation schedule or the assumption that maintenance requirements result in breaker operation twice/year, the updated CDF would be [ ]^{a,c} per year. This would result in a ΔCDF of ~ [ ]^{a,c} per year.

P-CBMA-152-106 was changed from [ ]^{a,c}
P-CBMA-152-202 was changed from [ ]^{a,c}
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 [ ]^{a,c}. 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 actuation signal and would be most affected by the extended test interval (LOCA, MSLB, SGTR) 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	[ ]^{a,c}
Case 2a	[ ]^{a,c}
ΔCDF	[ ]^{a,c}
Case 3a	[ ]^{a,c}
ΔCDF	[ ]^{a,c}

The results are also impacted by a major assumption in the PRA model. For Station Blackout (SBO) Events, the current Palisades PRA 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 then 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 [ ]^{a,c} per year. The CDF from extending the test interval is [ ]^{a,c} per year. This results in a ΔCDF of [ ]^{a,c} per year.

C4.2 SCOPE OF PRA

The Palisades PRA is an at-power, internal events PRA. 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 PRA 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 PRA 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 PRA 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 PRA model.

C4.2.3 PRA Detail Needed for Change

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

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 with in defined group by a specified failure mode, i.e., all safety injection pumps fail to start on demand due to common causes. This approach is used throughout the Palisades PRA. 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 Palisades is configured, edited and analyzed with SAPHIRE.

C4.3 QUALITY OF PALISADES PRA

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

- Formal qualification program for the PRA staff
- Use of procedures to control PRA processes
- Independent reviews (checks) of PRA documents
- Comprehensive PRA Configuration Control Program
  - Quarterly plant change monitoring program
  - Process to control PRA 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 PRA Technical Positions
- Commitment of continuous quality improvement

C4.4 RESULTS AND CONCLUSIONS

Ninety-nine percent (99%) of the Palisades PRA cut sets involve a loss of offsite power and no ESF condition. The component failures that contribute to the ΔCDF (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 PRA model. The dominant contributors to the CDF are failures that prohibit the EDG breakers from closing. Including an operator action to recover from load shed failures would drop the ΔCDF 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 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 ΔCDF [ ]^{a,c} is considered to be of low safety significance.

C.5.0 DEFENSE-IN-DEPTH AND SAFETY MARGIN EVALUATION

The objective of the defense-in-depth evaluation is to show that there are no time dependent failure modes for the Category A components and to support the conclusion of the risk analyses that extending the STI for the Integrated ESF/LOOP test results in only minor changes in plant risk. The change in the plant risk is evaluated deterministically by performing plant specific Failure Modes and Effect Analysis (FMEA) and a no significant hazards evaluation on systems and Equipment that is tested solely by the integrated ESF/LOOP test. The analysis should address the following areas:

- Failure Mode,
- Failure Mechanism (cause),
- Failure Effects and Consequences,
- Safety Significance and impact on margin of safety.

The evaluation should show that there are no time dependent failure modes. If any time dependent failure modes are identified, the plant must ensure that a preventive maintenance program is established to remove the time dependent failure mode and to assure that the component's hazard rate remains constant. In addition, the time dependent failure mode must be included the plant risk model.

To maintain plant defense-in-depth as described in the plant licensing basis, the licensee must ensure that there will be no significant increase in unavailability for a single ESF train when the integrated ESF/LOOP testing interval is doubled, i.e., changed to every other refueling outage. The deterministic analysis provides the necessary balance between risk and deterministic arguments required by RG 1.174.

C5.1 Failure Modes and Effects Analysis

The defense-in-depth analysis for extending a STI requires analysis of time-dependent failure modes. to identify any of the following:

- If the performed surveillance test covers all failure modes,
- If any of the identified failure modes are time dependent, meaning that the rate of change varies with time (i.e., heat exchanger fouling, time delay relay drift, etc.),
- If other plant activities, such as maintenance program or surveillance testing have identified a time-dependent failure mechanism,
- If a preventive maintenance program has been established to assure that the components hazard rate remains constant,
- If the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact,
- If any aspect of implementing an increased surveillance interval would introduce a potential for common cause failure.

C5.2 Significant Hazards Evaluation

The operability of the ESCS instrumentation and interlocks must ensure that when parameters monitored by each channel reaches its setpoint, an appropriate level of reliability of ESF instrumentation with sufficient redundancy is maintained to perform its intended functions. The operability of the ESF system is required to provide the overall reliability, redundancy, and diversity assumed available in the plant design for protection and mitigation of accident and transient conditions. For the above reasons, it is important that a safety evaluation be performed that considers each relevant failure mode against the possible impact on ESF system capability to perform its intended functions. Also, the evaluation must consider that at no time is the defense-in-depth of ESF system compromised, and it will function as described in the plant licensing bases.

The significant hazard analysis should include the following:

- Consequences of the identified failure mode,
- Safety significance of the failure mode,
- Effect of the failure mode on ESF actuation,
- If a preventive maintenance program has been established to assure that the components hazard rate remains constant,
- If the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact.

C.5.3 Palisades Category A Components

An assessment of Category A ESF components will be required to implement staggered integrated ESF surveillance testing at Palisades. This assessment will support RG 1.174 and consider relevant safety margins and defense in depth attributes including consideration of success criteria as well as equipment functionality, reliability, and availability. The analysis will be based on the methodology shown in Section 5.0 of this report and will incorporate the actual design, construction, operation and maintenance practices in effect at Palisades. The following is a list of example Category A components installed at Palisades that will be included in the assessment.

- Under Voltage Relays: 127-1/X1, 127-1/X2, 127-7X1, 127-7X2,
- Load Shed Relays: 194-108, 94-1909, 94-1109A, 94-1109B,
- Incoming breaker to bus 1C, 152-105 (UV trip),
- P-40A, Dilution Water Pump, breaker 152-102 (UV and SIS trip),
- Pressurizer Heater breaker, 152-302 (load shed).

C6.0 OVERALL CONCLUSION

Results of the Palisades risk analysis show that the change in core damage frequency and large early release fraction are insignificant and fall well within the acceptance criteria of RG 1.174. These results support implementing a staggered test basis for the integrated ESF/LOOP test at Palisades. An overall evaluation of the acceptability of this change, taking into consideration the deterministic assessment of the Category A components, will be included in the plant specific application.

APPENDIX D

APPLICATION OF WCAP-15830-NP TO WATERFORD STEAM ELECTRIC STATION UNIT 3

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

D1.0 ABSTRACT

Pressurized Water Reactor Owners Group (PWROG) CEOG Task 2016, Staggered Integrated ESF/LOOP Testing used a risk-informed, performance based approach to demonstrate that changing the integrated ESF/Loop test (termed the Emergency Diesel Generator (EDG)/Engineered Safety Features (ESF) test at WSES-3) from once per cycle on a sequential basis to once every other cycle on a staggered test basis results in a negligible change in risk. Currently, integrated EDG/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 basis for this change is the fact that the integrated EDG/ESF test is not the primary or sole operability test for most of the components/functions tested by the integrated EDG/ESF test. Other Technical Specification (TS) required surveillance procedures are performed on many of these components and functions on the same or a more frequent basis. Therefore, there may be considerable overlap exists between the integrated EDG/ESF test and other tests.

The approach used to demonstrate that the change in integrated EDG/ESF testing is acceptable may be summarized as follows. The failure probabilities for the components/functions that are tested only by the integrated EDG/ESF test were adjusted to reflect the increase in the test interval for the individual trains. The overall risk associated with the change was recalculated, and compared to the base case risk. In some cases, it was possible to develop a reasonable deterministic basis to demonstrate that the component failure mode addressed by the integrated EDG/ESF test was not risk-significant. These components were exempt from further Probabilistic Risk Assessment (PRA) review and analysis.

The methodology is consistent with NEI 04-10, Risk-Informed Technical Specifications Initiative 5b, "Risk-Informed Method for Control of Surveillance Frequencies". NEI 04-10 uses a risk-informed, performance-based approach to establish the surveillance frequency, which is consistent with the philosophy of NRC RG 1.174 for PRA methods to determine the risk impact of the revised intervals. Sensitivity studies were performed on important PRA parameters. PRA technical adequacy is addressed through NRC Regulatory Guide 1.200, which references the ASME PRA Standard, RA-S-2005b, for at-power, internal events. External events and shutdown are not considered for this evaluation.

This Appendix demonstrates the application of a staggered integrated EDG/ESF testing at Waterford Unit 3 (WSES-3). It includes the following elements of the process: procedure review, component categorization, component evaluation and risk analyses. The deterministic assessment of Category A components (Section 5.0 of the main report) is not included in the demonstration, but will be addressed by the applicant in a plant-specific submittal. The WSES-3 Technical Specification Surveillance Requirements addressed by the integrated EDG/ESF test are listed in Table D2.3a.

The following is a summary of the method employed to determine the impact of extending the interval between successive integrated EDG/ESF tests on a given train from every refueling interval [ ] months to every other refueling interval on a staggered basis [ ] months. The first part consisted of a review of WSES-3 procedures in conjunction with the matrix development. The second part consisted of the categorization of components and functions tested by the integrated EDG/ESF test. The third part included the preliminary PRA review and Category A component sub-categorization. The fourth part was finalization of the PRA review and categorization. The PRA model was updated to explicitly reflect the 18 month test interval. The PRA model reflecting the [ ] month test interval was quantified, then re-quantified with the failure rates corresponding to a [ ] month test interval. The difference between the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) corresponds to the change in risk for extending the Surveillance Test Interval (STI). The fifth part, the Defense-in-Depth Evaluation,

was not completed for this demonstration. The applicant must include the complete evaluation in the plant specific application. The last part is an overall assessment of the acceptability of the change in STI.

The risk contribution associated with extending the interval between successive integrated EDG/ESF tests on a given train from every refueling interval [ ] months to every other refueling interval on a staggered basis [ ] months has been quantitatively evaluated using the current WSES-3 PRA model. The calculated increase in Core Damage Frequency (ΔCDF) due to increasing the interval of integrated EDG/ESF testing on a given ESF train from once per normal refueling cycle [ ] months, with sequential testing, to once every other refueling cycle [ ] months, with staggered test basis, is [ ]^{a,c} per year. The estimated change in Large Early Release Frequency (ΔLERF) is [ ]^{a,c} per year. This change in risk is within the RG 1.174 criteria of 1E-06 per year for the CDF and 1E-07 per year for the LERF.

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

D2.0 BACKGROUND

The safety related instrumentation and controls of the Engineered Safety Feature Systems (ESFS) include the following: (1) 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) arrangement of components that perform protective actions after receiving a signal from either the ESFAS or the operator. A Combustion Engineering (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 (RPS), and is contained in the same physical enclosure. The combination of the ESFAS and RPS is designated the 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 the 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 de-energizes the bistable output relay. The bistable output relay de-energizes 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. 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 de-energization 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 de-energizes the seal-in relays of its associated channel. The seal-in relays ensure that the signal is not automatically removed once initiated.

Receipt of two selective SIAS initiation signals will de-energize 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.

There are only two initiating circuits in each MSIS channel (steam generator #1 and steam generator #2 pressure), 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 disrupting normal plant operation.

D2.1.2.2 Group Actuation

The components in the safety injection system are separated into groups; separation is made such that actuation of a group will not affect normal plant operation. Components of each group are actuated by a 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 4.16kV ESF buses are each supplied by a dedicated Emergency Diesel Generator (EDG). The Table D2.2.1a 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 4.16kV 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

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, 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 SIAS or by the undervoltage relay on the respective 4.16kV ESF bus. Sequencing equipment is provided to control 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 requirements are 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 de-energized, 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 SO 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. Timing of the change of state can be determined by reviews of the Sequence of Events Recorder from the plant monitoring computer.

D2.3 CURRENT TECHNICAL SPECIFICATIONS

Table D2.3a lists the Technical Specification Surveillance Requirements (SR) that applies to integrated EDG/ESF testing at WSES-3.

Table D2.3a
Existing Surveillance Test Intervals

SR	Surveillance Requirement	Interval
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.	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 de-energization 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 de-energization 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 not 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 CHANGES TO TECHNICAL SPECIFICATIONS

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

Table D2.4a
Change in Surveillance Test Intervals

SR	Surveillance Requirement	Interval
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 $\geq$ 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 de-energization 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 $\geq$ 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 de-energization of emergency busses with load shedding.	36 months on a Staggered Test Basis
4.8.1.1.2.e.7	Verify auto connected loads not 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 EDG/ESF Test (OP-903-115 and OP-903-116)

The Integrated EDG/ESF test is performed on A and B engineered safeguards trains, one train at a time, once every refueling interval (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, and 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 EDG/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. 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 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 EDG/ESF test and other tests, as well as a preliminary PRA evaluation and assessment. The preliminary PRA assessment performed by Westinghouse provided the foundation for the plant specific PRA calculation originally performed by WSES-3 in 2002. The WSES-3 PRA model was updated in 2007 and is referred to as Revision 3, Change 3.

The procedure review portion of the database used to develop the matrix is defined Table D3.1a. PRA 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.	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 PRA 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 main 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 EDG/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. The component end condition following the test was entered under each applicable function. 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 EDG/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 EDG/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 candidates other test procedures provided by WSES-3, Westinghouse made an assessment as to whether or not the integrated EDG/ESF test was the sole/primary test for each component. An initial categorization of the components was then made. These categories are defined as follows:

a,c

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

D3.2 TEST PROCEDURE REVIEW

Table D3.2a provides a list of the WSES-3 surveillance procedures included in the review, including the integrated EDG/ESF procedures. These procedures were reviewed by Westinghouse to develop the EDG/ESF surveillance test procedure matrix.

Table D3.2a
EDG/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
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 described in Section 4.0 of this report was used to develop the classification results for WSES-3 shown in Table D3.3a.

Table D3.3a
Categorization Summary for Waterford Unit 3

a,c

Category	Number of Components

Figures D3.3-1, D3.3-2 and D3.3-3 illustrate requirements that create an overlap in integrated EDG/ESF testing at WSES-3. These are simplified illustrations and therefore depict only a rough approximation of overlap; they are not intended to provide engineering and system design details. 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 D3.3-1 illustrates testing that addresses SIAS actuation. Figure D3.3-2 covers undervoltage sensing and load shedding. Figure D3.3-3 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 D3.3-1
ESFAS Surveillance Procedures – Waterford Unit 3

a.c

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

a,c

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

a,c

D4.0 PROBABILISTIC RISK ASSESSMENT FOR WSES-3

Westinghouse performed a preliminary categorization and assessment of components tested by the integrated EDG/ESF test for WSES-3. WSES-3 used the preliminary assessment as a foundation to perform the PRA 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 or solely by the integrated EDG/ESF test.

The WSES-3 PRA Master List of basic events was reviewed to determine if and how the model addresses each 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 basic event frequencies or modeling details that would be needed in order to quantify the change in risk associated with the change in the integrated EDG/ESF test frequency. The actual changes to the model and quantification of the model were initially performed by WSES-3. Westinghouse performed the requantification of the model using Revision 3, Change 3 of the WSES-3 internal events PRA model for Revision 1 of this document. The Revision 3, Change 3 internal events model is then integrated with the Large Early Release Frequency (LERF) model developed by WSES-3 in accordance with the NUREG/CR-6595 methodology.

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

The following are key inputs and assumptions associated with the WSES-3 analyses:

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

Component functions tested solely by integrated EDG/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.

There are a number of component load shed breakers attached to the buses. It was assumed that failure of two or more of these breakers to open following a load shed signal would result in failure of the associated EDG due to overload. It is assumed that the number of combinations of two or more independent failures of component breakers to trip on Loss of Offsite Power (LOOP) could be calculated using the binomial theorem for two or more of the component breakers failing. (Note: The standby failure rate model was used to calculate the average unavailability for the individual breakers.)

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 EDG/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 Station Service Distribution (SSD) Breakers for Buses 312A, 312B, 313A, 313B, 314A and 314B. This is already assumed for the Revision 3, Change 3 WSES-3 PRA 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 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 is 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 EDG/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 the 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. For a given test interval, the CCF unavailability contribution for a staggered test interval is approximately one-half of the CCF unavailability contribution for sequential testing at the same interval. For this report, the test interval is doubled, but the test is performed on a staggered basis. As a result, the CCF probabilities remain constant for an 18 month sequential test interval that changes to the 36 month staggered test interval.

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 opposed 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.

D4.1 MODEL ANALYSIS

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

Determination of Tested Components

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

Component Classification

Westinghouse identified the components/functions that are only tested during the integrated EDG/ESF test and compared them to the PRA 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. Category A components were further divided into the following four subcategories to delineate the actions required to support the determination of the change in CDF and LERF.

a,c

The functions and components identified by Westinghouse were checked against the PRA 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.

D4.1.1 Model Changes and Quantification of Changes

Integration of Changes

The WSES-3 PRA model was then updated to incorporate the changes required in order to model all the components and functions for the nominal 18 month testing frequency.

Quantification of CDF

The model was quantified two times in order to determine the increase in CDF and LERF due to changes in the test 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 a second time with the failure rates corresponding to a 36 month test interval.

Change in CDF Determination

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

Quantification of LERF

The change in LERF was determined using the LERF fault tree model developed for WSES-3 based on NUREG/CR-6595 methodology. This LERF fault tree was integrated with the internal events fault tree that represented the 18 month test interval. The integrated LERF fault tree was quantified to determine the LERF with the failure rates representative of the 18 month test interval. The LERF model was then quantified a second time with the failure rates corresponding to a 36 month test interval.

Change in LERF Determination

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

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. Westinghouse requantified the risk for this study.

Integration of Changes

Failure to shed – Individual Components

There are many components for which the failure to shed were not included in the WSES-3 PRA model. In order not to complicate the WSES-3 PRA model, the failure to shed all the components is combined into two basic events that would cause a failure-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 PRA model, Revision 3, Change 3.

The failure to shed basic events was added to the EDG fail-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 Blackout (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 were 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 PRA 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.

Table D4.1.1
Failure to Shed A Train Components

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
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 CVCEBKR31A-5C
36	CVCEBKR31AB-4C	CHARGING PUMP AB CVCEBKR31AB-4C
37	DC-EBKR-311A-14D	BATTERY CHARGER A1 DC-EBKR-311A-14D

Table D4.1.1
Failure to Shed A Train Components

No.	Associated Breaker	Component Short Description
38	DC-EBKR-311AB-2D	BATTERY CHARGER AB1 DC-EBKR-311AB-2D
39	DC-EBKR-311AB-2H	BATTERY CHARGER AB2 DC-EBKR-311AB-2H
40	DC-EBKR-312A-3B	BATTERY CHARGER A2 DC-EBKR-312A-3B
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	EGLEBKR-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
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 ID-EBKR31A-8C
75	ID-EBKR31AB-3B	COMPUTER SUPS BYPASS SUPPLY ID-EBKR31AB-3B
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 [ ]^{a,c} per demand for an 18 month surveillance interval. The failure probability for the having two or more failures out of 87 components is [ ]^{a,c} per demand for a 36 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 CC EBKR315B-4M
18	CC EBKR315B-5F	DRY COOLING TOWER B FAN 9 CC EBKR315B-5F
19	CC EBKR315B-5M	DRY COOLING TOWER B FAN 10 CC EBKR315B-5M
20	CC EBKR315B-7F	DRY COOLING TOWER B FAN 11 CC EBKR315B-7F
21	CC EBKR315B-7M	DRY COOLING TOWER B FAN 12 CC EBKR315B-7M
22	CC EBKR315B-8F	DRY COOLING TOWER B FAN 13 CC EBKR315B-8F
23	CC EBKR315B-8M	DRY COOLING TOWER B FAN 14 CC EBKR315B-8M
24	CC EBKR315B-9F	DRY COOLING TOWER B FAN 15 CC EBKR315B-9F
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 CVCEBKR31B-6C
34	DC-EBKR-311B-14D	BATTERY CHARGER B1 DC-EBKR-311B-14D
35	DC-EBKR-312B-3B	BATTERY CHARGER B2 DC-EBKR-312B-3B
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

Table D4.1.2
Failure to Shed B Train Components

No.	Associated Breaker	Component Short Description
40	EGLEBKR312B-5D	EG B LUBE OIL HEATER EGL-EBKR-312B-5D
41	HT-EBKR-312B-5M	CVCS SYSTEM B TRACING HT-EBKR-312B-5M
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 NORMAL FEEDER ID-EBKR312B-2F
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 for failure of two or more load shed breakers was calculated using the binomial distribution. The failure probability for having two or more failures out of 76 components is [ ]^{a,c} per demand for an 18-month surveillance interval. The failure probability for the having two or more failures out of 76

components is [ ]^{a,c} per demand for a 36 month surveillance interval. (Note: The average unavailability, failure probability for a breaker was calculated using the standby failure model.)

The CCF failure rate for the 18 month surveillance interval would be [ ]^{a,c} per demand using the CCF beta factor of 0.2. The CCF Beta factor was implemented as a lambda factor in the basic event database multiplied with the fail-to-shed basic event probability. These values would be the same value for both trains of safety related power.

For a given test interval, the CCF unavailability contribution for a staggered test interval is approximately one-half of the CCF unavailability contribution for a sequential testing with the same test interval. For the program developed in this report, the test interval is doubled, but the test is performed on a staggered basis. As a result, the CCF probabilities remain constant for an 18 month sequential test interval to the 36 month staggered test interval.

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 or 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 were explicitly included in the model. The CCF probabilities between the 3A and 3B buses will remain constant for the 18 month to the 36 month interval.

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 18 month surveillance interval the failure rate would be [ ]^{a,c} per demand. For the 36 month interval the failure rate would be [ ]^{a,c} per demand. The new bus fails to shed events are listed in Table D4.1.4.

The beakers 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 18 month surveillance interval would be [ ]^{a,c} per demand using a CCF beta factor of 0.2. The CCF probability for the 36 month surveillance interval would be [ ]^{a,c} per demand, which is the same as the 18 month test interval.

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 18 month surveillance interval was [ ]^{a,c} per demand. This is the [ ]^{a,c} per demand failure rate times the ten relays for the A train. The 36 month failure rate was twice the 18 month failure rate to account for the increase in time between the surveillances.

The B sequencer has nine 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, ERETIMESBX, 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 18 month surveillance interval was [ ]^{a,c} per demand. This is the [ ]^{a,c} per demand failure rate times the nine relays for the B train. The 36 month failure rate was twice the 18 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 sequencing-on would result in the failure to provide the PRA 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 PRA 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

a,c

Cooling Tower, Plant Condition and Test Interval	Basic Event Name	Binomial Failure Probability	Common Cause Failure probability	Total Failure Probability
		(per demand)	(per demand)	(per demand)

Quantification of Changes in CDF

The WSES-3 internal events PRA model was quantified twice. Once with the 18 month failure probabilities for the basic event tested by the integrated EDG/ESF surveillance, and once with the 36 month failure probabilities. The model with the 18 month failure probabilities resulted in a CDF of [ ]^{a,c} per year. The model with the 36 month failure probabilities resulted in a CDF of [ ]^{a,c} per year.

Change in CDF Determination

The resulting change in CDF is the difference between the 36 month CDF and 18 month CDF. The difference is [,]^{a,c} which is an increase in CDF of [ ]^{a,c} per year.

Quantification of Changes in LERF

The WSES-3 internal events LERF model was quantified twice. Once with the 18 month failure probabilities for the basic event tested by the integrated EDG/ESF surveillance, and once with the 36 month failure probabilities. The model with the 18 month failure probabilities resulted in a LERF of [ ]^{a,c} per year. The model with the 36 month failure probabilities resulted in a LERF of [ ]^{a,c} per year.

Change in LERF Determination

The change in LERF is [,]^{a,c} which is an increase in LERF of [ ]^{a,c} per year.

D4.1.2 Sensitivity Study

A notable assumption made in a PRA model is that all components in the pant have a constant failure rate during their scheduled testing cycle. All Category A components considered in this evaluation at WSES-3 are on an 18 month simultaneous test cycle (simultaneous meaning both trains of equipment are tested on the same schedule). Extending the IESF test interval to 36 months for these components will increase the probability of failures due to component aging. This sensitivity study approximates the impact of aging for components tested on a 36 month staggered testing cycle.

The affect of aging can be approximated using insights from the product hazard rate Bath-Tub Curve, illustrated in the figure below. As mentioned above, PRA models assume that the components in the plant are on the flat portion of this curve. However, this assumption has only been shown to be valid for the first 24 months of a test interval (based on the 24 month test cycle used at Calvert Cliffs). For this study, this assumption is revised to reflect a constant hazard rate for the first 24 months of the test interval. After the first 24 months, the hazard rate is adjusted as the component enters the increasing hazard rate portion of the Bath-Tub Curve.

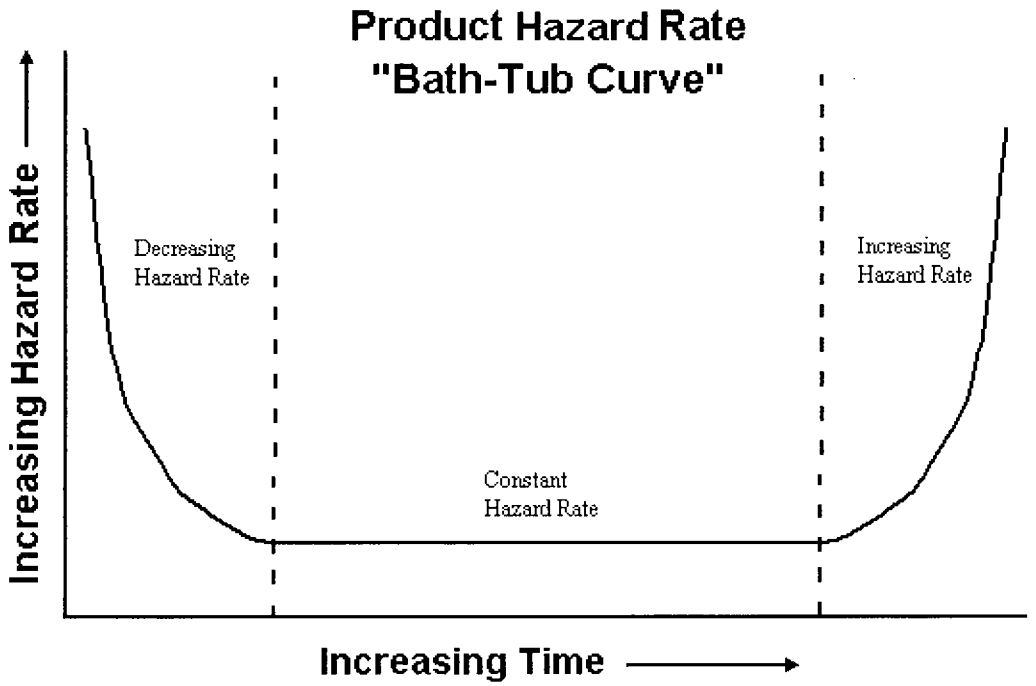


Figure D.4.1-1: Graphical Representation of the Component Hazard Rate Bath-Tub Curve

To estimate the impact of aging related failures, the failure rate of a given component can be increased during the final 12 months of the testing interval. Figure D.4.1-1 shows the increase in failure rate considered for this sensitivity. As shown, the nominal component failure rate (the component hazard rate multiplied by time) is assumed for the first 24 months. After 24 months, the failure rate doubles during the next 6 months. For the final 6 months of the testing cycle, the failure rate is assumed to be six times its nominal value.

a,c

Figure D.4.1-2: Probability of Failure for the Sensitivity Evaluation

The information shown in Figure D.4.1-2 cannot simply be applied to a basic event in a PRA model. The events in a PRA consider the average unavailability of a component which can be calculated as:

$$\overline{U} = \int_0^{\tau}\left(\frac{\lambda\, t}{\tau}dt\right) = \frac{\lambda\,\tau}{2}$$

where, $\overline{U}$ is the Average Unavailability
λ is the failure rate
τ is the testing interval, and
t is time

From this equation the average unavailability of the following cases can be calculated:

- 18 month testing cycle at a constant failure rate:

$$\overline{U} = \int_0^{18}\left(\frac{\lambda\, t}{18}dt\right) = 9\lambda$$

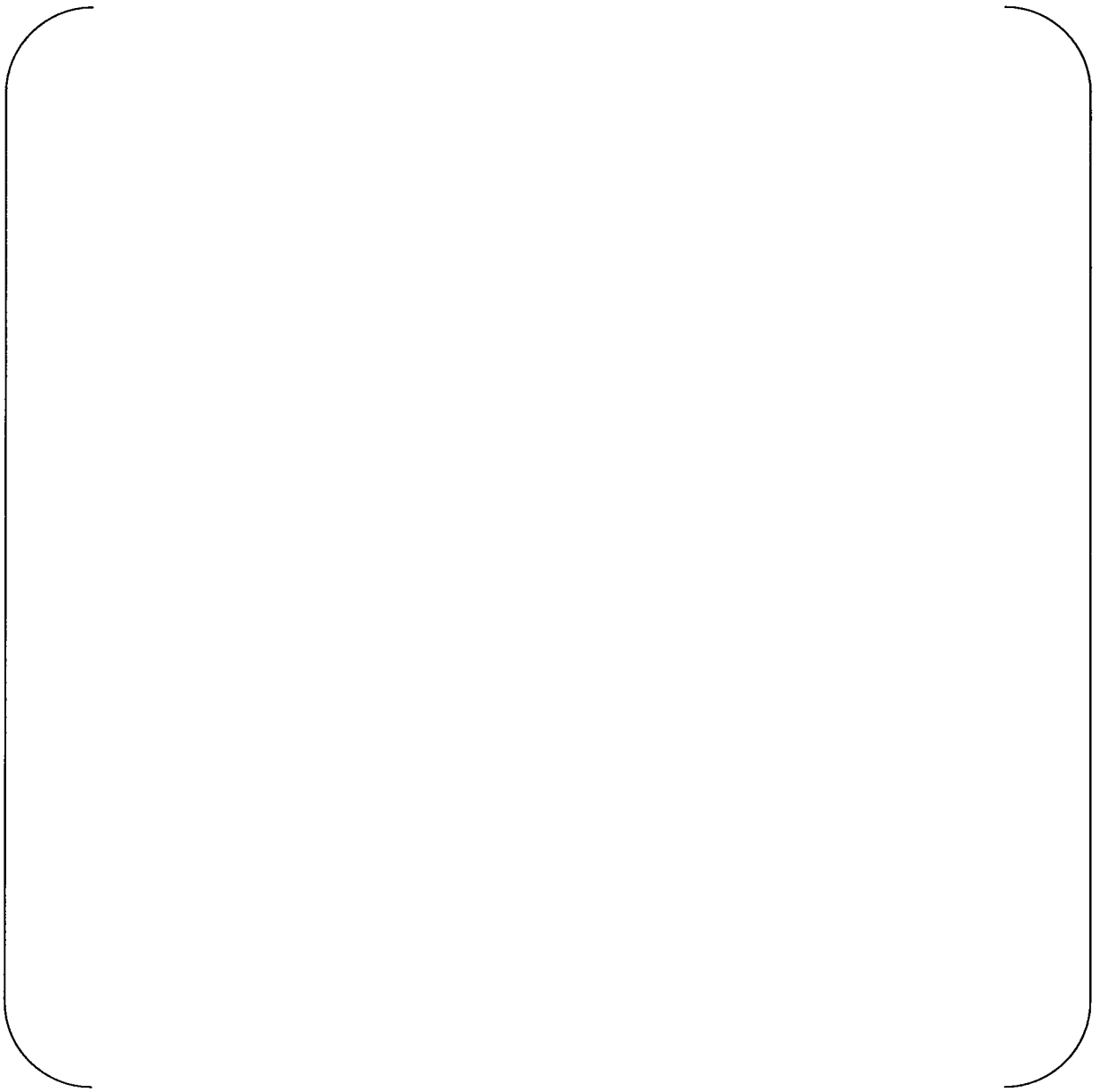
- 36 month testing cycle at a constant failure rate:

$$\overline{U} = \int_0^{36} \left(\frac{\lambda t}{36} dt \right) = 18\lambda$$

This shows that increasing the testing interval by a factor of 2 results in an average unavailability two times the original unavailability. This is consistent with the factor of 2 that was used to evaluate the impact of doubling the testing interval.

- 36 month testing cycle for the sensitivity case with the variable failure rate represented in Figure D.4.1-2:

a,c



D4.2 SCOPE OF PRA

The WSES-3 Revision 3, Change 3 PRA model is an at-power, internal-events PRA model that has an integrated LERF model based on NUREG/CR-6595 methodology. 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 internal Condition Reports. These capture important plant failure modes, events, and trends.

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

D4.2.2 Shutdown Risk Assessment

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

D4.2.3 PRA Detail Needed for Change

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

D4.2.3.1 Modeling and Quantification

Common Cause

PWROG 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 trip.

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 FORTE engine.

D4.2.3.2 Truncation Limits

The truncation for CDF was set to 1.0E-10, which is three to four orders of magnitude below the most significant sequences identified in the analysis. The truncation for LERF was set to 1.0E-11.

D4.3 QUALITY OF WATERFORD UNIT 3 PRA

Entergy Operations utility personnel have constructed the Revision 3, Change 3 PRA model with a strong commitment toward developing a complete and accurate PRA. This commitment can be seen through the following elements:

- Formal qualification program for the PRA staff
- Use of procedures to control PRA processes
- Independent reviews (checks) of PRA documents
- Comprehensive PRA Configuration Control Program
  - Process to control PRA 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 PRA Technical Positions
- Commitment of continuous quality improvement

The Revision 2, Change 1 WSES-3 model was peer reviewed in January 2000. The Revision 3, Change 3 WSES-3 PRA model for this analysis contains several refinements. Considering the scope, level of detail, processes and peer review results, the Revision 3, Change 3 WSES-3 PRA model is sufficient to support a technically defensible and realistic evaluation of the risk associated with the evaluation that was performed to demonstrate proof-of-principle.

D4.4 PRA SOFTWARE

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

D4.4.1 CAFTA

CAFTA is a commercial software 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 resulting cutsets.

D4.4.2 PRAQuant

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

D4.4.3 FORTE

FORTE is a 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 OF RISK ANALYSIS

The calculated increase in Core Damage Frequency (ΔCDF) due to increasing the surveillance interval from an 18 month interval to a 36 month staggered test interval is [ ]^{a,c} per year.

The estimated change in Large Early Release Frequency (ΔLERF) is [ ]^{a,c} per year.

D.5.0 DEFENSE-IN-DEPTH AND SAFETY MARGIN EVALUATION

The objective of the defense-in-depth evaluation is to show that there are no time dependent failure modes and to support the conclusion of the risk-informed basis that extending the TS surveillance test interval for the integrated EDG/ESF test results in an insignificant change in plant risk. The impact on plant risk is evaluated deterministically by performing plant specific Failure Modes and Effect Analysis (FMEA) and a significant hazards evaluation on Systems/Equipment (S/E) that is tested solely by the integrated EDG/ESF test. The plant specific analysis evaluates the following for all Category A components:

- Failure Mode,
- Failure Mechanism (cause),
- Failure Effects and Consequences
- Safety Significance and impact on margin of safety

The evaluation determined whether or not there are time dependent failure modes. If any time-dependent failure modes are identified, the plant must ensure that a preventive maintenance program is established to remove the time dependent failure mode and to assure that the component's hazard rate remains constant. Any time dependent failure mode must also be included the plant risk model.

To maintain plant defense-in-depth as described in the plant licensing basis, the licensee must ensure that there will be no significant increase in unavailability for a single ESF train when the integrated EDG/ESF testing interval is doubled, i.e., changed to every other refueling outage. The deterministic analysis is needed to reinforce the conclusions of the corresponding risk informed analysis performed to support the change. It provides the necessary balance between risk and deterministic arguments required by RG 1.174 (Reference 2). A defense-in-depth analysis consists of two basic parts: 1) a Failure Modes and Effects Analysis and 2) a Significant Hazards Analysis.

D.5.1 Failure Modes and Effects Analysis

The defense-in-depth analysis for extending a TS surveillance interval requires analysis of time-dependent failure modes. This is done by performing a Failure Modes and Effects Analysis (FMEA) on each component to identify:

- If the surveillance test performed covers all failure modes,
- If any of the identified failure modes are time dependent, e.g., heat exchanger performance that degrades with time or drift in the setting of a time delay relay,
- If other plant activities, such as maintenance program or surveillance testing have identified a time dependent failure mechanism,
- If a preventive maintenance program has been established to assure that the components hazard rate remains constant,
- If the time dependent failure rate for the affected component has been included in the single ESF train risk model to account for the risk impact.
- If any aspect of implementing an increased surveillance interval would introduce a potential for common cause failure.

D.5.2 Significant Hazards Evaluation

The operability of the ESFAS instrumentation and interlocks must ensure that when parameters monitored by each channel reaches its setpoint, an appropriate level of reliability of ESF instrumentation with sufficient redundancy is maintained to perform its intended functions. The operability of the ESF system is required to provide the overall reliability, redundancy, and diversity assumed available in the plant design for protection and mitigation of accident and transient conditions. For these reasons, it is important that a safety evaluation be performed that considers each relevant failure mode against the possible impact on ESF system capability to perform its intended functions. Also, the evaluation must consider that at no time is the defense-in-depth of ESF system compromised, and it will function as described in the plant licensing bases.

The significant hazard analysis should include the following:

- Consequences of the identified failure mode,
- Safety significance of the failure mode,
- Effect of the failure mode on ESF actuation,
- Confirmation that the effect of the failure on ESFAS functionality does not create the possibility of a new or different kind of accident from any accident previously evaluated, and
- Confirmation that the failure does not involve a significant reduction in a margin of safety.

D5.3 Waterford Unit 3 Category A Components

An assessment of Category A ESF components will be required to implement staggered integrated ESF surveillance testing at WSES-3. This assessment will support RG 1.174 and consider relevant safety margins and defense in depth attributes including consideration of success criteria as well as equipment functionality, reliability, and availability. The analysis will be based on the methodology shown in Section 5.0 of this report and will incorporate the actual design, construction, operation and maintenance practices in effect at WSES-3. The following is a list of example Category A components installed at WSES-3 that will be included in the assessment.

- Under Voltage Relay 27, ABB Model 411T5375-L,
- EDG A Sequencer Relay, S61X, Time-Delay Pick Up (TDPU) Relay, Agastat Model E7000,
- MCC-312A Safety to Non-safety tie, Breaker SSDEBKR312A-8M.

D6.0 OVERALL CONCLUSION

Results of the Waterford Unit 3 risk analysis show that the change in CDF and LERF fraction are insignificant and fall well within the acceptance criteria of RG 1.174. These results support implementing a staggered test basis for the integrated EDG/ESF tests at WSES-3. An overall evaluation of the acceptability of this change, taking into consideration the deterministic assessment of the Category A components, will be included in the plant specific application.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355