OCRWM	DESIGN CALCULATION OR ANALYSIS COVER SHEET		1. QA: QA 2. Page 1					
3. System Electrical		4. Document Identifier 100-PSA-EE00-00100-000-00A						
5. Title Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System								
6. Group Preclosure Safety Assessment								
7. Document Status Designation ☒ Preliminary ☐ Final ☐ Cancelled								
8. Notes/Comments								
Attachments			Total Number of Pages					
Attachment A Electrical Power Distribution System Architecture and Fault Tree Model - Side A			34					
Attachment B Fault Tree Model - Side B			14					
RECORD OF REVISIONS								
9. No.	10. Reason For Revision	11. Total # of Pgs.	12. Last Pg. #	13. Originator (Print/Sign/Date)	14. Checker (Print/Sign/Date)	15. QER (Print/Sign/Date)	16. Approved/Accepted (Print/Sign)	17. Date
00A	Initial Issue	104	B-14	N. Ramirez <i>N. Ramirez</i> 12-16-04	S.F. Deng <i>S.F. Deng</i> 12/16/04	S. Castro <i>Sandra Castro</i> 12/16/04	D.C. Richardson <i>Dennis Richardson</i>	12/16/04

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
<u>ACRONYMS</u>	7
<u>1. PURPOSE</u>	9
<u>2. QUALITY ASSURANCE</u>	9
<u>3. USE OF COMPUTER SOFTWARE</u>	9
<u>3.1 SOFTWARE APPROVED FOR QUALITY ASSURANCE WORK</u>	9
<u>3.2 OTHER SOFTWARE</u>	10
<u>4. INPUTS</u>	10
<u>5. ASSUMPTIONS</u>	11
<u>6. ANALYSIS</u>	13
<u>6.1 OBJECTIVE</u>	13
<u>6.2 METHODOLOGY</u>	13
<u>6.2.1 Step One: Identify Top Event to be Analyzed</u>	13
<u>6.2.2 Step Two: Understand the System</u>	13
<u>6.2.3 Step Three: Make a Logic Model</u>	14
<u>6.2.4 Step Four: Assess the Probability of Basic Events</u>	15
<u>6.2.5 Step Five: Perform Common-Cause Failure Analysis</u>	16
<u>6.2.6 Step Six: Interpret Qualified and Quantified Results</u>	18
<u>6.3 FAULT TREE ANALYSIS</u>	18
<u>6.3.1 Electrical Power Distribution System Description</u>	19
<u>6.3.2 Fault Tree Logic Model</u>	21
<u>6.3.3 Basic Events Quantification</u>	34
<u>6.3.4 Common-Cause Failure Analysis</u>	38
<u>6.4 FAULT TREE ANALYSIS RESULTS</u>	40
<u>7. SENSITIVITY ANALYSIS</u>	42
<u>7.1 FTA OF ENTIRE POWER GRID WITH EMERGENCY POWER</u>	43
<u>7.2 FTA OF ONE SIDE OF GRID WITH EMERGENCY POWER</u>	45
<u>7.3 FTA OF ONE SIDE OF GRID WITH NO EMERGENCY POWER</u>	47
<u>7.4 FTA OF EMERGENCY POWER ONLY–TWO SIDES</u>	49
<u>7.5 FTA OF EMERGENCY POWER ONLY – ONE SIDE</u>	51
<u>8. CONCLUSIONS AND RECOMMENDATIONS</u>	53
<u>9. REFERENCES</u>	55
<u>9.1 DOCUMENTS CITED</u>	55
<u>9.2 CODES, STANDARDS, REGULATIONS AND PROCEDURES</u>	56

CONTENTS (Continued)

	Page
<u>ATTACHMENT A</u> <u>ELECTRICAL POWER DISTRIBUTION SYSTEM ARCHITECTURE AND FAULT TREE MODEL - SIDE A</u>	A-1
<u>ATTACHMENT B</u> <u>FAULT TREE MODEL - SIDE B</u>	B-1

FIGURES

	Page
<u>1. CCF Input to an OR-Gate</u>	16
<u>2. CCF Input to an AND-Gate</u>	17
<u>A-1. Electrical Power Distribution System for the Monitored Geologic Repository</u>	A-3
<u>A-2. Electrical Power Distribution from LC A and LC B to Supply and Exhaust Fan Motors (Assumption 5.7)</u>	A-5
<u>A-3. Normal 125V DC Power Distribution System</u>	A-7
<u>A-4. Emergency 125V DC Power Distribution Systems</u>	A-9
<u>A-5. FT Model of the Electrical Power Distribution System with no Emergency Power</u> ..	A-11
<u>A-6. Subtree DISCONNECT_SWGRE A</u>	A-13
<u>A-7. Subtree BUS_SWGRE A</u>	A-15
<u>A-8. Subtree SWYDA_SWGRE A</u>	A-17
<u>A-9. Subtree CBUS_SWYDA</u>	A-19
<u>A-10. Subtree CBUS_SWYDB</u>	A-21
<u>A-11. Subtree LO SP_SWYDA</u>	A-23
<u>A-12. FT Model of the Normal 125V DC Distribution System</u>	A-25
<u>A-13. FT Model of the Emergency 125V DC Distribution System</u>	A-27
<u>A-14. FT Model of the Emergency Diesel Generator A</u>	A-29
<u>A-15. FT Model of Entire Power Grid with Emergency Power</u>	A-30
<u>A-16. FT Model of One Side of Power Grid with Emergency Power</u>	A-31
<u>A-17. FT Model of One Side of Power Grid with No Emergency Power</u>	A-32
<u>A-18. FT Model of the Emergency Power Only – Two Sides</u>	A-33
<u>A-19. FT Model of Emergency Power Only - One Side</u>	A-34
<u>B-1. Subtree DISCONNECT_SWGRE B</u>	B-3
<u>B-2. Subtree BUS_SWGRE B</u>	B-5
<u>B-3. Subtree SWYDB_SWGRE B</u>	B-7
<u>B-4. Subtree 12VDC_SIDE B</u>	B-9
<u>B-5. Subtree 125VDC_SWGRE B</u>	B-11
<u>B-6. Subtree EDGB_SWGRE B</u>	B-13

TABLES

	Page
1. <u>Basic Event Failure Rates and Probability Calculations</u>	36
2. <u>Alpha Factor Expressions for Common Cause Failure (Staggered Maintenance)</u>	39
3. <u>SAHPIRE Cut Sets Report for the entire Electrical Power Distribution System with no Emergency Power</u>	41
4. <u>SAPHIRE Cut Sets Report for the Entire Power Grid with Emergency Power</u>	44
5. <u>SAPHIRE Cut Sets Report for One Side of Power Grid with Emergency Power</u>	46
6. <u>SAPHIRE Cut Sets Report for One Side of Grid with No Emergency Power</u>	48
7. <u>SAPHIRE Cut Sets Report of the Emergency Power Only – Two Sides</u>	50
8. <u>SAPHIRE Cut Sets Report of the Emergency Power Only – One Side</u>	52
9. <u>Summary of Fault Tree Analyses</u>	54

ACRONYMS

AC	alternating current
CCF	common-cause failure
CCCF	Central Control Center Facility
CHF	Canister Handling Facility
CSNF	commercial spent nuclear fuel
DC	direct current
DTF	Dry Transfer Facility
EDG	emergency diesel generator
ESB	Emergency SWGR Building
FHF	Fuel Handling Facility
FT	fault tree
FTA	fault tree analysis
HVAC	heating, ventilation, and air-conditioning
LC	load center
MCC	motor control center
NRC	U.S. Nuclear Regulatory Commission
SWGR	switchgear
SWGR EA	emergency switchgear A
SWGR EB	emergency switchgear B

INTENTIONALLY LEFT BLANK

1. PURPOSE

A design requirement probability of 0.01 or less in a 4-hour period ensures that the nuclear heating, ventilation, and air-conditioning (HVAC) system in the primary confinement areas of the Dry Transfer Facilities (DTFs) and Fuel Handling Facility (FHF) is working during a Category 1 drop event involving commercial spent nuclear fuel (CSNF) assemblies (BSC 2004a, Section 5.1.1.48). This corresponds to an hourly HVAC failure rate of $2.5\text{E-}3$ per hour or less, which is contributed to by two dominant causes: equipment failure and loss of electrical power. Meeting this minimum threshold ensures that a Category 1 initiating event followed by the failure of HVAC is a Category 2 event sequence.

The two causes for the loss of electrical power include the loss of offsite power and the loss of onsite power distribution. Thus, in order to meet the threshold requirement aforementioned, the failure rate of mechanical equipment, loss of offsite power, and loss of onsite power distribution must be less than or equal to $2.5\text{E-}3$ per hour for the nuclear HVAC system in the primary confinement areas of the DTFs and FHF. The loss of offsite power occurs at a frequency of $1.1\text{E-}5$ per hour (BSC 2004a, Section 5.1.1.48).

The purpose of this analysis is to determine the probability of occurrence of the unavailability of the nuclear HVAC system in the primary confinement areas of the DTFs and FHF due to loss of electrical power. In addition, this analysis provides insights on the contribution to the unavailability of the HVAC system due to equipment failure. The scope of this analysis is limited to finding the frequency of loss of electrical power to the nuclear HVAC system in the primary confinement areas of the DTFs and FHF.

2. QUALITY ASSURANCE

The development of this analysis is subject to requirements of the *Quality Assurance Requirements and Description* (DOE 2004). This analysis is developed in accordance with procedure AP-3.12Q, *Design Calculations and Analyses*. Technical product inputs and references are identified and tracked in accordance with AP-3.15Q, *Managing Technical Product Inputs*.

3. USE OF COMPUTER SOFTWARE

3.1 SOFTWARE APPROVED FOR QUALITY ASSURANCE WORK

- Title: SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations)
- Version/Revision Number: 7.18
- Software Tracking Number: 10325-7.18-00
- Status/Operating System: Microsoft Windows 2000 Professional
- Computer Type: DELL GX240 Desktop PC
- Computer Number: CRWMS M&O Tag Number 501141

The software code SAPHIRE V7.18 (BSC 2002) is used to develop and quantify fault trees in this analysis. SAPHIRE V7.18 (BSC 2002) is a state-of-the-art probabilistic risk analysis software program that utilizes integrated event tree and fault tree methodology to develop and analyze the logical interactions that may occur between systems and components to determine the probability of an event's occurrence.

SAPHIRE V7.18 (BSC 2002) is qualified software that was obtained from Software Configuration Management. Independent software testing and verification using test cases of physical problems are documented in *Independent Verification and Validation Report for Legacy Code SAPHIRE V7.18* (BSC 2003, Section 3.5). This software is appropriate for use in the present analysis, and is used only within its range of validation in accordance with LP-SI.11Q-BSC, *Software Management*.

3.2 OTHER SOFTWARE

The Microsoft Excel 97 spreadsheet program is used to perform simple calculations as documented in Section 6.3.3. User-defined formulas, inputs, and results are documented in sufficient detail in Sections 6.1 through 6.4 to allow for the independent duplication of various computations without recourse to the originator. This software is exempt from the requirements of LP-SI.11Q-BSC, *Software Management*.

4. INPUTS

- 4.1 Electrical power system description is established by the *Electrical Power System Description Document* (BSC 2004b). This input contains the latest design information available for this report.
- 4.2 Electrical power system architecture is established by the *Electrical Power System Description Document* (BSC 2004b, Figure 4-1 and 4-3), and *Switchyard Switchgear Bldg Single Line Diagram 125 V DC System* (BSC 2004c). These inputs contain the latest design information available for this report.
- 4.3 Sources used for failure rate data are the *Generic Component Failure Data Base* (Eide and Calley 1993, Tables 1 and 2) and *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Powered Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)). These sources have compiled failure rate data for use in probabilistic risk assessment.
- 4.4 *Categorization of Event Sequences for License Application* (BSC 2004a, Sections 5.1.1.48 and 6.3.1.3) establishes the threshold failure probability that ensures that a Category 1 initiating event followed by the failure of HVAC is a Category 2 event sequence. This input also provides the failure rate for the loss of offsite power.
- 4.5 *Reliability Analysis of the Mechanical System in Selected Portions of the Nuclear HVAC System* (BSC 2004d, Section 6.3) establishes the success requirement for the nuclear HVAC system in the primary confinement areas of the DTFs and FHF.

5. ASSUMPTIONS

- 5.1 *Assumption:* Electrical power to at least one important motor control center (MCC I) is sufficient to prevent the failure of the nuclear HVAC system in the primary confinement areas of the DTFs and FHF.

Basis: The basis comes from the success requirement in the *Reliability Analysis of the Mechanical System in Selected Portions of the Nuclear HVAC System* (BSC 2004d, Section 6.3), which identifies the threshold for success of the HVAC system as being two supply fans and two exhaust fans for the DTFs and one supply fan and one exhaust fan for the FHF. An MCC I powers two supply and two exhaust fans at a time for the DTFs, while an MCC I powers one supply and one exhaust fan at a time for the FHF.

Used in: Sections 6.2.1, 6.2.3, 6.3, 7.2, 7.3, 7.5 and Figure A-2.

- 5.2 *Assumption:* Failures on loads not used for the distribution of power to the fans of interest are not analyzed in detail, but are compared to other loads of their kind that are fully analyzed.

Basis: Most loads that feed from the same power bus have the same components and distribute power similarly. Thus, by analyzing the failure of one load, an educated estimate can be done for the other loads.

Used in: Sections 6.3.2.1, 6.3.2.2, 6.3.2.3.2, and 6.3.3.

- 5.3 *Assumption:* If the emergency diesel generator (EDG) is successfully started and connected to the emergency SWGR of interest, all appropriate loads will be sequentially connected and powered.

Basis: The EDG is actuated automatically by an electronic control system, which when successful, will also work to sequentially connect the loads to the emergency SWGR bus. Automatic connection of EDGs and automatic sequencing of breakers to the emergency SWGR buses is described in *Electrical Power System Description Document* (BSC 2004b, Section 4.1.1.4).

Used in: Section 7.

- 5.4 *Assumption:* The basic mission time (t) used for calculating the failure probabilities of components is equal to 4 hours, which is the time required for the HVAC in the primary confinement areas of the DTFs and FHF to be in operation after a Category 1 drop involving CSNF assemblies.

Basis: This is a design requirement that ensures that a Category 1 initiating event followed by the failure of HVAC is a Category 2 event sequence (BSC 2004a, Section 5.1.1.48).

Used in: Sections 6.2.4, 6.3.3, 6.4, and 7.

- 5.5 *Assumption:* No credit is given for human operator interaction with the electrical power distribution system and thus, no human failure is analyzed in the Fault Tree Analysis (FTA).

Basis: The *Electrical Power System Description Document* (BSC 2004b, Section 3.2.6) does not specify human operator interaction within the system other than the manual connection of Substation B to the switchyard. It does describe most functions within the electrical power distribution system as being automated. When more operator interaction information is available, human error will be considered as a failure mode for this system.

Used in: Throughout document.

- 5.6 *Assumption:* Maintenance on redundant subsystems and components will be performed with a staggered schedule.

Basis: This is a recommended practice for highly reliable systems as a means of reducing the probability of common-cause failure (CCF). This permits use of the staggered maintenance Alpha Factor Model for CCF.

Used in: Sections 6.2.5, and 6.3.4.

- 5.7 *Assumption:* Power distribution from LC A and LC B to the supply and exhaust fans on the MCC Is will be as shown in Figure A-2.

Basis: This is standard design as described in the *Electrical Power System Description Document* (BSC 2004b).

Used in: Throughout document.

- 5.8 *Assumption:* Normal cooling of all electrical components is always present.

Basis: There is not enough information to indicate that loss of cooling to electrical components located in the equipment room is a potential cause of power failure in the required 4-hr mission time. When this information is available, loss of cooling to electrical equipment will be considered as a failure mode for this system. Currently, the failure rates of some of the electrical components include generic overheating.

Used in: Throughout document.

6. ANALYSIS

6.1 OBJECTIVE

The objective of this analysis is to perform an FTA on the portion of the onsite electrical power distribution system that provides power from the offsite power source to the Nuclear HVAC supply and exhaust fans in the primary confinement areas of the DTFs and FHF to determine its reliability. Because the loss of power distribution to the nuclear HVAC system in the primary confinement areas of the DTFs (DTF 1 and DTF 2) and FHF occurs the same way, only one FTA is performed. The text in the FTA refers to the DTF 1, but the results apply to the DTF 1, DTF 2, and FHF.

6.2 METHODOLOGY

FTA is a deductive failure analysis that focuses on one particular undesired event, called a top event, and provides a logic model for determining causes and quantifying the probability of occurrence for that event. FTA is performed to determine the safety and reliability of a system with the use of Boolean logic and probability theory. It also helps to improve the understanding of the system in question, identify components that may need further testing or redundancy, and identify root causes of equipment failure. This analysis is performed using the methods of the *Fault Tree Handbook* (Vesely et al. 1981). Steps in the analysis process are described in Sections 6.2.1 through 6.2.6.

6.2.1 Step One: Identify Top Event to be Analyzed

The undesirable event for the system in question is termed top event. The top event is then logically broken down into all credible ways it can occur. Because the lower level break down of the top event includes only those faults that contribute to this top event, it is important to identify the specific top event, which corresponds to a particular system failure mode. The top event for this analysis is “Failure of the electrical power distribution system to provide power to the nuclear HVAC system in the DTF 1 primary confinement.”

Once the top event has been established, success criteria must be identified. Identifying the success criteria helps break down the top event by defining the specific threshold that must be met in order to maintain the system in working order. For example, the nuclear HVAC system in the primary confinement areas of the DTFs is successful as long as one MCC I, which contains one set of two supply fans and one set of two exhaust fans, is powered (Assumption 5.1). This means that anything less than one MCC I powered designates failure and results in the top event.

6.2.2 Step Two: Understand the System

In order to identify the events that directly contribute to the top event, it is necessary to have a good understanding of the system being analyzed. Research must be done to understand how the system works as a whole, the direct interface between its subsystems, and the function performed by all components in each subsystem to accomplish the overall system function. This will help depict the interrelationships of basic events that lead to the top event. A basic event is found at the lowest level of break down of an FT and can represent the failure of an individual component, a particular human action, a CCF event, or an undeveloped event. A circle is used in

an FT to represent basic events, except for undeveloped events, which are represented with a diamond shape. Undeveloped events are those events that have not enough available information, but are modeled for completeness of the FT and can be developed at a later time.

In the study of the Electric Power Distribution system, it is important to understand how the overall system works (i.e., substations, switchyards, switchgears, and DC power), identify the specific path of power distribution from the outside source to the DTFs and FHF supply and exhaust fans, and know in detail the duty of each component along that path in order to conduct this power.

6.2.3 Step Three: Make a Logic Model

The FT model is done by breaking down the top event into combinations of basic events that lead to it. This is done with the use of Boolean logic gates. Logic gates show the relationships of events needed for the occurrence of a higher event. The higher event is the output of the gate; the lower events are the inputs to the gate. The gate symbol denotes the type of relationship of the input events required for the output event (Vesely et al. 1981, p. IV-1).

Boolean logic analysis consists of binary inputs and outputs to a gate such as 1s or 0s, and TRUE or FALSE. The two basic types of logic gates are AND and OR. The output of an OR-gate is TRUE if one or more of the input events is TRUE; otherwise, it is FALSE. This gate is used for components in series, only when each component is essential for the successful operation of a system. For example, in order to have successful power distributed to a load, it is necessary that safety devices placed in series such as circuit breakers and interrupter switches, remain closed to connect the load. Because the spurious opening of any of these devices will cause loss of power distribution to the load, they should be input to an OR-gate.

The output of an AND-gate is TRUE only if all the input events are TRUE; otherwise, it is FALSE. This gate is used for components in parallel only when not all components are essential for the operation of a system, meaning they are redundant. For example, a successful HVAC system requires only one MCC I to be successful (Assumption 5.1), yet the electrical power distribution system provides power to two MCC Is. Because only one MCC I is needed for the success of the HVAC, the second MCC I is redundant and the failure of the two MCC Is is represented by an AND-gate. Systems with components in series, when they are essential for the successful operation of a system, are less reliable than those with components in parallel that are also redundant. To quantify an OR-gate, inputs to it are added; to quantify an AND-gate, inputs to it are multiplied together.

It is important to note that components in series may be redundant to a system, and components in parallel may all be essential for the successful operation of a system.

With the use of logic gates, one is able to work backward to determine the intermediate events that lead to the top event and continue the process until arriving at the basic events (Section 6.2.2). The final FT can be constructed and analyzed with the use of computer program software such as SAPHIRE.

6.2.4 Step Four: Assess the Probability of Basic Events

Once the FT model has been made, the basic events are quantified using reliability data resources and probability calculations. A process of gathering and assembling component failure rate data from reliability databases for basic events is first done. Such databases include the *Generic Component Failure Data Base* (Eide and Calley 1993, Tables 1 and 2) and *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Powered Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)). Component reliability is expressed as a failure rate, symbolized as λ , and having units of “per hour”, or as a failure probability, symbolized as q , and having units of “per demand.”

The probability calculation of basic event failure is done with the use of the Poisson equation from NUREG/CR-2300 (NRC 1983, Section 5.5.2.4.1) and the mission time. The Poisson equation for predicting the probability of a specific number of failures (r) in mission time (t) is:

$$P(r) = \frac{(\lambda t)^r e^{(-\lambda t)}}{r!} \quad (\text{Eq. 1})$$

where:

- r = number of failures in time (t)
- λ = failure rate per hour
- t = mission time in hours
- $P(r)$ = probability of getting r failures in time t

The probability of having one or more failures (r) in the mission time (t) is given as:

$$P(r \geq 1) = 1 - P(r = 0) = 1 - e^{(-\lambda t)} \quad (\text{Eq. 2})$$

For small values of λ , Equation 2 can be approximated as:

$$q = \lambda t \quad (\text{Eq. 3})$$

where q is the probability of failure in time t .

Note that “per demand” failure probabilities are already in the form q and do not need to be multiplied by the mission time.

The mission time is the time required for the system to be successfully in operation. For example, if there was a drop of a CSNF assembly in the DTFs, the time required for the HVAC to be in operation to clean up the concentration of a radiological release in the air is the mission time. The mission time is set by the design requirement to be 4 hours (Assumption 5.4).

After all basic events are assessed and probability values are calculated, they are input into SAPHIRE.

6.2.5 Step Five: Perform Common-Cause Failure Analysis

CCFs occur simultaneously in two or more identical and redundant components with the same manufacturer due to a single cause. The root cause may be operation, maintenance errors, design, or location (Mosleh 1998).

The assessment of CCF events (Section 6.2.2) is done by multiplying the redundant component's failure probability by a special factor that considers how many are in the redundant group and how many are needed for success. There are many methods of CCF modeling such as the Beta Factor, the Multiple Greek Letter, and the Alpha Factor. The method recommended by the U.S. Nuclear Regulatory Commission (NRC) is the Alpha Factor in NUREG/CR-5497 (Marshall 1998) and NUREG/CR-5485 (Mosleh 1998). A table shown in Section 6.3.4 is a guideline for using the alpha factor method in CCF analyses (BSC 2004e, Table II-2) assuming staggered maintenance on redundant components (Assumption 5.6).

Figure 1 shows the basic way of modeling CCF in OR-gates. Logic analysis shows that whenever redundant events are inputs to an OR-gate, the success criteria for the CCF basic event is n-of-n, where n is the number of redundant events in the system. The CCF basic event is then quantified by multiplying the failure probability of the redundant basic event by the alpha factor of n-of-n in Section 6.3.4

Figure 1. CCF Input to an OR-Gate

It is important to note from Figure 1 that a CCF input to an OR-gate is only qualitatively important because quantitatively it does not contribute significantly to the output of the FT. In

this case, the output without CCF is $3.0\text{E-}3$, whereas with CCF, it is $3.1\text{E-}3$. Note that the CCF failure probability of $6.2\text{E-}5$ is equal to the component failure probability of $1.0\text{E-}3$ times the alpha factor of 0.062 for a 3-out-of-3 success from Section 6.3.4.

Figure 2 shows the basic way of modeling CCF in AND-gates. Logic analysis shows that whenever redundant events are inputs to an AND-gate, the success criteria for the CCF basic event is always 1-of-n, where n is the number of redundant events in the system. The CCF basic event is then quantified by multiplying the failure probability of the redundant basic event by the alpha factor of 1-of-n in Section 6.3.4.

Figure 2. CCF Input to an AND-Gate

A CCF event to an AND-gate is modeled with the use of an OR-gate as shown in Figure 2. This CCF event is qualitatively and quantitatively important to the output of the FT. In this case, the output without CCF is $1.0\text{E-}9$ whereas with CCF, it is $2.6\text{E-}5$, which is the value of the CCF and dominates the total output. Note that the CCF failure probability of $2.6\text{E-}5$ is equal to the component failure probability of $1.0\text{E-}3$ times the alpha factor of 0.026 for a 1-out-of-3 success from Section 6.3.4.

CCF is not applied to human action events or to undeveloped events.

6.2.6 Step Six: Interpret Qualified and Quantified Results

Once the FT has been modeled and failure probabilities have been input into all the basic events, it is ready to be evaluated. With the aid of SAPHIRE, the appropriate Boolean algebra is performed and the result is output in a cut set report that contains the minimal cut sets. A minimal cut set is the smallest combination of component failures, which, if they all occur, will cause the top event to occur. If one of the failures in the cut set does not occur, then the top event will not occur by this combination (Vesely et al. 1981, VII-15). A cut set report can be either qualitative, quantitative, or both.

A qualitative cut set report shows all the different combinations of basic events that make the top event TRUE. Each combination is a minimal cut set that can range from one event to six or more, depending on the complexity of the tree. The report arranges minimal cut sets in increasing order, which shows how sensitive the system is to each cut set. The most critical events in an FT are those at the top of the report because it takes fewer components to make the top event occur, whereas the higher the number of events in a cut set, the more components it takes to make the top event occur.

A quantitative cut set report shows the same arrangement of minimal cut sets as the qualitative report, but contains the probability of each cut set to occur and the percentage contribution of the cut set to the total system failure. This report provides insight in the major contributors to the top event.

A cut set report analysis can improve the system's reliability by identifying the main contributing events and either adding redundancy to these components or using more reliable ones.

6.3 FAULT TREE ANALYSIS

The FTA discussed in Sections 6.3 through 6.4 analyzes the entire portion of the onsite electrical power distribution system that provides power from the offsite power source to the Nuclear HVAC supply and exhaust fans in the primary confinement areas of the DTFs and FHF. The FTA discussed in Sections 6.3 through 6.4 does not take credit for any backup power such as standby or emergency. Sensitivity analyses discussed in Sections 7.1 through 7.4 consider options where emergency power is credited. The drawings used for this analysis are Figures A-1, A-2, A-3, and A-4.

Because the loss of power distribution to the nuclear HVAC system in the primary confinement areas of the DTFs (DTF 1 and DTF 2) and FHF occurs the same way, only one FTA is performed. The text in the FTA refers to the DTF 1, but the results apply to the DTF 1, DTF 2, and FHF.

Top Event

The top event of the FT in Figure A-5 is described as "Failure of the Electrical Power Distribution system to provide power to the Nuclear HVAC system in the DTF 1 Primary Confinement." It is represented by an AND-gate called LOSP_ONSITE.

Success Criteria

The success criteria determine what the top logic gate should be. In this case, the nuclear HVAC system in the primary confinement areas of the DTF 1 is successful as long as one MCC I, which contains one set of two supply fans and one set of two exhaust fans, is powered (Assumption 5.1). One MCC I is on side A and another on side B. No credit is given for partial success, meaning that no credit is given for the success of each individual fan. It is apparent from Figure A-2 that if an MCC I fails, then the fans attached to it (one set of two supply fans and one set of 2 exhaust fans) will fail to be powered. Because of the success criterion aforementioned, losing power to one MCC I does not mean failure. In order to lose power to the HVAC, both MCC Is would have to be lost. This is represented with an AND-gate that has inputs FANS_SIDEA and FANS_SIDEB.

6.3.1 Electrical Power Distribution System Description

Figure A-1 depicts the power distribution path from an offsite source at Substations A and B to the DTF 1, DTF 2, and FHF. The electrical power distribution system starts with two substations, A and B, that receive the power transmitted from the electrical power utility company, and then step down the voltages for distribution to the monitored geologic repository. Substation A receives 230 kiloVolts (kV) of electricity, and with the use of its main transformer A, steps down the power to 12.47kV of electricity to be distributed to the entire repository through the switchyard, which is a bus that can split the distribution off in multiple directions. The switchyard bus has medium voltage circuit breakers so that the substation can be disconnected from the transmission grid, or separate distribution lines can be disconnected from the substations when necessary. Substation B works the same as Substation A, but receives only 138kV, which is used only if and when Substation A fails (BSC 2004b, Section 4.1.1.1). Other components in each substation include a coupling capacitor voltage transformer, which is used for metering, protection, and control of high voltages; a power circuit breaker that isolates the transmission power from the distribution power when necessary; a normally closed 4,000 Amp medium voltage circuit breaker; and protection devices such as surge and lightning arrestors. Note that the power circuit breaker consists of two motor operated disc switches and one medium voltage circuit breaker.

As shown in Figure A-1, the switchyard bus is composed of two main SWGR buses (A and B) that are connected by a 4,000 Amp medium voltage circuit breaker that is normally closed. The switchyard provides power to South Portal and North Portal facilities through a number of distribution lines. Each distribution line is called a load to the switchyard bus. When the switchyard bus fails to be powered, all medium voltage circuit breakers that connect the distribution lines to the repository facilities will automatically open and shed all the loads until they are sequentially reconnected when another source of power is acknowledged. Other sources of power, which are not initially connected to the switchyard unless the preferred (Substation A) supply fails, are Substation B and standby diesel generators, respectively. These sources are started and connected manually upon loss of power to the switchyard. All medium voltage circuit breakers along the 12.47kV switchyard also open or trip when a current fault on its load is detected. This is to prevent damage to the supplying switchyard bus.

Following the distribution along the bolded lines to the emergency SWGR loads A and B, there is another step down transformer reducing the power from 12.47kV to 4.16kV that is to be used by the loads of each emergency SWGR bus. The line that connects each emergency SWGR load to the switchyard has a medium voltage fused interrupter switch downstream of the 12.47kV to 4.16kV transformer and a medium voltage circuit breaker upstream of the transformer for protection of the switchyard in case of a current fault in the emergency SWGR load.

Emergency SWGRs A and B provide power through five distribution lines to different parts of the DTF 1, DTF 2, FHF, Canister Handling Facility (CHF), and Central Control Center Facility (CCCF) (Figure A-1). Each distribution line going to each building is called a load to the particular emergency SWGR. When the 4.16kV emergency SWGR bus fails to be powered, all medium voltage circuit breakers that connect the distribution lines to the facilities will automatically open until they are sequentially reconnected when another source of power is acknowledged. There is one EDG on each emergency SWGR and it is the other source of power that is to be used if normal power is lost. The EDG is initially disconnected from the emergency SWGR until it is started, and then connected automatically upon loss of power to it. Medium voltage circuit breakers along the 4.16kV Emergency SWGRs A and B also open or trip when a current fault on its load is detected. This is to prevent damage to the particular emergency SWGR bus.

Each load line connected to an emergency SWGR bus has a step down transformer that reduces the power from the 4.16kV to 480V, which is used by the load center (LC) bus in each building (Figure A-1). Each load line has a medium voltage circuit breaker and a medium voltage fused interrupter switch that disconnect the load in case of a current fault for protection of the emergency SWGR bus, as explained earlier.

Figure A-2 shows the continuing distribution of power from the 480V LC A bus and the 480V LC B bus, shown in Figure A-1, to the MCCs that feed motor loads. The LC A has four lines of distribution loads: MCC I, MCC A, MCC B, and MCC C. The LC B has four lines of distribution loads: MCC I(B), MCC X, MCC Y, and MCC Z. Each line has a molded case circuit breaker that trips and sheds its load in case of a current fault in the particular MCC load.

The MCC I in the LC A has one set of two supply fan motors and one set of two exhaust fan motors of the primary confinement areas of the DTF 1, while the same is true for the MCC I in the LC B. The DTF 2 has the same arrangement as the DTF 1. The FHF has the same arrangement as the DTF 1 and the DTF 2, except the MCC I on each side has only one supply fan and one exhaust fan.

All medium voltage circuit breakers are DC powered and therefore, it is also important to understand the normal and emergency 125V DC distribution systems shown in Figures A-3 and A-4. The normal 125V DC system (Figure A-3) consists of a 125V DC panelboard powered by 480V AC from MCC through a rectifier unit and a battery system (BSC 2004b, Section 4.1.1.3). There are two 125V DC distribution buses, A and B. Each has a 125V battery cell and a battery charger unit that delivers DC power by rectifying the 480V AC from an MCC. There is also a backup battery charger that can provide power to DC buses A and B in the event their charger fails. The function of the battery charger is to provide the transformed 125V DC power as well as keeping the set of battery cells fully charged (BSC 2004b, Section 4.1.1.3). The 125V DC

distribution bus A is the primary DC power distributor to the 12.47kV Main SWGR A and the backup DC supply to the 12.47kV Main SWGR B circuit breakers. The 125V DC distribution bus B is the primary DC power distributor to the 12.47kV Main SWGR B and the backup DC supply for the 12.47kV Main SWGR A circuit breakers. The emergency 125V DC systems (Figure A-4) located in the Emergency SWGR Building (ESB) provide control power for the 4.16kV emergency SWGR circuit breakers. Each emergency 125V DC system consists of a 125V DC distribution panelboard, a 125V DC battery bank and a battery charger (BSC 2004b, Section 4.1.1.4). Power to the emergency 125V DC distribution panelboard can be provided by the battery cell or battery charger. Each emergency battery charger is fed from the 480V AC on the MCC, which is fed from the emergency SWGR (Figure A-4).

6.3.2 Fault Tree Logic Model

Once the top event and its success criteria have been defined (Section 6.3), the rest of the FT can be developed. Figure A-5 shows that in order for the top event (represented by AND-gate LOSP_ONSITE) to occur, MCC Is on both sides of the distribution grid must fail. As explained in Section 6.3.1, one set of two supply fan motors and one set of two exhaust fan motors are powered by the same MCC I. To model the loss of power to more than two supply fans and two exhaust fans, only two inputs to AND-gate LOSP_ONSITE are necessary. Each input FANS_SIDEA and FANS_SIDEB represents the loss of power to MCC I and MCC I (B), respectively.

This analysis is approached by using the emergency SWGR bus as a pivot point, since it is the nearest source of power to each MCC I (Figure A-2). The following three events can cause the loss of power distribution to an MCC I and thus, can make OR-gates FANS_SIDEA and FANS_SIDEB occur:

- A disconnect of the DTF 1 load carrying the MCC I from the emergency SWGR bus. This is represented with TRANSFER-gate inputs, DISCONNECT_SWGRE A and DISCONNECT_SWGREB.
- The unavailability of the emergency SWGR bus. This is represented with TRANSFER-gate inputs, BUS_SWGRE A and BUS_SWGREB.
- The loss of power to the emergency SWGR bus. This is represented with TRANSFER-gate inputs, SWYDA_SWGRE A and SWYDA_SWGREB.

Note that each TRANSFER-gate (i.e. triangular shaped event) is the top event of a subtree developed on a different page.

Because the logic break down of FANS_SIDEA and FANS_SIDEB is the same, only side A is explained in this analysis. Figures A-6 through A-13 represent the logic break down of FAN_SIDEA and are explained in Sections 6.3.2.1 through 6.3.2.5. Different types of bullets are used throughout this report to emphasize the hierarchy of events in the FT. CCF events are explained in Section 6.3.4.

The FT model for FANS_SIDEB is shown in Attachment B.

6.3.2.1 Disconnect from Emergency Switchgear A

Figure A-6 shows subtree DISCONNECT_SWGREA, which is a sub-top event defined as “Failure of MCC I to remain connected to the Emergency Switchgear A.” The distribution path from the emergency SWGR to the MCC I is made up of components in series (Section 6.3.1). Therefore, the sub-top event is represented by an OR-gate (Section 6.2.3), which means that if any of the inputs to it are TRUE, the top event occurs. This is one major cause for the loss of power distribution to one set of two supply fans and one set of two exhaust fans (Section 6.3.2), and is the expansion of TRANSFER-gate DISCONNECT_SWGREA in Figure A-5. The following events are inputs to DISCONNECT_SWGREA based on Figure A-1:

- TRANSFER-gate 125VDC_SWGREA: 125V DC System fails to supply power to SWGR EA Medium Voltage Circuit Breakers (Section 6.3.2.5).
- Basic Event MCKTBRKR_O_DTF1: Medium Voltage Circuit Breaker fails to remain closed to connect DTF 1 load.
- Basic Event FUSE_O_DTF1: Fused interrupter switch fails to remain closed to connect DTF 1 load.
- Basic Event XFMR_DTF1: 4160-480V Transformer fails to operate.
- Basic Event LINE_DTF1: Power line fails to remain intact to connect DTF 1 load.
- OR-gate DISCONNECT_LCA: Failure of MCC I to remain connected to Load Center A.
- OR-gate BUS_LCA: Load Center A Bus failure.

Input 125VDC_SWGREA is explained in Section 6.3.2.5 and CCF inputs are explained in Section 6.3.4.

The DTF 1 load refers to the entire load as seen by SWGR EA (Figure A-1), and LC A refers to the bus that powers the MCCs on the DTF 1 load (Figure A-2). DISCONNECT_LCA continues the series of break down from the LC A down to the MCC I that powers one set of two supply fans and one set of two exhaust fans in the DTF 1 primary confinement area (Figure A-2). The following three events are inputs to DISCONNECT_LCA that can cause a disconnect of the MCC I from the LC A:

- ⇒ Basic Event IBUS_MCCI: MCC I bus fails short circuited. Notice that this is not a direct disconnect, but an indirect one that will cause the circuit breaker to disconnect MCC I from LC A when this event occurs.
- ⇒ Basic Event LINE_MCCI: Power line fails to remain intact to connect MCC I load.
- ⇒ Basic Event LCKTBRKR_O_MCCI: Low Voltage Circuit Breaker fails to remain closed to connect MCC I load.

Note that CCF inputs are explained in Section 6.3.4.

BUS_LCA is another subtree input to DISCONNECT_SWGREA that shows the failure of the LC A bus that will cause an indirect disconnect from the SWGR EA by the protective medium voltage fused interrupter switch or the medium voltage circuit breaker (Figure A-1). Failures in electric current such as “shorts” and “overloads” are what cause protective devices to trip. The following two events are inputs to OR-gate BUS_LCA that describe faults in electric current on the LC A bus:

⇒ Basic Event IBUS_LCA: LC A Bus fails short circuited.

⇒ OR-gate CBUS_LCA: LC A Bus fails overloaded.

CBUS_LCA is a subtree that describes the failure of the LC A bus due to all MCC loads connected to it causing an overload. Due to the protective devices in each load, this is a rare failure, but nonetheless, must be modeled.

There are three other MCC loads besides the MCC I feeding from LC A: MCC A, MCC B, and MCC C (Figure A-2). If one of these loads has an unknown electrical current fault, and if the circuit breaker fails to isolate this fault, the LC A bus will suffer an overload, which means it is unavailable to the remaining loads connected to it. The time period of the unavailability of LC A may be short and thus, may not completely cease power to the loads, but will cause a disconnect from SWGR EA by the protective devices. The following four events are inputs to OR-gate CBUS_LCA that describe a possible overload to LC A by any of its MCC loads:

✧ AND-gate OLOAD_MCCI: MCC I fault fails to be shed from LC A bus.

✧ AND-gate OLOAD_MCCA: MCC A fault fails to be shed from LC A bus.

✧ AND-gate OLOAD_MCCB: MCC B fault fails to be shed from LC A bus.

✧ AND-gate OLOAD_MCCC: MCC C fault fails to be shed from LC A bus.

OLOAD_MCCI will occur if MCC I bus fails short circuited, represented by basic event IBUS_MCCI, and the low voltage circuit breaker fails to shed it upon demand, represented by basic event LCKTBRKR_S_MCCI. It is important to note that basic event IBUS_MCCI will cause a disconnect from the LC A bus (as seen in subtree DISCONNECT_LCA), given that the low voltage circuit breaker works. Otherwise, if the low voltage circuit breaker fails, IBUS_MCCI will cause an overload on the LC A bus as seen in OLOAD_MCCI. In turn, OLOAD_MCCI will cause a disconnect from the SWGR EA (as seen in subtree BUS_LCA), given that the medium voltage circuit breaker or medium voltage fused interrupter switch works.

The rest of the above mentioned gates are TRUE only if there is an unknown fault in the load, represented by undeveloped event FAULT_MCCX, and the low voltage circuit breaker fails to shed it upon demand, represented by basic event LCKTBRKR_S_MCCX. Each undeveloped fault is assumed to be comparable to the fault in the MCC I (Assumption 5.2), IBUS_MCCI.

6.3.2.2 Emergency Switchgear A Bus Unavailable

Figure A-7 shows subtree BUS_SWGREA, which is a sub-top event defined as “Emergency Switchgear A Bus Unavailable.” The SWGR EA bus will be unavailable to power the MCC I if it has an electrical current failure due to a “short” or an “overload.” This is another major cause for the loss of power distribution to one set of two supply fans and one set of two exhaust fans (Section 6.3.2), and is the expansion of TRANSFER-gate BUS_SWGREA in Figure A-5. BUS_SWGREA is represented by an OR-gate with the following inputs based on Figure A-1:

- Basic Event IBUS_SWGREA: SWGR EA bus fails short circuited.
- OR-gate CBUS_SWGREA: SWGR EA bus fails overloaded.

CBUS_SWGREA is a subtree that describes the failure of the SWGR EA bus due to all loads connected to it causing an overload. Due to the protective devices in each load, this is a rare failure, but nonetheless, must be modeled.

There are four other loads besides LC A feeding from SWGR EA: LC C, MCC S, LC G, and MCC K (Figure A-1). If one of these loads has an unknown electrical current fault and if the circuit breaker fails to isolate this fault, the SWGR EA bus will suffer an overload, which means it is unavailable to the remaining loads connected to it. The time period of the unavailability of SWGR EA may be short and thus, may not completely cease power to the loads, but for conservatism, it is modeled in this analysis. Notice that the EDG is not one of the contributing loads to the overload of the SWGR EA because it is not connected to it. A current fault on the SWGR EA bus can also cause a disconnect from Main SWGR A by the protective devices as will be seen in Section 6.3.2.3.1. The following five events are inputs to OR-gate CBUS_SWGREA that describe a possible overload to SWGR EA by any of its loads:

- ⇒ AND-gate OLOAD_LCC: LC C fault fails to be shed from SWGR EA bus.
- ⇒ AND-gate OLOAD_MCCS: MCC S fault fails to be shed from SWGR EA bus.
- ⇒ AND-gate OLOAD_LCG: LC G fault fails to be shed from SWGR EA bus.
- ⇒ AND-gate OLOAD_MCCK: MCC K fault fails to be shed from SWGR EA bus.
- ⇒ AND-gate OLOAD_LCA: LC A fault fails to be shed from SWGR EA bus.

OLOAD_LCA will occur if LC A bus fails due to a current fault, represented by FAULT_LCA, and the medium voltage circuit breaker or the fused interrupter switch fails to shed it upon demand, represented by basic events MCKTBRKR_S_LCA and FUSE_S_LCA, respectively. FAULT_LCA represents the current fault that was developed in subtree DISCONNECT_SWGREA (Figure A-6), BUS_LCA, and a failure in the 4160-480V transformer of the DTF 1 load, represented by XFMR_DTF1. The DTF 1 load refers to the entire load as seen by SWGR EA (Figure A-1), and LC A refers to the bus that powers the MCCs on the DTF 1 load (Figure A-2). It is important to note that BUS_LCA and XFMR_DTF1 will cause a disconnect from the SWGR EA bus (as seen in subtree DISCONNECT_SWGREA), given the medium voltage circuit breaker or medium voltage fused

interrupter switch works (Section 6.3.2.1). Otherwise, if the medium voltage circuit breaker and medium voltage fused interrupter switch fail, BUS_LCA and XFMR_DTF1 will cause an overload on the SWGR EA bus as seen in OLOAD_LCA.

Note that CCF inputs are explained in Section 6.3.4.

The rest of the above mentioned gates are TRUE only if there is an unknown fault in the load, represented by undeveloped event FAULT_XXX; the medium voltage circuit breaker fails to shed it upon demand, represented by basic event MCKTBRKR_S_XXX; and the fused interrupter switch fails to open after a fault in the load, represented by FUSE_S_XXX. Each undeveloped fault is assumed to be comparable to the fault on the LC A bus (Assumption 5.2), FAULT_LCA.

6.3.2.3 Loss of Power to the Emergency Switchgear A

The power distributed to SWGR EA is supplied by Main SWGR A (Figure A-1). Therefore, any failures along the path of distribution from the Main SWGR A to SWGR EA will cause loss of power to SWGR EA. This is one last major cause for the loss of power distribution to one set of two supply fans and one set of two exhaust fans (Section 6.3.2), and it is the expansion of TRANSFER-gate SWYDA_SWGREA in Figure A-5.

Figure A-8 shows subtree SWYDA_SWGREA, which is a sub-top event defined as “Failure of Main Switchgear A to power Emergency Switchgear A.” The following three overall events can make OR-gate SWYDA_SWGREA occur based on Figure A-1:

- A disconnect of the SWGR EA load carrying the MCC I from its nearest source of power, the Main SWGR A bus. This is represented with subtree DISCONNECT_SWYDA.
- The unavailability of the Main SWGR A bus. This is represented with subtree BUS_SWYDA.
- The loss of power to the Main SWGR A bus. This is represented with TRANSFER-gate input LOSEP_SWYDA.

Sections 6.3.2.3.1 through 6.3.2.3.3 describe in detail each subtree mentioned above that is an input to OR-gate SWYDA_SWGREA.

6.3.2.3.1 Disconnect from Main SWGR A

Figure A-8 shows subtree DISCONNECT_SWYDA, which is defined as “Failure of SWGR EA to remain connected to Main SWGR A.” The distribution path from Main SWGR A to SWGR EA is made up of components in series (Section 6.3.1) and therefore, DISCONNECT_SWYDA is represented by an OR-gate. The following events are inputs to DISCONNECT_SWYDA based on Figure A-1:

- TRANSFER-gate 125VDC_SIDEA: 125V DC System fails to supply power to Side A Medium Voltage Circuit Breakers (Section 6.3.2.4).

- Basic Event MCKTBRKR1_O_SWGREA: Medium Voltage Circuit Breaker 1 fails to remain closed to connect the SWGR EA load.
- Basic Event FUSE_O_SWGREA: Fused interrupter switch fails to remain closed to connect the SWGR EA load.
- Basic Event XFMR_SWGREA: 12.47-4.16kV Transformer fails to operate.
- Basic Event LINE_SWGREA: Power line fails to remain intact to connect the SWGR EA load.
- Basic Event MCKTBRKR2_O_SWGREA: Medium Voltage Circuit Breaker 2 fails to remain closed to connect the SWGR EA load.
- TRANSFER-gate BUS_SWGREA: Emergency Switchgear A bus unavailable (Section 6.3.2.2).

Input 125VDC_SIDEA is explained in Section 6.3.2.4 and CCF inputs are explained in Section 6.3.4.

It is important to note that while subtree BUS_SWGREA (Section 6.3.2.2) represents the unavailability of power to the DTF 1, it also causes a disconnect from the Main SWGR A bus, given the medium voltage circuit breaker or medium voltage fused interrupter switch works.

Otherwise, if the medium voltage circuit breaker and medium voltage fused interrupter switch fail, BUS_SWGREA will cause an overload on the Main SWGR A bus. This possibility is discussed in the next section.

6.3.2.3.2 Main SWGR A Bus Unavailable

Figure A-8 shows subtree BUS_SWYDA, which is defined as “Main SWGR A Bus Unavailable.” The Main SWGR A bus will be unavailable to power the SWGR EA load if it has an electrical current failure due to a “short” or an “overload”. Due to the interconnect circuit breaker that connects Main SWGR A to Main SWGR B, the unavailability of Main SWGR B must also be considered for the case in which the interconnect circuit breaker fails to isolate the failure. The following three inputs can make OR-gate BUS_SWYDA occur based on Figure A-1:

- Basic Event IBUS_SWYDA: Main SWGR A Bus fails short circuited.
- TRANSFER-gate CBUS_SWYDA: Main SWGR A Bus fails overloaded.
- AND-gate BUSINT_SWYDB: Interconnect Medium Voltage Circuit Breaker fails to isolate failure in Main SWGR B.

Note that CCF inputs are explained in Section 6.3.4.

Figure A-9 shows subtree CBUS_SWYDA, which is defined as “Main SWGR A Bus fails overloaded.” This figure is the expansion of TRANSFER-gate CBUS_SWYDA in Figure A-8 that if TRUE, can make the Main SWGR A bus unavailable. This subtree describes the failure of the Main SWGR A bus due to all loads connected to it causing an overload.

There are seven other loads in addition to SWGR EA, feeding from Main SWGR A: LC 12, SWGR 01A, SWGR 08, SWGR 06, 2MVA, 11.7MVA, and SWGR C (Figure A-1). If one of these loads has an unknown electrical current fault, and if the circuit breaker or fused interrupter switch fails to isolate this fault, the Main SWGR A bus will suffer an overload, which means it is unavailable to remaining loads connected to it. The time period of the unavailability of Main SWGR A may be short and thus, may not completely cease power to the loads, but for conservatism, it is modeled in this analysis. A current fault on the Main SWGR A bus can also cause load disconnects from Main SWGR A by the protective devices. Notice that the two standby diesel generators are not contributing loads to the overload of Main SWGR A because they are not connected to it. The following eight events are inputs to OR-gate CBUS_SWYDA that describe a possible overload to Main SWGR A by any of its loads:

- ⇒ AND-gate OLOAD_LC12: LC 12 fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_SWGR01A: SWGR 01A fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_SWGR08: SWGR 08 fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_SWGR06: SWGR 06 fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_2MVA: 2MVA fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_11.7MVA: 11.7MVA fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_SWGRC: SWGR C fault fails to be shed from Main SWGR A bus.
- ⇒ AND-gate OLOAD_SWGREA: SWGR EA fault fails to be shed from Main SWGR A bus.

OLOAD_SWGREA will occur if the SWGR EA bus fails due to a current fault, represented by FAULT_SWGREA, and the medium voltage circuit breaker or the medium voltage fused interrupter switch fails to shed it upon demand, represented by basic events MCKTBRKR_S_SWGREA and FUSE_S_SWGREA, respectively. FAULT_SWGREA represents the current fault that was developed in subtree BUS_SWGREA, and a failure in the 12.47-4.16kV transformer of the SWGR EA load, represented by XFMR_SWGREA. It is important to note that event BUS_SWGREA will cause a disconnect from the Main SWGR A bus (as seen in subtree DISCONNECT_SWYDA), given the medium voltage circuit breaker or medium voltage fused interrupter switch works (Section 6.3.2.3.1). Otherwise, if the medium voltage circuit breaker and medium voltage fused interrupter switch fail, BUS_SWGREA will cause an overload on the Main SWGR A bus, as seen in OLOAD_SWGREA.

Note that CCF inputs are explained in Section 6.3.4.

With the exception of OLOAD_2MVA, OLOAD_11.7MVA, and OLOAD_SWGRC, the rest of the above mentioned gates are TRUE only if there is an unknown fault in the load, represented by undeveloped event FAULT_XXX; the medium voltage circuit breaker fails to shed it upon demand, represented by basic event MCKTBRKR_S_XXX; and the fused interrupter switch fails to open after a fault in the load, represented by FUSE_S_XXX.

OLOAD_2MVA or OLOAD_11.7MVA can occur if there is an unknown fault in the load, represented by undeveloped event FAULT_XXX, and the medium voltage circuit breaker fails to shed it upon demand, represented by basic event MCKTBRKR_S_XXX.

OLOAD_SWGRC can occur if there is an unknown fault in the load, represented by undeveloped event FAULT_SWGRC; medium voltage circuit breaker 1 fails to shed it upon demand, represented by basic event MCKTBRKR_S1_SWGRC; and medium voltage circuit breaker 2 fails to shed it upon demand, represented by basic event MCKTBRKR_S2_SWGRC.

Each undeveloped fault is assumed to be comparable to the fault on the SWGR EA bus (Assumption 5.2), FAULT_SWGRE.

Figure A-8 shows subtree BUSINT_SWYDB, which is a third input to OR-gate BUS_SWYDA that if TRUE, can make the Main SWGR A bus unavailable and successively FANS_SIDEA will occur. BUSINT_SWYDB is defined as “Interconnect Medium Voltage Circuit Breaker fails to isolate failure in Main SWGR B.” Also, note that when BUSINT_SWYDB is TRUE, Main SWGR B bus has failed to provide power to SWGR EB, which carries an MCC I and successively FANS_SIDEB occurs. Because BUSINT_SWYDB makes FANS_SIDEA and FANS_SIDEB occur simultaneously, AND-gate LOSEP_ONSITE in Figure A-5 is TRUE and the top event occurs. The following two inputs must both be TRUE in order for AND-gate BUSINT_SWYDB to occur:

- ⇒ Basic event ICKTBRKR_S: Interconnect Medium Voltage Circuit Breaker fails to open after a failure on Main SWGR B.
- ⇒ OR-gate BUS_SWYDBB: Main SWGR B bus failure.

Subtree BUS_SWYDBB in Figure A-8 describes the failure of the Main SWGR B bus. This subtree is similar to OR-gate BUS_SWYDA, which describes the failure of the Main SWGR A bus, except for BUS_SWYDBB describes the failure of Main SWGR B and has only two inputs:

- ✧ Basic event IBUS_SWYDB: Main SWGR B bus fails short circuited.
- ✧ TRANSFER-gate CBUS_SWYDB: Main SWGR B bus fails overloaded.

Figure A-10 shows subtree CBUS_SWYDB, which is defined as “Main SWGR B Bus fails overloaded.” This figure is the expansion of TRANSFER-gate CBUS_SWYDB in Figure A-8 that if TRUE, can cause the failure of the Main SWGR B bus. This subtree describes the failure of the Main SWGR B bus due to all loads connected to it causing an overload.

There are eight other loads in addition to SWGR EB, feeding from Main SWGR B: SWGR 01B, LC 13, SWGR 09, SOLAR POWER, SWGR 07, 3.8MVA, 11.8MVA, and SWGR D

(Figure A-1). If one of these loads has an unknown electrical current fault and if the circuit breaker or fused interrupter switch fails to isolate this fault, the Main SWGR B bus will suffer an overload, which means it is unavailable to remaining loads connected to it. Notice that the two standby diesel generators are not contributing loads to the overload of Main SWGR B because they are not connected to it. The following nine events are inputs to OR-gate CBUS_SWYDB that describe a possible overload to Main SWGR B by any of its loads:

- AND-gate OLOAD_SWGR01B: SWGR 01B fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_LC13: LC 13 fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_SWGR09: SWGR 09 fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_SOLAR: SOLAR POWER fault fails to be shed from the Main SWGR B bus.
- AND-gate OLOAD_SWGR07: SWGR 07 fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_3.8MVA: 3.8MVA fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_11.8MVA: 11.8MVA fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_SWGRD: SWGR D fault fails to be shed from Main SWGR B bus.
- AND-gate OLOAD_SWGREB: SWGR EB fault fails to be shed from Main SWGR B bus.

OLOAD_SWGREB will occur if SWGR EB bus fails due to a current fault, represented by FAULT_SWGREB, and the medium voltage circuit breaker or the medium voltage fused interrupter switch fails to shed it upon demand, represented by basic events MCKTBRKR_S_SWGREB and FUSE_S_SWGREB, respectively.

Note that CCF inputs are explained in Section 6.3.4.

With the exception of OLOAD_3.8MVA, OLOAD_11.8MVA, and OLOAD_SWGRD, the rest of the above mentioned gates are TRUE only if there is an unknown fault in the load, represented by undeveloped event FAULT_XXX; the medium voltage circuit breaker fails to shed it upon demand, represented by basic event MCKTBRKR_S_XXX; and the fused interrupter switch fails to open after a fault in the load, represented by FUSE_S_XXX.

OLOAD_3.8MVA or OLOAD_11.8MVA can occur if there is an unknown fault in the load, represented by undeveloped event FAULT_XXX, and the medium voltage circuit breaker fails to shed it upon demand, represented by basic event MCKTBRKR_S_XXX.

OLOAD_SWGRD can occur if there is an unknown fault in the load, represented by undeveloped event FAULT_SWGRD; medium voltage circuit breaker 1 fails to shed it upon demand, represented by basic event MCKTBRKR1_S_SWGRD; and medium voltage circuit breaker 2 fails to shed it upon demand, represented by basic event MCKTBRKR2_S_SWGRD.

Each undeveloped fault is assumed to be comparable to the fault on the SWGR EB bus (Assumption 5.2), FAULT_SWGREB.

6.3.2.3.3 Loss of Power to the Main SWGR A

Figure A-11 shows subtree LO SP_SWYDA, which is defined as “Failure of 230kV system to supply power to Main SWGR A.” This is another cause for the loss of power distribution from Main SWGR A to SWGR EA (Section 6.3.2.3) and is the expansion of TRANSFER-gate LO SP_SWYDA in Figure A-8. Loss of power distribution to Main SWGR A will occur if Substation A fails to deliver power to it. As explained in Section 6.3.1, Main SWGRs A and B are normally connected by an interconnect medium voltage circuit breaker and powered by the preferred source of power, Substation A. If this source fails, Substation B will act as a backup to power Main SWGRs A and B. For the event that a shift in power source is necessary (i.e. from Substation A to Substation B), power to the Main SWGRs A and B will be interrupted for a period of time during which Substation B is connected and loads sequenced back on to the Main SWGRs A and B. This event is considered loss of power and thus no credit is given for Substation B as a source of power. This subtree, based on Figure A-1, describes the way Substation A can fail to supply power to Main SWGR A since it is directly connected to it. Because all the components in Substation A are in series, LO SP_SWYDA is described by an OR-gate. Any of the following six inputs, if TRUE, can make subtree LO SP_SWYDA occur:

- Basic Event SOURCE_230KV: Loss of 230kV source.
- Basic Event CCVTA_230KV: Coupling Capacitor Voltage Transformer A fails to operate.
- Basic Event PWRCKTBRKRA_230KV: Power Circuit Breaker A fails to remain closed to connect 230kV power. Note that the power circuit breaker consists of two motor operated disc switches and one medium voltage circuit breaker (Section 6.3.1).
- Basic Event XFMRA_230KV: 230-12.47kV Main Transformer A fails to operate.
- Basic Event 4KCKTBRKR_O_230KV: 4kA Medium Voltage Circuit Breaker fails to remain closed to connect 230kV power.
- Basic Event LINE_230KV: Power line fails to remain intact to connect 230kV power.

Note that CCF inputs are explained in Section 6.3.4.

6.3.2.4 Normal 125V DC System Failure - Side A

Figure A-12 shows subtree 125VDC_SIDEA, which is defined as “125V DC System fails to supply power to Side A medium voltage circuit breakers.” This causes the disconnection of SWGR EA from the Main SWGR A. Thus, it is the expansion of TRANSFER-gate 125VDC_SIDEA in subtree DISCONNECT_SWYDA (Figure A-8).

In Figure A-3 and Section 6.3.1, it is shown that all normal medium voltage circuit breakers on Side A of the power grid are powered by the 125V DC distribution bus A and can be powered from 125V DC distribution bus B when bus A is unavailable. Thus, in order for AND-gate 125VDC_SIDEA to occur, the following two events must occur:

- OR-gate DCBUSA_SIDEA: Failure of 125V DC Distribution Bus A to supply power to Side A Circuit Breakers.
- OR-gate DCBUSB_SIDEA: Failure of 125V DC Distribution Bus B to supply backup power to Side A Circuit Breakers.

Subtree DCBUSA_SIDEA describes the failure of the 125V DC distribution bus A to power all normal medium voltage circuit breakers on side A of the power grid. The following four events are inputs that can make OR-gate DCBUSA_SIDEA occur:

- ⇒ Basic Event LCKTBRKR_O_SIDEA: Low voltage circuit breaker fails to remain closed to connect Side A load.
- ⇒ Basic Event LINE_SIDEA: Power line fails to remain intact to connect Side A load.
- ⇒ Basic Event DCBUSA: 125V DC Distribution Bus A fails short circuited.
- ⇒ AND-gate POWER_DCBUSA: Loss of DC power to Distribution Bus A.

Note that CCF inputs are explained in Section 6.3.4.

Subtree POWER_DCBUSA describes the loss of power to the distribution bus A from the battery chargers and the 125V DC battery cell shown in Figure A-3. In order for AND-gate POWER_DCBUSA to occur, the following two events must occur:

- ✧ Basic Event BATTERY_DCBUSA: 125V DC Distribution Bus A battery fails to operate.
- ✧ AND-gate CHARGR_DCBUSA: 125V DC Distribution Bus A Battery Chargers fail to operate.

CHARGR_DCBUSA occurs if battery charger D11 and backup battery charger D13 fail to operate simultaneously, represented by basic events CHARGRD11_DCBUSA and CHARGRD13_BACKUP, respectively.

Subtree DCBUSB_SIDEA describes the failure of the 125V DC distribution bus B to supply backup power to all normal medium voltage circuit breakers on side A of the power grid. The following four events are inputs that can make OR-gate DCBUSB_SIDEA occur:

- ⇒ Basic Event LCKTBRKRB_C_SIDEA: Low voltage circuit breaker fails to close upon demand to connect Side A load.
- ⇒ Basic Event LINEB_SIDEA: Power line fails to remain intact to connect Side A load.

⇒ Basic Event DCBUSB: 125V DC Distribution Bus B fails short circuited.

⇒ AND-gate POWER_DCBUSB: Loss of DC power to Distribution Bus B.

Note that CCF inputs are explained in Section 6.3.4.

Subtree POWER_DCBUSB describes the loss of power to the distribution bus B from the battery chargers and the 125V DC battery cell shown in Figure A-3. In order for AND-gate POWER_DCBUSB to occur, the following two events must occur:

✧ Basic Event BATTERY_DCBUSB: 125V DC Distribution Bus B battery fails to operate.

✧ AND-gate CHARGR_DCBUSB: 125V DC Distribution Bus B Battery Chargers fail to operate.

CHARGR_DCBUSB occurs if battery charger D12 and backup battery charger D13 fail to operate simultaneously, represented by basic events CHARGRD12_DCBUSB and CHARGRD13_BACKUP, respectively.

It is important to note that the 480V AC power that supplies the chargers is not modeled in this FT because the loss of AC power is modeled by the entire FTA and would make the top event occur much faster than modeling it in this FT.

6.3.2.5 Emergency 125V DC System Failure – SWGR EA

Figure A-13 shows subtree 125VDC_SWGREA, which is defined as “125V DC System fails to supply power to SWGR EA medium voltage circuit breakers.” This causes the disconnection of the DTF 1 load from SWGR EA. Thus, it is the expansion of TRANSFER-gate 125VDC_SWGREA in subtree DISCONNECT_SWGREA (Figure A-6).

In Figure A-4 and Section 6.3.1, it is shown that all emergency medium voltage circuit breakers on SWGR EA are powered by an independent emergency 125V DC system that is fed by SWGR EA. The emergency 125V DC system can fail if it fails to remain connected SWGR EA or the 125V DC system components fail. Thus, in order for OR-gate 125VDC_SWGREA to occur, the following two events must occur:

➤ OR-gate DISCONN_SWGREA: Failure of MCC to remain connected to Emergency SWGR A.

➤ OR-gate 125VDC: 125V DC system fails to supply power to SWGR EA Medium Voltage Circuit Breakers.

Subtree DISCONN_SWGREA describes the failure of the emergency 125V DC system located in the ESB, to remain connected to SWGR EA. The following seven events are inputs that can make OR-gate DISCONN_SWGREA occur:

⇒ OR-gate DISCONN_MCC: Failure of 125V DC system to remain connected to MCC.

- ⇒ Basic Event MCKTBRKR_O_ESB: Medium Voltage Circuit Breaker fails to remain closed to connect ESB load.
- ⇒ Basic Event FUSE_O_ESB: Fused Interrupter Switch fails to remain closed to connect ESB load.
- ⇒ Basic Event XFMR_ESB: 4160-480V Transformer fails to operate.
- ⇒ Basic Event LINE_ESB: Power line fails to remain intact to connect ESB load.
- ⇒ Basic Event LCKTBRKR_O_ESB: Low Voltage Circuit Breaker fails to remain closed to connect ESB load.
- ⇒ Basic Event IBUS_MCC: MCC bus fails short circuited.

Note that CCF inputs are explained in Section 6.3.4.

Subtree DISCONN_MCC describes the failure of the emergency 125V DC system to remain connected to the MCC located in the ESB as shown in Figure A-4. In order for OR-gate DISCONN_MCC to occur, any of the following two events must occur:

- ✧ Basic Event LINE_125VDC: Power line fails to remain intact to connect 125V DC load.
- ✧ Basic Event LCKTBRKR_O_125VDC: Low Voltage Circuit Breaker fails to remain closed to connect 125V DC.

Subtree 125VDC describes the failure of the emergency 125V DC system components. The following four events are inputs that can make OR-gate 125VDC occur:

- ⇒ Basic Event LCKTBRKR_O_SWGREA: Low Voltage Circuit Breaker fails to remain closed to connect SWGR EA load.
- ⇒ Basic Event LINE_SWGEA: Power line fails to remain intact to connect SWGR EA load.
- ⇒ Basic Event DCBUS_SWGREA: 125V DC distribution bus for SWGR EA fails short circuited.
- ⇒ AND-gate DCPOWER_SWGREA: Loss of DC power to 125VDC distribution bus to SWGR EA.

Note that CCF inputs are explained in Section 6.3.4.

Subtree DCPOWER_SWGREA describes the loss of power to the 125V DC distribution bus from the battery charger and the 125V DC battery cell shown in Figure A-4. In order for AND-gate DCPOWER_SWGREA to occur, the following two events must occur:

- ✧ OR-gate SWGREA_CHARGR: SWGR EA 125V DC battery charger fails to operate.
- ✧ OR-gate SWGREA_BATTERY: SWGR EA 125V DC battery fails to operate.

SWGREA_CHARGR occurs if the battery charger fails to operate or if the low voltage circuit breaker fails to remain closed to connect the battery charger to the 125V DC distribution bus, represented by basic events CHARGR_SWGREA and LCKTBRKR_O_CHARGRA, respectively.

SWGREA_BATTERY occurs if the battery fails to operate or if the low voltage circuit breaker fails to remain closed to connect the battery to the 125V DC distribution bus, represented by basic events BATTERY_SWGREA and LCKTBRKR_O_BATTA.

Note that CCF inputs are explained in Section 6.3.4.

6.3.3 Basic Events Quantification

Once the FT logic model is completed as seen in Figures A-5 through A-13, probabilities of all basic events are assessed (Section 6.2.4). Component failure rate data for this FTA were gathered from two main component reliability information sources: *Generic Component Failure Data Base* (Eide and Calley 1993, Tables 1 and 2) and *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Powered Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)). These sources have compiled failure rate data for use in probabilistic risk assessment from nuclear facilities, fossil-fired generating stations, chemical industries, transmission grids and industrial plants. However, data in *Generic Component Failure Data Base* (Eide and Calley 1993, Tables 1 and 2) is mostly based on nuclear power plant standards.

The collected data represents the failure rate of generic components in failure per million hours (λ) or per demand (q). The *Generic Component Failure Data Base* (Eide and Calley 1993, Tables 1 and 2) shows two modes per component, failure to start and failure to continue operation. The *IEEE Guide* (IEEE Std 500-1984 (Reaffirmed 1991)) has failure rates for specific failure modes of components as well as failure rates that represent the summation of all failure modes.

All component reliability numbers must be converted to probabilities before they are input into SAPHIRE. Equation 3 is used to turn failure rates (λ) into probabilities, while per demand probabilities (q) are already in this form. All generic components used for basic events are compiled in Table 1, which was developed with the use of Microsoft Excel 97.

The first column in Table 1 contains the generic component name as listed in the database. The second column describes the failure mode(s) used in the FT for each component. The failure rates and failure probabilities for each component's failure mode and their units are found in columns three and four, respectively. For components whose specific failure modes were not listed, the number used for the failure rate or probability was conservatively taken as the "all failure" mode, which is the summation of all failure modes, including the needed failure mode. The data source and reference columns identify the source where the data were taken from for each component. The basis for probability column gives the basis for obtaining a probability,

which is given in the next column, for each component to be input for basic events into SAPHIRE. Lastly, the comment column in Table 1 indicates which components in the FT model are represented by those probabilities. It is important to note that SAPHIRE displays only two significant digits.

All basic events in the FT can be found on this table except for CCFs; all undeveloped events termed FAULT_XXX that describe unknown faults in loads connected to the SWGR EA, Main SWGR A, Main SWGR B; and basic event termed PWRCKTBRKRA_230KV that describe the failure of the power circuit breaker configuration in substation A.

The offsite power loss failure rate was gathered from BSC (2004a, Section 5.1.1.48).

The power circuit breakers shown in Figure A-1 as part of Substations A and B, and described in subtree LO SP_SWYDA, are not listed on Table 1. The power circuit breakers are configured by two motor operated disc switches and a medium voltage circuit breaker and thus, is not found as a single component on any database source. Therefore, the failure probability used to represent the failure of the power circuit breaker, as shown on basic event PWRCKTBRKRA_230KV on subtree LO SP_SWYDA, is a combination of two motor operated switches and one medium voltage circuit breaker. This failure probability is 9.2E-6.

All undeveloped events termed FAULT_XXX that describe unknown faults in loads connected to SWGR EA, Main SWGR A, and Main SWGR B are not listed on Table 1.

All undeveloped events in subtree DISCONNECT_SWGRE A are quantified based on the similarities between all MCCs (Assumption 5.2) connected to LC A. Therefore, FAULT_MCCA, FAULT_MCCB, and FAULT_MCCC are given the same failure probability of 1.92E-6 as IBUS_MCCI, which is the fault of the MCC I load.

All undeveloped events in subtree BUS_SWGRE A are quantified based on the similarities between all loads connected to SWGR EA. Therefore, FAULT_LCC, FAULT_MCCS, FAULT_LCG, and FAULT_MCCK are given a failure probability of 3.88E-6, which is obtained by adding BUS_LCA and XFMR_DTF1, described in subtree DISCONNECT_SWGRE A.

Table 1. Basic Event Failure Rates and Probability Calculations

Component/ Subsystem Type	Failure Mode	Failure Rate	Unit	Data Source	Reference	Basis for Probability	Probability of Basic Event in FT Model	Comment
Substation Transformer Liquid Filled, 3 phase 146-242kV	Fails to operate	2.23×10^{-06}	h	IEEE Std 500-1991	p. 392	λt	8.92×10^{-06}	Used for 230kV-12.47kV Main Transformer A
Substation Transformer Liquid Filled, 3 phase 73-145kV	Fails to operate	1.24×10^{-06}	h	IEEE Std 500-1991	p. 391	λt	4.96×10^{-06}	Used for 138kV-12.47kV Main Transformer B
Transmission Tie Transformer - Liquid Filled, 3 phase 2-30kV	Fails to operate	0.49×10^{-06}	h	IEEE Std 500-1991	p. 372	λt	1.96×10^{-06}	Used for 12.47kV-4.16kV Transformer and 4.16kV-480V Transformer
Power Cables	Fails to conduct power	4.84×10^{-06}	h	IEEE Std 500-1991	p. 747	λt	1.94×10^{-05}	Used for all Internal Power Lines
Bus Duct 480V, 3phase 100-1600 Amps	Fails short circuited	0.48×10^{-06}	h	IEEE Std 500-1991	p. 797	λt	1.92×10^{-06}	Used for LCA, LCB, and all MCC Buses
Bare Buses, Outdoor Switchgear	Fails short circuited	0.26×10^{-06}	h	IEEE Std 500-1991	p. 804	λt	1.04×10^{-06}	Used for Main SWGR A and B, Emergency Switchgear A and B, and 125V DC Distribution Bus A and B
Metal Clad Drawout Circuit Breaker Above 600 Amps	Fails to close	0.30×10^{-06}	h	IEEE Std 500-1991	p. 146	λt	1.20×10^{-06}	Used for Medium Voltage Circuit Breakers
	Fails to shed							
	Fails to connect							
Molded Case Circuit Breaker	Fails to close	1.13×10^{-06}	h	IEEE Std 500-1991	p. 124	λt	4.52×10^{-06}	Used for Low Voltage Circuit Breaker
	Fails to shed							
	Fails to connect							
Diesel Generator	Fails to start	1.00×10^{-02}	d	Eide and Calley 1993	p. 1177	q	1.00×10^{-02}	Used for Emergency Diesels A and B
	Fails to operate	5.00×10^{-03}	h	Eide and Calley 1993	p. 1177	λt	2.00×10^{-02}	

Table 1. Basic Event Failure Rates and Probability Calculations (Continued)

Component/ Subsystem Type	Failure Mode	Failure Rate	Unit	Data Source	Reference	Basis for Probability	Probability of Basic Event in FT Model	Comment
Wet Cell Battery	Fails to operate	0.10×10^{-06}	h	IEEE Std 500-1991	p. 76	λt	0.40×10^{-06}	Used for 125V DC Batteries
Battery Charging Unit	Fails to operate	1.69×10^{-06}	h	IEEE Std 500-1991	p. 63	λt	6.76×10^{-06}	Used for 125V DC Battery Chargers
Relay, General	Fails to open	3.00×10^{-04}	d	Eide and Calley 1993	p. 1179	q	3.00×10^{-04}	Used for all Fused Interrupter Switches
	Spurious opening	5.00×10^{-07}	h	Eide and Calley 1993	p. 1179	λt	2.00×10^{-06}	Used for all Fused Interrupter Switches
Offsite Power	Loss	1.10×10^{-05}	h	BSC 2004a	Section 5.1.1.48	λt	4.40×10^{-05}	Used for 230kV Source and 138kV Source
General Switch	Spurious operation	1.00×10^{-06}	h	Eide and Calley 1993	p. 1179	λt	4.00×10^{-06}	Used for Motor Operated Disc Switches on 230kV and 138kV Lines
Transmission Tie Transformer - Liquid Filled, 3 phase 146-242kV	Fails to operate	1.32×10^{-06}	h	IEEE Std 500-1991	p. 375	λt	5.28×10^{-06}	Used for CCVT on Side A
Transmission Tie Transformer - Liquid Filled, 3 phase 73-145kV	Fails to operate	1.02×10^{-06}	h	IEEE Std 500-1991	p. 374	λt	4.08×10^{-06}	Used for CCVT on Side B

NOTES: Mission Time = 4 hr (Assumption 5.4)

q Failure on demand of in-service component

λt Unavailability of in-service components during mission time = $1 - \exp(-\text{Failure rate} \times \text{Mission Time}) \cong \text{Failure rate} \times \text{Mission Time}$
(NRC 1983, Section 5.3.1.1, Eq. 5.1)

All undeveloped events in subtree CBUS_SWYDA are quantified based on the similarities between all loads connected to Main SWGR A. Therefore, FAULT_LC12, FAULT_SWGR01A, FAULT_SWGR08, FAULT_SWGR06, FAULT_2MVA, FAULT_11.7MVA, and FAULT_SWGRC are given a failure probability of 3.00E-6, which is obtained by adding BUS_SWGREA and XFMR_SWGREA, as described in subtree BUS_SWGREA and SWYDA_SWGREA, respectively.

All undeveloped events in subtree CBUS_SWYDB are quantified based on the similarities between all loads connected to Main SWGR B. Therefore, FAULT_SWGR01B, FAULT_LC13, FAULT_SOLAR, FAULT_SWGR09, FAULT_SWGR07, FAULT_3.8MVA, FAULT_11.8MVA, and FAULT_SWGRD are given a failure probability of 3.00E-6, which is obtained by adding BUS_SWGREB and XFMR_SWGREB, as described in subtree BUS_SWGREB and SWYDB_SWGREB, respectively.

The quantification of all CCF events is discussed in the following section.

6.3.4 Common-Cause Failure Analysis

CCF analysis is omitted from the discussion of the fault tree logic model in Section 6.3.2 and basic event quantification in Section 6.3.3 because it cannot be performed until the FT model is built and quantified.

The first step in CCF analysis is identifying which components are identical and redundant in a subsystem and subject to a root cause failure (Section 6.2.5). Figures A-6 through A-13 show subtrees that represent subsystems of the electrical power distribution system. Each subtree is scoped for common events, starting with subtree DISCONNECT_SWGREA in Figure A-6. Common events are determined by type of component and failure mode. If two components are alike and redundant, but have different failure modes, they do not share a root cause failure. Next, the probability of the identified CCF events is derived by multiplying the failure probability of the independent event by the alpha factor found in column four of Table 2.

The first column of Table 2 identifies the number of redundant components subject to CCF in a system. The second column defines how many out of the group are needed for success. The third column contains the formulas used to derive the alpha factor values, which are in column four. These factors are based on a staggered maintenance schedule for the components (Assumption 5.6)

For example, subtree DISCONNECT_SWGREA has three CCF events, CCF_LINE_SWGREAB, CCF_480VBUS_LCAB, and CCF_LCKTBRKR_S_LCA. CCF_LINE_SWGREAB describes the failure of the power lines to remain intact to connect the DTF 1 loads to SWGR EA and SWGR EB. To obtain success, it is necessary that one power line remain intact. This is represented by a basic event termed CCF_LINE_SWGREAB, described as “CCF Power Line (1/2) – DTF 1 load Side A and Side B.” This event is then quantified by multiplying the event failure probability of 1.94E-5 from Table 1 by a factor of 0.047 from Table 2 that represents a 1-out-of-2 success configuration. This results in a failure probability of 9.12E-7 for CCF_LINE_SWGREAB.

Table 2. Alpha Factor Expressions for Common Cause Failure (Staggered Maintenance)

Common Cause Component Group CCG Size	Success Configuration	CCF Probability: Staggered Testing	Value CCF Probability/ q_T - Staggered Testing
2	1 of 2 2 of 2	$\alpha_2 \times q_T$	0.047
3	1 of 3 2 of 3 3 of 3	$\alpha_3 \times q_T$ $(3 \times \alpha_2 / 2 + \alpha_3) \times q_T$	0.026 0.062
4	1 of 4 2 of 4 3 of 4 4 of 4	$\alpha_4 \times q_T$ $(4 \times \alpha_3 / 3 + \alpha_4) \times q_T$ $(4 \times \alpha_2 / 2 + 4 \times \alpha_3 / 3 + \alpha_4) \times q_T$	0.019 0.032 0.075
5	1 of 5 2 of 5 3 of 5 4 of 5 5 of 5	$\alpha_5 \times q_T$ $(5 \times \alpha_4 / 4 + \alpha_5) \times q_T$ $(5 \times \alpha_3 / 3 + 5 \times \alpha_4 / 4 + \alpha_5) \times q_T$ $(5 \times \alpha_2 / 2 + 5 \times \alpha_3 / 3 + 5 \times \alpha_4 / 4 + \alpha_5) \times q_T$	0.015 0.022 0.039 0.085
6	1 of 6 2 of 6 3 of 6 4 of 6 5 of 6 6 of 6	$\alpha_6 \times q_T$ $(6 \times \alpha_5 / 5 + \alpha_6) \times q_T$ $(6 \times \alpha_4 / 4 + 6 \times \alpha_5 / 5 + \alpha_6) \times q_T$ $(6 \times \alpha_3 / 3 + 6 \times \alpha_4 / 4 + 6 \times \alpha_5 / 5 + \alpha_6) \times q_T$ $(6 \times \alpha_2 / 2 + 6 \times \alpha_3 / 3 + 6 \times \alpha_4 / 4 + 6 \times \alpha_5 / 5 + \alpha_6) \times q_T$	0.012 0.018 0.027 0.047 0.091
7	1 of 7 2 of 7 3 of 7 4 of 7 5 of 7 6 of 7 7 of 7	$\alpha_7 \times q_T$ $(7 \times \alpha_6 / 6 + \alpha_7) \times q_T$ $(7 \times \alpha_5 / 5 + 7 \times \alpha_6 / 6 + \alpha_7) \times q_T$ $(7 \times \alpha_4 / 4 + 7 \times \alpha_5 / 5 + 7 \times \alpha_6 / 6 + \alpha_7) \times q_T$ $(7 \times \alpha_3 / 3 + 7 \times \alpha_4 / 4 + 7 \times \alpha_5 / 5 + 7 \times \alpha_6 / 6 + \alpha_7) \times q_T$ $(7 \times \alpha_2 / 2 + 7 \times \alpha_3 / 3 + 7 \times \alpha_4 / 4 + 7 \times \alpha_5 / 5 + 7 \times \alpha_6 / 6 + \alpha_7) \times q_T$	0.010 0.013 0.019 0.030 0.050 0.094
8	1 of 8 2 of 8 3 of 8 4 of 8 5 of 8 6 of 8 7 of 8 8 of 8	$\alpha_8 \times q_T$ $(8 \times \alpha_7 / 7 + \alpha_8) \times q_T$ $(8 \times \alpha_6 / 6 + 8 \times \alpha_7 / 7 + \alpha_8) \times q_T$ $(8 \times \alpha_5 / 5 + 8 \times \alpha_6 / 6 + 8 \times \alpha_7 / 7 + \alpha_8) \times q_T$ $(8 \times \alpha_4 / 4 + 8 \times \alpha_5 / 5 + 8 \times \alpha_6 / 6 + 8 \times \alpha_7 / 7 + \alpha_8) \times q_T$ $(8 \times \alpha_3 / 3 + 8 \times \alpha_4 / 4 + 8 \times \alpha_5 / 5 + 8 \times \alpha_6 / 6 + 8 \times \alpha_7 / 7 + \alpha_8) \times q_T$ $(8 \times \alpha_2 / 2 + 8 \times \alpha_3 / 3 + 8 \times \alpha_4 / 4 + 8 \times \alpha_5 / 5 + 8 \times \alpha_6 / 6 + 8 \times \alpha_7 / 7 + \alpha_8) \times q_T$	0.009 0.011 0.015 0.022 0.034 0.055 0.098

Source: BSC 2004e, Table II-2.

CCF_480VBUS_LCAB describes the failure of the LC A bus and LC B bus. To obtain success, it is necessary that one bus be operating properly. This is represented by a basic event termed CCF_480VBUS_LCAB, described as “CCF 480V Bus (1/2) – LC A Bus & LC B.” This event is then quantified by multiplying the event failure probability of $1.92\text{E-}6$ from Table 1 by a factor of 0.047 from Table 2 that represents a 1-out-of-2 success configuration. This results in a failure probability of $9.02\text{E-}8$ for CCF_480VBUS_LCAB.

CCF_LCKTBRKR_S_LCA describes the failure of the low voltage circuit breakers to shed MCC I, MCC A, MCC B, and MCC C upon demand. To obtain success, it is necessary that all four low voltage circuit breakers be operating properly. This is represented by a basic event termed CCF_LCKTBRKR_S_LCA, described as “CCF Low Voltage Circuit Breaker Shed (4/4) – LC A Bus.” This event is then quantified by multiplying the event failure probability of $4.52\text{E-}6$ from Table 1 by a factor of 0.075 from Table 2 that represents a 4-out-of-4 success configuration. This results in a failure probability of $3.39\text{E-}7$ for CCF_LCKTBRKR_S_LCA.

The OR-gates termed MCCI_LCKTBRKR_S, MCCA_LCKTBRKR_S, MCCB_LCKTBRKR_S, and MCCC_LCKTBRKR_S are a result of including the CCF as a possibility of failure of all low voltage circuit breakers.

The remaining CCF events in Figures A-7 through A-13 are derived in the same fashion as that explained above.

6.4 FAULT TREE ANALYSIS RESULTS

Once the FT has been modeled and failure probabilities have been input into all basic events, the FT is solved with the aid of SAPHIRE to identify and quantify the minimal cut sets (Section 6.2.6). The result is output in a quantitative cut set report.

The summary of the cut set report, shows that the top event can occur from any one of 26 “singles” that combine to give a probability of $9.456\text{E-}5$, any one of 763 “doubles” that combine to give a probability of $2.610\text{E-}8$, and any one of 44 “triples” that combine to give a probability of $1.412\text{E-}13$. All cut sets are added together and result in a final probability of $9.458\text{E-}5$ (Table 3) for the occurrence of the top event in a 4-hour mission time (Assumption 5.4) or $2.365\text{E-}5$ failures per hour. This result applies to the DTF 1, DTF 2, and FHF.

A detailed quantitative cut set list of the top 37 cut sets is shown on Table 3, providing the exact event name(s), event description(s), and failure probability for each cut set, including its percentage contribution to the total probability. Table 3 shows that the dominant contributors to the top event making 76.7 percent of the total probability are three singles, which are independent events. The top three “singles” are independent events that involve the loss of offsite power, a power line failure, and a power circuit breaker failure at Substation A, respectively, and are found in subtree LOSP_SWYDA.

Table 3. SAHPIRE Cut Sets Report for the entire Electrical Power Distribution System with no Emergency Power

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 9.458E-005				
Cut No.	Cutset %	Prob.]	Basic Event	Description
1	46.5	4.4E-005	SOURCE_230KV	LOSS OF 230KV SOURCE
2	20.5	1.9E-005	LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
3	9.7	9.2E-006	PWRCKTBRKRA_230KV	POWER CKT BRKR A FAILS TO REMAIN CLOSED TO CONNECT 230KV POW
4	9.4	8.9E-006	XFMRA_230KV	230-12.47KV MAIN TRANSFORMER A FAILS TO OPERATE
5	5.6	5.3E-006	CCVTA_230KV	COUPLING CAPACITOR VOLTAGE TRANSFORMER A FAILS TO OPERATE
6	1.3	1.2E-006	4KCKTBRKR_O_230KV	4KA MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT 230K
7	1.0	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGRE A & SWGRE B
8	1.0	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGRE A & SWGRE B
9	1.0	9.1E-007	CCF_LINE_SUBAB	CCF POWER LINE (1/2) - SUBSTATIONS A & B
10	1.0	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGRE A & SWGRE B
11	1.0	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
12	0.5	4.3E-007	CCF_PWRCKTBRKR_SUBAB	CCF POWER CIRCUIT BREAKER (1/2) - SUBSTATIONS A & B
13	0.3	2.5E-007	CCF_CCVT_SUBAB	CCF COUPLING CAPACITOR VOLTAGE TRANSFORMER (1/2) - SUBSTATION
14	0.2	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGRE A & SWGRE B
15	0.2	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGRE A & SWGRE B
16	0.2	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGRE A & SWGRE B
17	0.1	9.4E-008	CCF_FUSE_ESB	CCF FUSED INTERRUPTER SWITCH (1/2) - 125VDC SWGRE A & SWGRE B
18	0.1	9.2E-008	CCF_XFMR_ESB	CCF 4160-480V TRANSFORMER (1/2) - 125VDC SWGRE A & SWGRE B
19	0.1	9.0E-008	CCF_480VBUS_LCAB	CCF 480V BUS (1/2) - LC A BUS & LC B BUS
20	0.1	9.0E-008	CCF_MCC_ESB	CCF MCC BUS (1/2) - 125VDC SWGRE A & SWGRE B
21	0.1	5.6E-008	CCF_4KCKTBRKR_O_AB	CCF 4KA MED VOLT CKT BRKR CONNECT (1/2) - SUBSTATIONS A & B
22	0.1	5.6E-008	CCF_MCKTBRKR_ESB	CCF MED VOLT CKT BRKR (1/2) - 125VDC SWGRE A & SWGRE B
23	0.1	5.6E-008	CCF_MCKTBRKR_O_SWYDAB	CCF MEDIUM VOLTAGE CIRCUIT BREAKER CONNECT (1/2) - SWITCHYAR
24	0.1	4.9E-008	CCF_BUS_DCBUSAB	CCF SWITCHGEAR BUS (1/2) - 125V DC DIST BUS A & B
25	0.1	4.9E-008	CCF_BUS_SWYDAB	CCF BUS (1/2) - MAIN SWGRS A & B
26	0.1	4.9E-008	CCF_DCBUS_SWGRAB	CCF DC BUS (1/2) - 125VDC SWGRE A & SWGRE B
27	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
28	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_DTF1B	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
29	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_ESBB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
30	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_MCCIB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCIB LOAD
31	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_SWGEB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREB LOAD
32	0.0	3.8E-010	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_SWGREB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGR EB LOAD
33	0.0	3.8E-010	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
34	0.0	3.8E-010	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_ESB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
35	0.0	3.8E-010	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_MCCI	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCI LOAD
36	0.0	3.8E-010	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_SWGEA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGRE A LOAD
37	0.0	3.8E-010	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			LINE_SWGRE A	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGR EA LOAD

7. SENSITIVITY ANALYSIS

As indicated in Section 6.4, the failure of the electrical power distribution system to distribute power to the nuclear HVAC system in the primary confinement areas of the DTF 1, DTF 2, and FHF is $2.365\text{E-}5/\text{hr}$. Note that this number takes credit for the entire power grid from the offsite source at Substation A to the supply and exhaust fans at each building powered by Emergency SWGRs A and B (Section 6.3), but not for backup or emergency power. This number is approximately four orders of magnitude below the required failure rate of $2.5\text{E-}3/\text{hr}$ mentioned in Section 1, which confirms that the power grid is very reliable. Sections 7.1 through 7.5 discuss other options to meet the required reliability goal, including taking credit for emergency power.

FTA of Emergency Diesel Generators

As mentioned in Section 6.3.1, each emergency SWGR bus has an EDG as a source of emergency power. The EDG is started and connected automatically upon loss of power to the emergency SWGR. Loads on the emergency SWGR are then sequentially reconnected to the bus. Figure A-14 shows subtree EDGA_SWGREA, which represents the failure of the EDG to power the SWGR EA bus. Both EDGs are identical and for practical purposes only, one is explained in this section. Based on the success criterion explained in Section 6.3, only one successful EDG is necessary to keep the top event from occurring. This subtree assumes that if the EDG is successfully started and connected, all appropriate loads to the emergency SWGR bus will be sequentially connected and powered (Assumption 5.3).

There are eight events that are inputs to OR-gate EDGA_SWGREA that if TRUE, can make it occur:

- Basic Event START_EDGA: EDG A fails to start operation.
- Basic Event RUN_EDGA: EDG A fails to continue operation.
- Basic Event MCKTBRKR_O_EDGA: Medium Voltage Circuit Breaker fails to remain closed to connect EDG A.
- Basic Event LINE_EDGA: Power line fails to remain intact to connect EDGA.
- Basic Event CCF_START_EDGAB: CCF Diesel Start (1/2) – EDG A & EDG B.
- Basic Event CCF_RUN_EDGAB: CCF Diesel Run (1/2) – EDG A & EDG B.
- Basic Event CCF_MCKTBRKR_O_EDGAB: CCF Medium Voltage Circuit Breaker Connect (1/2) – EDG A & EDG B.
- Basic Event CCF_LINE_EDGAB: CCF Power Line (1/2) – EDG A & EDG B.

Except for CCFs, the quantification of each basic event was done with the use of Table 1 (Section 6.3.3). CCF events were identified and quantified for redundant components between both EDGs based on Section 6.3.4. The resulting failure probability of EDGA_SWGREA is $3.119\text{E-}2$ in a 4-hour mission time (Assumption 5.4) or $7.798\text{E-}3$ failures per hour.

7.1 FTA OF ENTIRE POWER GRID WITH EMERGENCY POWER

Figure A-15 shows the FT model that credits the entire power grid as well as all emergency power to prevent the occurrence of the top event. The entire power grid with emergency power is the path of power distribution from the offsite power received at Substation A down to the Emergency SWGRs A and B (Figure A-1), which are powered by EDGs A and B, to two MCC Is of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF.

This FT is the same as that explained in Section 6.3.2 with the only difference that the third overall event, which is the loss of power to the emergency SWGR bus, requires two events for failure: failure of the EDG and switchyard to power the emergency SWGR bus. This is represented with AND-gates LO SP_SWGREA and LO SP_SWGREB.

The summary of the cut set report, shows that the top event can occur from 13 “singles” that give a probability of 4.756E-6, any one of 456 “doubles” that combine to give a probability of 1.445E-7, any one of 2454 “triples” that combine to give a probability of 8.189E-8, and 60 “quadruples” that combine to give a probability of 6.561E-13. All cut sets are added together and result in a final probability of 4.982E-6 (Table 4) for the occurrence of the top event in a 4-hour mission time, or 1.246E-6 failures per hour. This result applies to the DTF 1, DTF 2, and FHF.

A detailed quantitative cut set list of the top 27 cut sets is shown in Table 4, providing the exact event name(s), event description(s), and failure probability for each cut set, including its percentage contribution to the total probability. Table 4 shows that the dominant contributors to the top event making 73.2 percent of the total probability are four “singles”, which are CCF events that involve power line failure events that occur on both emergency SWGR buses and are found in subtrees 125VDC_SWGREA and DISCONNECT_SWGREA.

Table 4. SAPHIRE Cut Sets Report for the Entire Power Grid with Emergency Power

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 4.982E-006				
Cut No.	CutSet %	Prob.	Basic Event	Description
1	18.3	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
2	18.3	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
3	18.3	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
4	18.3	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
5	4.3	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
6	4.3	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
7	4.3	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
8	1.9	9.4E-008	CCF_FUSE_ESB	CCF FUSED INTERRUPTER SWITCH (1/2) - 125VDC SWGREA & SWGREB
9	1.9	9.2E-008	CCF_XFMR_ESB	CCF 4160-480V TRANSFORMER (1/2) - 125VDC SWGREA & SWGREB
10	1.8	9.0E-008	CCF_480VBUS_LCAB	CCF 480V BUS (1/2) - LC A BUS & LC B BUS
11	1.8	9.0E-008	CCF_MCC_ESB	CCF MCC BUS (1/2) - 125VDC SWGREA & SWGREB
12	1.1	5.6E-008	CCF_MCKTBRKR_ESB	CCF MED VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
13	1.0	4.9E-008	CCF_DCBUS_SWGRAB	CCF DC BUS (1/2) - 125VDC SWGREA & SWGREB
14	0.8	4.1E-008	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
			SOURCE_230KV	LOSS OF 230KV SOURCE
15	0.4	2.1E-008	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
			SOURCE_230KV	LOSS OF 230KV SOURCE
16	0.4	1.8E-008	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
			LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
17	0.4	1.8E-008	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
			SOURCE_230KV	LOSS OF 230KV SOURCE
18	0.2	9.1E-009	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
			LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
19	0.2	8.8E-009	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			SOURCE_230KV	LOSS OF 230KV SOURCE
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION
20	0.2	8.8E-009	RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
			SOURCE_230KV	LOSS OF 230KV SOURCE
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
21	0.2	8.7E-009	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
			PWRCKTBRKRA_230KV	POWER CKT BRKR A FAILS TO REMAIN CLOSED TO CONNECT 230KV POW
22	0.2	8.4E-009	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
			XFMR_A_230KV	230-12.47KV MAIN TRANSFORMER A FAILS TO OPERATE
23	0.2	7.8E-009	LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
24	0.1	5.0E-009	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
			CCVTA_230KV	COUPLING CAPACITOR VOLTAGE TRANSFORMER A FAILS TO OPERATE
25	0.1	4.4E-009	SOURCE_230KV	LOSS OF 230KV SOURCE
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION
26	0.1	4.3E-009	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
			PWRCKTBRKRA_230KV	POWER CKT BRKR A FAILS TO REMAIN CLOSED TO CONNECT 230KV POW
27	0.1	4.2E-009	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
			XFMR_A_230KV	230-12.47KV MAIN TRANSFORMER A FAILS TO OPERATE

7.2 FTA OF ONE SIDE OF GRID WITH EMERGENCY POWER

From Assumption 5.1, it is known that electrical power to at least one MCC I is sufficient to prevent the failure of the nuclear HVAC system in the primary confinement areas of the DTFs and FHF. Thus, it is not necessary to take credit for the entire grid as evidenced in Sections 6.3.2 through 6.4 and Section 7.1.

Figure A-16 shows the FT model that credits one side of the power grid (Side A) as well as its emergency power (EDG A) to prevent the occurrence of the top event. One side of the power grid with emergency power involves the path of power distribution from the offsite power received at Substation A to Main SWGRs A and B to SWGR EA (Figure A-1), which is powered by EDG A, to an MCC I of the nuclear HVAC system in the primary confinement areas of DTF 1 (Figure A-2), DTF 2, and FHF.

This FT is the same as that explained in Section 7.1 with the exception that only one input, FANS_SIDEA, to the AND-gate LOSEP_ONSITE is analyzed.

The summary of the cut set report, shows that the top event can occur from any one of 33 “singles” that give a probability of $1.380\text{E-}4$, any one of 182 “doubles” that combine to give a probability of $3.694\text{E-}6$, and any one of 59 “triples” that combine to give a probability of $1.988\text{E-}11$. All cut sets are added together and result in a final probability of $1.417\text{E-}4$ (Table 5) for the occurrence of the top event in a 4-hour mission time, or $3.543\text{E-}5$ failures per hour. This result applies to the DTF 1, DTF 2, and FHF.

A detailed quantitative cut set list of the top 38 cut sets is shown in Table 5, providing the exact event name(s), event description(s), and failure probability for each cut set, including its percentage contribution to the total probability. Table 5 shows that the dominant contributors to the top event making 68.5 percent of the total probability are five “singles”, which are independent events that involve power line failure events that occur upstream of SWGR EA and are found in subtrees 125VDC_SWGREA and DISCONNECT_SWGREA.

Table 5. SAPHIRE Cut Sets Report for One Side of Power Grid with Emergency Power

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 1.417E-004				
Cut No.	CutSet %	Prob.	Basic Event	Description
1	13.7	1.9E-005	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
2	13.7	1.9E-005	LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
3	13.7	1.9E-005	LINE_ESB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
4	13.7	1.9E-005	LINE_MCCI	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCI LOAD
5	13.7	1.9E-005	LINE_SWGREA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREA LOAD
6	3.2	4.5E-006	LCKTBRKR_O_125VDC	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT 125VDC
7	3.2	4.5E-006	LCKTBRKR_O_ESB	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
8	3.2	4.5E-006	LCKTBRKR_O_MCCI	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT MCCI
9	3.2	4.5E-006	LCKTBRKR_O_SWGREA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA L
10	1.4	2.0E-006	FUSE_O_DTF1	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT D
11	1.4	2.0E-006	FUSE_O_ESB	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT E
12	1.4	2.0E-006	XFRM_ESB	4160-480V TRANSFORMER FAILS TO OPERATE
13	1.4	2.0E-006	XFRM_DTF1	4160-480V TRANSFORMER FAILS TO OPERATE
14	1.4	1.9E-006	IBUS_LCA	LC A BUS FAILS SHORT CIRCUITED
15	1.4	1.9E-006	IBUS_MCC	MCC BUS FAILS SHORT CIRCUITED
16	1.4	1.9E-006	IBUS_MCCI	MCCI BUS FAILS SHORT CIRCUITED
17	0.9	1.2E-006	MCKTBRKR_O_DTF1	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT DTF1 LOA
18	0.9	1.2E-006	MCKTBRKR_O_ESB	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
19	0.7	1.0E-006	DCBUS_SWGREA	125VDC DISTRIBUTION BUS FOR SWGREA FAILS SHORT CIRCUITED
20	0.7	1.0E-006	IBUS_SWGREA	SWGR EA BUS FAILS SHORT CIRCUITED
21	0.6	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
22	0.6	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
23	0.6	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
24	0.6	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
25	0.6	8.8E-007	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			SOURCE_230KV	LOSS OF 230KV SOURCE
26	0.3	4.4E-007	SOURCE_230KV	LOSS OF 230KV SOURCE
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
27	0.3	3.9E-007	LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
28	0.3	3.9E-007	LINE_SWGREA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGR EA LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
29	0.2	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
30	0.2	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
31	0.2	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
32	0.1	1.9E-007	LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
33	0.1	1.9E-007	LINE_SWGREA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGR EA LOAD
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
34	0.1	1.8E-007	PWRCKTBRKRA_230KV	POWER CKT BRKR A FAILS TO REMAIN CLOSED TO CONNECT 230KV POW
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
35	0.1	1.8E-007	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			XFMRA_230KV	230-12.47KV MAIN TRANSFORMER A FAILS TO OPERATE
36	0.1	1.1E-007	CCVTA_230KV	COUPLING CAPACITOR VOLTAGE TRANSFORMER A FAILS TO OPERATE
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
37	0.1	9.4E-008	CCF_FUSE_ESB	CCF FUSED INTERRUPTER SWITCH (1/2) - 125VDC SWGREA & SWGREB
38	0.1	9.2E-008	CCF_XFRM_ESB	CCF 4160-480V TRANSFORMER (1/2) - 125VDC SWGREA & SWGREB

7.3 FTA OF ONE SIDE OF GRID WITH NO EMERGENCY POWER

From Assumption 5.1, it is known that electrical power to at least one MCC I is sufficient to prevent the failure of the nuclear HVAC system in the primary confinement areas of the DTFs and FHF. Thus, it is not necessary to take credit for the entire grid as evidenced in Sections 6.3.2 through 6.4 and Section 7.1.

Figure A-17 shows the FT model that credits one side of the power grid with no emergency power to prevent the occurrence of the top event. One side of the power grid without emergency power involves the path of power distribution from the offsite power received at Substation A to Main SWGRs A and B to SWGR EA (Figure A-1), then to an MCC I of the nuclear HVAC system in the primary confinement areas of DTF 1 (Figure A-2), DTF 2, and FHF.

This FT is the same as that explained in Section 7.2 with the exception that the third input, AND-gate LOSP_SWGRE, is replaced with TRANSFER-gate SWYDA_SWGRE.

The summary of the cut set report, shows that the top event can occur from any one of 53 “singles” that give a probability of 2.555E-4, any one of 38 “doubles” that combine to give a probability of 7.211E-10, and eight “triples” that combine to give a probability of 1.021E-14. All cut sets are added together and result in a final probability of 2.555E-4 (Table 6) for the occurrence of the top event in a 4-hour mission time, or 6.388E-5 failures per hour. This result applies to the DTF 1, DTF 2, and FHF.

A detailed quantitative cut set list of the top 47 cut sets is shown in Table 6, providing the exact event name(s), event description(s) and failure probability for each cut set, including its percentage contribution to the total probability. Table 6 shows that the dominant contributors to the top event making 70.4 percent of the total probability are eight “singles”, which are independent events that involve loss of offsite power at Substation A, and power line failure events that occur at Substation A, the 125VDC emergency distribution system, and that cause the disconnection of the MCC I load, DTF 1 load, and SWGR EA load. These events are found in subtrees DISCONNECT_SWGRE, SWYDA_SWGRE, 125VDC_SWGRE and LOSP_SWYDA.

Table 6. SAPHIRE Cut Sets Report for One Side of Grid with No Emergency Power

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 2.555E-004				
Cut No.	CutSet %	Prob.	Basic Event	Description
1	17.2	4.4E-005	SOURCE_230KV	LOSS OF 230KV SOURCE
2	7.6	1.9E-005	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
3	7.6	1.9E-005	LINE_230KV	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 230KV POWER
4	7.6	1.9E-005	LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
5	7.6	1.9E-005	LINE_ESB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
6	7.6	1.9E-005	LINE_MCCI	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCI LOAD
7	7.6	1.9E-005	LINE_SWGEA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREA LOAD
8	7.6	1.9E-005	LINE_SWGREA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGR EA LOAD
9	3.6	9.2E-006	PWRCKTBRKRA_230KV	POWER CKT BRKR A FAILS TO REMAIN CLOSED TO CONNECT 230KV POW
10	3.5	8.9E-006	XFMR_A_230KV	230-12.47KV MAIN TRANSFORMER A FAILS TO OPERATE
11	2.1	5.3E-006	CCVTA_230KV	COUPLING CAPACITOR VOLTAGE TRANSFORMER A FAILS TO OPERATE
12	1.8	4.5E-006	LCKTBRKR_O_125VDC	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT 125VDC
13	1.8	4.5E-006	LCKTBRKR_O_ESB	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
14	1.8	4.5E-006	LCKTBRKR_O_MCCI	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT MCCI
15	1.8	4.5E-006	LCKTBRKR_O_SWGREA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA
16	0.8	2.0E-006	FUSE_O_DTF1	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT
17	0.8	2.0E-006	FUSE_O_ESB	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT
18	0.8	2.0E-006	FUSE_O_SWGREA	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT
19	0.8	2.0E-006	XFMR_ESB	4160-480V TRANSFORMER FAILS TO OPERATE
20	0.8	2.0E-006	XFMR_SWGREA	12.47-4.16KV TRANSFORMER FAILS TO OPERATE
21	0.8	2.0E-006	XFMR_DTF1	4160-480V TRANSFORMER FAILS TO OPERATE
22	0.8	1.9E-006	IBUS_LCA	LC A BUS FAILS SHORT CIRCUITED
23	0.8	1.9E-006	IBUS_MCC	MCC BUS FAILS SHORT CIRCUITED
24	0.8	1.9E-006	IBUS_MCCI	MCCI BUS FAILS SHORT CIRCUITED
25	0.5	1.2E-006	4KCKTBRKR_O_230KV	4KA MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT 230K
26	0.5	1.2E-006	MCKTBRKR1_O_SWGREA	MED VOLT CKT BRKR 1 FAILS TO REMAIN CLOSED TO CONNECT SWGR
27	0.5	1.2E-006	MCKTBRKR2_O_SWGREA	MED VOLT CKT BRKR 2 FAILS TO REMAIN CLOSED TO CONNECT SWGR
28	0.5	1.2E-006	MCKTBRKR_O_DTF1	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT DTF1 LOA
29	0.5	1.2E-006	MCKTBRKR_O_ESB	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
30	0.4	1.0E-006	DCBUS_SWGREA	125VDC DISTRIBUTION BUS FOR SWGREA FAILS SHORT CIRCUITED
31	0.4	1.0E-006	IBUS_SWGREA	SWGR EA BUS FAILS SHORT CIRCUITED
32	0.4	1.0E-006	IBUS_SWYDA	MAIN SWGR A BUS FAILS SHORT CIRCUITED
33	0.4	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
34	0.4	9.1E-007	CCF_LINE_DCBUSAB	CCF POWER LINE (1/2) - 125V DC DIST BUS A & B
35	0.4	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
36	0.4	9.1E-007	CCF_LINE_SUBAB	CCF POWER LINE (1/2) - SUBSTATIONS A & B
37	0.4	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
38	0.4	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
39	0.2	4.3E-007	CCF_PWRCKTBRKR_SUBAB	CCF POWER CIRCUIT BREAKER (1/2) - SUBSTATIONS A & B
40	0.1	2.5E-007	CCF_CCVT_SUBAB	CCF COUPLING CAPACITOR VOLTAGE TRANSFORMER (1/2) - SUBSTATION
41	0.1	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
42	0.1	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
43	0.1	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
44	0.0	9.4E-008	CCF_FUSE_ESB	CCF FUSED INTERRUPTER SWITCH (1/2) - 125VDC SWGREA & SWGREB
45	0.0	9.2E-008	CCF_XFMR_ESB	CCF 4160-480V TRANSFORMER (1/2) - 125VDC SWGREA & SWGREB
46	0.0	9.0E-008	CCF_480VBUS_LCAB	CCF 480V BUS (1/2) - LC A BUS & LC B BUS
47	0.0	9.0E-008	CCF_MCC_ESB	CCF MCC BUS (1/2) - 125VDC SWGREA & SWGREB

7.4 FTA OF EMERGENCY POWER ONLY-TWO SIDES

Another option to meet the required reliability goal includes taking credit for emergency power only on side A and B to power the MCC Is.

Figure A-18 shows the FT model that credits two sides of the power grid with only emergency power to prevent the occurrence of the top event. Emergency power on both sides of the power grid involves the path of power distribution from emergency SWGRs A and B, which are powered by EDG A and EDG B (Figure A-1), to two MCC Is of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF.

This FT is the same as that explained in Section 6.3.2 with the only difference that the third overall event, which is the loss of power to the emergency SWGR bus, depends solely on the failure of the EDG to power the emergency SWGR bus. This is represented with TRANSFER-gates EDGA_SWGREa and EDGB_SWGREB.

The summary of the cut set report, shows that the top event can occur from any one of 17 “singles” that give a probability of 1.415E-3, any one of 580 “doubles” that combine to give a probability of 9.090E-4, and any one of 68 “triples” that combine to give a probability of 5.309E-12. All cut sets are added together and result in a final probability of 2.323E-3 (Table 7) for the occurrence of the top event in a 4-hour mission time, or 5.808E-4 failures per hour. It is important to note that this number does not reflect the failure rate of offsite power, which is 1.1E-5/hr (BSC 2004a, Section 5.1.1.48). This result applies to the DTF 1, DTF 2 and FHF.

A detailed quantitative cut set list of the top 27 cut sets is shown on Table 7, providing the exact event name(s), event description(s), and failure probability for each cut set, including its percentage contribution to the total probability. Table 7 shows that the dominant contributors to the top event making 60.7 percent of the total probability are two “singles”, which are CCF events that involve the start and continuing operation of both EDGs and are found in subtrees EDGA_SWGREa and EDGB_SWGREB.

Table 7. SAPHIRE Cut Sets Report of the Emergency Power Only – Two Sides

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 2.323E-003				
Cut No.	CutSet %	Prob.]	Basic Event	Description
1	40.5	9.4E-004	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
2	20.2	4.7E-004	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
3	17.2	4.0E-004	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
4	8.6	2.0E-004	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION
5	8.6	2.0E-004	RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
6	4.3	1.0E-004	START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION
7	0.0	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
8	0.0	9.1E-007	CCF_LINE_EDGAB	CCF POWER LINE (1/2) - EMERGENCY DIESEL GENS A & B
9	0.0	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
10	0.0	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
11	0.0	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
12	0.0	3.9E-007	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
13	0.0	3.9E-007	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
14	0.0	3.9E-007	LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
15	0.0	3.9E-007	LINE_DTF1B	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
16	0.0	3.9E-007	LINE_EDGA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT EDG A
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
17	0.0	3.9E-007	LINE_EDGB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT EDG B
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
18	0.0	3.9E-007	LINE_ESB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
19	0.0	3.9E-007	LINE_ESBB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
20	0.0	3.9E-007	LINE_MCCI	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCI LOAD
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
21	0.0	3.9E-007	LINE_MCCIB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCIB LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
22	0.0	3.9E-007	LINE_SWGEA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREA LOAD
			RUN_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO CONTINUE OPERATION
23	0.0	3.9E-007	LINE_SWGEB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREB LOAD
			RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
24	0.0	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
25	0.0	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
26	0.0	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
27	0.0	1.9E-007	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION
28	0.0	1.9E-007	LINE_125VDCB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
			START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
29	0.0	1.9E-007	LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
			START_EDGB	EMERGENCY DIESEL GENERATOR B FAILS TO START OPERATION

7.5 FTA OF EMERGENCY POWER ONLY – ONE SIDE

From Assumption 5.1, it is known that electrical power to at least one MCC I is sufficient to prevent the failure of the nuclear HVAC system in the primary confinement areas of the DTFs and FHF. Thus, it is not necessary to take credit for emergency power on sides A and B of the power grid as was done in Section 7.4.

Figure A-19 shows the FT model that credits one side of the power grid with only emergency power to prevent the occurrence of the top event. Emergency power on one side of the power grid involves the path of power distribution from SWGR EA, which is powered by EDG A (Figure A-1), to one MCC I of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF.

This FT is the same as that explained in Section 7.4 with the exception that only one input, FANS_SIDEA, to the AND-gate LOSEP_ONSITE is analyzed.

The summary of the cut set report, shows that the top event can occur from any one of 41 “singles” that give a probability of $3.132\text{E-}2$, any one of 22 “doubles” that combine to give a probability of $8.853\text{E-}11$, and any one of four “triples” that combine to give a probability of $5.773\text{E-}15$. All cut sets are added together and result in a final probability of $3.132\text{E-}2$ (Table 8) for the occurrence of the top event in a 4-hour mission time, or $7.830\text{E-}3$ failures per hour. It is important to note that this number does not reflect the failure rate of offsite power, which is $1.1\text{E-}5/\text{hr}$ (BSC 2004a, Section 5.1.1.48). This result applies to the DTF 1, DTF 2, and FHF.

A detailed quantitative cut set list of the top 44 cut sets is shown in Table 8, providing the exact event name(s), event description(s), and failure probability for each cut set, including its percentage contribution to the total probability. Table 8 shows that the dominant contributors to the top event making 95.8 percent of the total probability are two “singles”, which are independent events that involve the start and continuing operation of EDG A and are found in subtree EDGA_SWGREA.

Table 8. SAPHIRE Cut Sets Report of the Emergency Power Only – One Side.

FAULT TREE CUT SETS REPORT				
Fault Tree: LOSP_ONSITE				
Total Failure Probability : 3.132E-002				
Cut No.	CutSet %	Prob.	Basic Event	Description
1	63.9	2.0E-002	RUN_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO CONTINUE OPERATION
2	31.9	1.0E-002	START_EDGA	EMERGENCY DIESEL GENERATOR A FAILS TO START OPERATION
3	3.0	9.4E-004	CCF_RUN_EDGAB	CCF DIESEL RUN (1/2) - EMERGENCY DIESEL GENS A & B
4	1.5	4.7E-004	CCF_START_EDGAB	CCF DIESEL START (1/2) - EMERGENCY DIESEL GENS A & B
5	0.1	1.9E-005	LINE_125VDC	POWER LINE FAILS TO REMAIN INTACT TO CONNECT 125VDC LOAD
6	0.1	1.9E-005	LINE_DTF1	POWER LINE FAILS TO REMAIN INTACT TO CONNECT DTF1 LOAD
7	0.1	1.9E-005	LINE_EDGA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT EDG A
8	0.1	1.9E-005	LINE_ESB	POWER LINE FAILS TO REMAIN INTACT TO CONNECT ESB LOAD
9	0.1	1.9E-005	LINE_MCCI	POWER LINE FAILS TO REMAIN INTACT TO CONNECT MCCI LOAD
10	0.1	1.9E-005	LINE_SWGEA	POWER LINE FAILS TO REMAIN INTACT TO CONNECT SWGREA LOAD
11	0.0	4.5E-006	LCKTBRKR_O_125VDC	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT 125VDC
12	0.0	4.5E-006	LCKTBRKR_O_ESB	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
13	0.0	4.5E-006	LCKTBRKR_O_MCCI	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT MCCI
14	0.0	4.5E-006	LCKTBRKR_O_SWGREA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA
15	0.0	2.0E-006	FUSE_O_DTF1	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT
16	0.0	2.0E-006	FUSE_O_ESB	FUSED INTERRUPTER SWITCH FAILS TO REMAIN CLOSED TO CONNECT
17	0.0	2.0E-006	XFMR_ESB	4160-480V TRANSFORMER FAILS TO OPERATE
18	0.0	2.0E-006	XFRM_DTF1	4160-480V TRANSFORMER FAILS TO OPERATE
19	0.0	1.9E-006	IBUS_LCA	LC A BUS FAILS SHORT CIRCUITED
20	0.0	1.9E-006	IBUS_MCC	MCC BUS FAILS SHORT CIRCUITED
21	0.0	1.9E-006	IBUS_MCCI	MCCI BUS FAILS SHORT CIRCUITED
22	0.0	1.2E-006	MCKTBRKR_O_DTF1	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT DTF1 LOA
23	0.0	1.2E-006	MCKTBRKR_O_EDGA	MED VOLT CKT BRKR FAILS TO OPERATE TO CONNNECT EDG A
24	0.0	1.2E-006	MCKTBRKR_O_ESB	MED VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT ESB LOAD
25	0.0	1.0E-006	DCBUS_SWGREA	125VDC DISTRIBUTION BUS FOR SWGREA FAILS SHORT CIRCUITED
26	0.0	1.0E-006	IBUS_SWGREA	SWGR EA BUS FAILS SHORT CIRCUITED
27	0.0	9.1E-007	CCF_LINE_125VDC	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
28	0.0	9.1E-007	CCF_LINE_EDGAB	CCF POWER LINE (1/2) - EMERGENCY DIESEL GENS A & B
29	0.0	9.1E-007	CCF_LINE_ESB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
30	0.0	9.1E-007	CCF_LINE_SWGRAB	CCF POWER LINE (1/2) - 125VDC SWGREA & SWGREB
31	0.0	9.1E-007	CCF_LINE_SWGREAB	CCF POWER LINE (1/2) - DTF1 LOAD SIDE A AND SIDE B
32	0.0	2.1E-007	CCF_LCKTBRKR_125VDC	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
33	0.0	2.1E-007	CCF_LCKTBRKR_ESB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
34	0.0	2.1E-007	CCF_LCKTBRKR_SWGRAB	CCF LOW VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
35	0.0	9.4E-008	CCF_FUSE_ESB	CCF FUSED INTERRUPTER SWITCH (1/2) - 125VDC SWGREA & SWGREB
36	0.0	9.2E-008	CCF_XFMR_ESB	CCF 4160-480V TRANSFORMER (1/2) - 125VDC SWGREA & SWGREB
37	0.0	9.0E-008	CCF_480VBUS_LCAB	CCF 480V BUS (1/2) - LC A BUS & LC B BUS
38	0.0	9.0E-008	CCF_MCC_ESB	CCF MCC BUS (1/2) - 125VDC SWGREA & SWGREB
39	0.0	5.6E-008	CCF_MCKTBRKR_ESB	CCF MED VOLT CKT BRKR (1/2) - 125VDC SWGREA & SWGREB
40	0.0	5.6E-008	CCF_MCKTBRKR_O_EDGAB	CCF MED VOLT CKT BRKR CONNECT (1/2) -EMERGENCY DIESEL GENS
41	0.0	4.9E-008	CCF_DCBUS_SWGRAB	CCF DC BUS (1/2) - 125VDC SWGREA & SWGREB
42	0.0	3.1E-011	CHARGR_SWGREA	SWGREA 125VDC BATTERY CHARGER FAILS TO OPERATE
43	0.0	2.0E-011	LCKTBRKR_O_BATTA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA
			LCKTBRKR_O_BATTA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA
			LCKTBRKR_O_CHARGRA	LOW VOLT CKT BRKR FAILS TO REMAIN CLOSED TO CONNECT SWGREA
44	0.0	8.6E-012	FAULT_MCCA	MCC A LOAD FAILURE
			LCKTBRKR_S_MCCA	LOW VOLT CKT BRKR FAILS TO SHED MCC A LOAD UPON DEMAND

8. CONCLUSIONS AND RECOMMENDATIONS

The FTA for the electrical power distribution system presented in Sections 6.3 through 6.4 and the sensitivity analyses presented in Sections 7.1, 7.2, 7.3, 7.4, and 7.5 demonstrate that the probability of loss of power to the nuclear HVAC system in the primary confinement areas of the DTF 1, DTF 2, and FHF, due to a loss of offsite and onsite electrical power distribution, is less than the design requirement failure rate of $2.5\text{E-}3$ per hour (BSC 2004a, Section 5.1.1.48). A summary of the FTAs presented in this report is shown in Table 9.

The first FTA presented in Sections 6.3 through 6.4 credits the entire power grid, without emergency power, to prevent the occurrence of the top event. The entire power grid is the path of power distribution from the offsite power received at Substation A down to emergency SWGRs A and B (Figure A-1) to two MCC Is of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. This also includes the normal and emergency 125V DC system, which are support systems to the power grid (Figure A-3 and A-4). The FTA results give a failure rate of $2.365\text{E-}5$ per hour, which is only 0.95 percent of the reliability requirement and leaves 99.05 percent for HVAC mechanical failure.

The FTA presented in Section 7.1 credits the entire power grid, with emergency power, to prevent the occurrence of the top event. The entire power grid with emergency power is the path of power distribution from the offsite power received at Substation A down to the emergency SWGRs A and B (Figure A-1), including EDG A and EDG B, to two MCC Is of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. This FTA results in a failure rate of $1.246\text{E-}6$ per hour, which is 0.05 percent of the reliability requirement and leaves 99.95 percent for HVAC mechanical failure.

The FTA presented in Section 7.2 credits one side of the power grid, with emergency power, to prevent the occurrence of the top event. One side of the power grid with emergency power involves the path of power distribution from the offsite power received at Substation A down to Main SWGR A and Main SWGR B down to SWGR EA (Figure A-1), including EDG A, to one MCC I of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. This FTA results in a failure rate of $3.543\text{E-}5$ per hour, which is only 1.42 percent of the reliability requirement and leaves 98.58 percent for HVAC mechanical failure.

The FTA presented in Section 7.3 credits one side of the power grid, without emergency power, to prevent the occurrence of the top event. One side of the power grid without emergency power involves the path of power distribution from the offsite power received at Substation A down to the Main SWGR A and Main SWGR B down to SWGR EA (Figure A-1), to one MCC I of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. This FTA results in a failure rate of $6.388\text{E-}5$ per hour, which is only 2.56 percent of the reliability requirement and leaves 97.44 percent for HVAC mechanical failure.

The FTA presented in Section 7.4 credits only emergency power on both sides of the power grid to prevent the occurrence of the top event. Emergency power on both sides of the power grid involves the path of power distribution from the emergency SWGRs A and B, powered by EDGs A and B (Figure A-1), to two MCC Is of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. Including loss of offsite power, this results in

a failure rate of $5.918\text{E-}4$ per hour, which is 23.67 percent of the reliability requirement and leaves 76.33 percent for HVAC mechanical failure.

The last FTA presented in Section 7.5 credits only emergency power on one side of the power grid to prevent the occurrence of the top event. Emergency power on one side of the power grid involves the path of power distribution from SWGR EA, powered by EDG A (Figure A-1), to one MCC I of the nuclear HVAC system in the primary confinement areas of the DTF 1 (Figure A-2), DTF 2, and FHF. Including the loss of offsite power, this results in a failure rate of $7.841\text{E-}3$ per hour, which is over $2.5\text{E-}3$ per hour and thus, does not satisfy the reliability requirement.

In order to limit the amount of components credited to prevent the top event and still meet the reliability requirement of $2.5\text{E-}3$ per hour, while leaving room for mechanical failure, it is recommended that credit be taken for either one side of the power grid with no emergency power (Section 7.3) or emergency power only on both sides of the power grid (Section 7.4).

The results presented in this analysis indicate that the outputs are reasonable compared to the identified inputs and that the results are suitable for their intended use.

Table 9. Summary of Fault Tree Analyses

Fault Tree Analysis		Failure Rate ^a (h ⁻¹)
Entire Power Grid	No Emergency Power	$2.365\text{E-}5$
	Emergency Power	$1.246\text{E-}6$
One Side of Power Grid	No Emergency Power	$6.388\text{E-}5$
	Emergency Power	$3.543\text{E-}5$
Emergency Power Only	Both Sides of Power Grid	$5.918\text{E-}4$
	One Side of Power Grid	$7.841\text{E-}3$

NOTE: ^a Failure rates reflect loss of offsite power $1.1\text{E-}5$ per hour (BSC 2004a, Section 5.1.1.48).

9. REFERENCES

9.1 DOCUMENTS CITED

- 160873 BSC (Bechtel SAIC Company) 2002. *Software Code: SAPHIRE*. V7.18. PC - Windows 2000/NT 4.0. 10325-7.18-00.
- 169234 BSC (Bechtel SAIC Company) 2003. *Independent Verification and Validation Report for Legacy Code SAPHIRE V7.18*. STN: 10325-7.18-00. Las Vegas, Nevada: Bechtel SAIC Company. ACC: [MOL.20040112.0070](#).
- 171429 BSC (Bechtel SAIC Company) 2004a. *Categorization of Event Sequences for License Application*. 000-00C-MGR0-00800-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. TBV#7102.
- 171342 BSC (Bechtel SAIC Company) 2004b. *Electrical Power System Description Document*. 000-3YD-EE00-00200-000-003. Las Vegas, Nevada: Bechtel SAIC Company. TBV#7022.
- 171210 BSC (Bechtel SAIC Company) 2004c. *Switchyard Switchgear Bldg Single Line Diagram 125 V DC System*. 27A-E10-EEC0-00201-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: [ENG.20040518.0005](#).
- 171491 BSC (Bechtel SAIC Company) 2004d. *Reliability Analysis of the Mechanical System in Selected Portions of the Nuclear HVAC System*. 100-PSA-MGR0-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. TBV#7109.
- 169554 BSC (Bechtel SAIC Company) 2004e. *Waste Package Transporter Preclosure Safety Analysis*. 800-MQC-HET0-00200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: [ENG.20040623.0002](#).
- 171539 DOE (U.S. Department of Energy) 2004. *Quality Assurance Requirements and Description*. DOE/RW-0333P, Rev. 16. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: [DOC.20040907.0002](#).
- 146564 Eide, S.A. and Calley, M.B. 1993. "Generic Component Failure Data Base." PSA '93, Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, Clearwater Beach, Florida, January 26-29, 1993. 2, 1175-1182. La Grange Park, Illinois: American Nuclear Society. TIC: [247455](#).
- 171825 IEEE Std 500-1984 (Reaffirmed 1991). 1991 IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations. New York, New York: Institute of Electrical and Electronics Engineers. TIC: [256281](#).

- 167710 Marshall, F.M.; Rasmuson, D.M.; and Mosleh, A. 1998. *Common-Cause Failure Parameter Estimations*. NUREG/CR-5497. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: [MOL.20040220.0105](#).
- 167711 Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: [MOL.20040220.0106](#).
- 106591 NRC (U.S. Nuclear Regulatory Commission) 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: [205084](#).
- 128494 Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook*. NUREG - 0492. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: [208328](#).

9.2 CODES, STANDARDS, REGULATIONS AND PROCEDURES

AP-3.12Q. *Design Calculations and Analyses*.

AP-3.15Q. *Managing Technical Product Inputs*.

LP-SI.11Q-BSC. *Software Management*.

ATTACHMENT A
ELECTRICAL POWER DISTRIBUTION SYSTEM ARCHITECTURE AND FAULT
TREE MODEL - SIDE A

INTENTIONALLY LEFT BLANK

Source: BSC 2004b, Figure 4-3

Figure A-1. Electrical Power Distribution System for the Monitored Geologic Repository

INTENTIONALLY LEFT BLANK

Figure A-2. Electrical Power Distribution from LC A and LC B to Supply and Exhaust Fan Motors (Assumption 5.7)

INTENTIONALLY LEFT BLANK

Source: BSC 2004c

Figure A-3. Normal 125V DC Power Distribution System

INTENTIONALLY LEFT BLANK

Source: BSC 2004b, Figure 4-1

Figure A-4. Emergency 125V DC Power Distribution Systems

INTENTIONALLY LEFT BLANK

Figure A-5. FT Model of the Electrical Power Distribution System with no Emergency Power

INTENTIONALLY LEFT BLANK

Figure A-6. Subtree DISCONNECT_SWGREA

INTENTIONALLY LEFT BLANK

Figure A-7. Subtree BUS_SWGREA

INTENTIONALLY LEFT BLANK

Figure A-8. Subtree SWYDA_SWGRE A

INTENTIONALLY LEFT BLANK

Figure A-9. Subtree CBUS_SWYDA

INTENTIONALLY LEFT BLANK

Figure A-10. Subtree CBUS_SWYDB

INTENTIONALLY LEFT BLANK

Figure A-11. Subtree LO SP, SWYDA

INTENTIONALLY LEFT BLANK

Figure A-12. FT Model of the Normal 125V DC Distribution System

INTENTIONALLY LEFT BLANK

Figure A-13. FT Model of the Emergency 125V DC Distribution System

INTENTIONALLY LEFT BLANK

Figure A-14. FT Model of the Emergency Diesel Generator A

Figure A-15. FT Model of Entire Power Grid with Emergency Power

Figure A-16. FT Model of One Side of Power Grid with Emergency Power

Figure A-17. FT Model of One Side of Power Grid with No Emergency Power

Figure A-18. FT Model of the Emergency Power Only – Two Sides

Figure A-19. FT Model of Emergency Power Only - One Side

ATTACHMENT B
FAULT TREE MODEL - SIDE B

INTENTIONALLY LEFT BLANK

Figure B-1. Subtree DISCONNECT_SWGREB

INTENTIONALLY LEFT BLANK

Figure B-2. Subtree BUS_SWGREB

INTENTIONALLY LEFT BLANK

Figure B-3. Subtree SWYDB_SWGREB

INTENTIONALLY LEFT BLANK

Figure B-4. Subtree 12VDC_SIDE B

INTENTIONALLY LEFT BLANK

Figure B-5. Subtree 125VDC_SWGREB

INTENTIONALLY LEFT BLANK

Figure B-6. Subtree EDGB_SWGREB

INTENTIONALLY LEFT BLANK