ENG.20050315.0003

OCRWM	DESIGN CALCULATION OR ANALYSIS COVER SHEET	1. QA: QA 2. Page 1

3. System
Monitored Geologic Repository

4. Document Identifier
100-PSA-MGR0-00100-000-00A

5. Title
Reliability Analysis of the Mechanical System in Selected Portions of the Nuclear HVAC System

6. Group
Preclosure Safety Analysis

7. Document Status Designation
☒ Preliminary □ Final □ Cancelled

8. Notes/Comments

NOTICE OF OPEN CHANGE DOCUMENTS - THIS DOCUMENT IS IMPACTED BY THE LISTED CHANGE DOCUMENTS AND CANNOT BE USED WITHOUT THEM.

--

1) ECN-001, DATED 08/11/2005

Attachments	Total Number of Pages
Attachment A Architecture of the DTF 1 Primary Confinement Nuclear HVAC System	12
Attachment B Architecture of the FHF Primary Confinement Nuclear HVAC System	10
Attachment C Fault Tree Model for the DTF 1 Primary Confinement Nuclear HVAC System	14
Attachment D Fault Tree Model for the FHF Primary Confinement Nuclear HVAC System	14
Attachment E Glossary	2

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	113	E-2	N. Ramirez 3/14/05	S. F. Alex Deng 03/14/05	A. Barnes 3/14/2005	D. Richardson Dennis Richardson	3/14/05

CONTENTS

Page

FIGURES

TABLES

ACRONYMS

AHU	air-handling unit
CCCG	common-cause component group
CCF	common-cause failure
CSNF	commercial spent nuclear fuel
DTF	Dry Transfer Facility
FHF	Fuel Handling Facility
FT	fault tree
FTA	fault tree analysis
HEPA	high-efficiency particulate air
HVAC	heating, ventilation, and air-conditioning
NRC	U.S. Nuclear Regulatory Commission

1. PURPOSE

The purpose of this analysis is to determine the probability of occurrence of the unavailability of the nuclear heating, ventilation, and air-conditioning (HVAC) systems in the primary confinement areas of the Dry Transfer Facilities (DTFs) and Fuel Handling Facility (FHF) due to equipment failure. In addition, this analysis summarizes the results of the overall reliability of the HVAC systems in the primary confinement areas of the DTFs and FHF.

A design requirement that will ensure that the probability that the HVAC system, including HEPA filtration, in the primary confinement areas of the DTF and FHF becomes unavailable during a 4-h mission time is 0.01 or less without credit for backup electrical power (BSC 2005, Section 5.1.1.48). This corresponds to an hourly HVAC failure rate of 2.5E-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 failure of onsite power distribution. Thus, to meet the threshold requirement aforementioned, the failure rate of mechanical equipment, the loss of offsite power, and the failure of onsite power distribution must be less than or equal to 2.5E-3 per hour for the nuclear HVAC systems in the primary confinement areas of the DTFs and FHF. The failure of onsite power distribution, including the loss of offsite power, has been evaluated in *Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System* (BSC 2004a, Section 7.3).

Because the designs of the nuclear HVAC for the DTFs and the FHF are conceptual in nature, the intended use of this analysis is to provide estimates of HVAC reliability and develop solutions to support conceptual and preliminary design activities to provide reasonable assurance that the unavailability requirement can be achieved. The scope of this analysis is limited to evaluating the reliability of the HVAC systems in the primary confinement areas of the DTFs and the FHF.

A glossary of terms is provided in Attachment E. In some cases, meanings of words are slightly different in reliability analyses than traditionally used in nuclear power plant discussions.

2. QUALITY ASSURANCE

The development of this analysis is subject to the requirements of *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 LP-3.15Q-BSC, *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) (BSC 2002)
- 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 uses an integrated event tree/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 obtained from Software Configuration Management. Independent software testing and verification using test cases of physical problems is 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 this 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 Sections 6.3 and 6.3.3. User-defined formulas, input, and results are documented in sufficient detail in Sections 6.1 through 6.4 to allow for 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 The system architecture for the DTF 1 primary confinement HVAC system is established by *Dry Transfer Facility #1 Primary Confinement HVAC System Block Flow Diagram* (BSC 2004b), *Dry Transfer Facility #1 Primary Supply HVAC System Air Handling Unit Ventilation Flow Diagram* (BSC 2004c), *Dry Transfer Facility #1 Primary Confinement HVAC System Air Distribution Ventilation Flow Diagram* (BSC 2004d), *Dry Transfer Facility #1 Primary Confinement HVAC System Remote HEPA Filters Ventilation Flow Diagram* (BSC 2004e), and *Dry Transfer Facility #1 Primary Confinement HVAC System Exhaust Ventilation Flow Diagram* (BSC 2004f). These inputs contain the best design information available to proceed with a meaningful analysis of the system reliability.

Because this calculation is a preliminary estimate of the reliability, to ensure feasibility of the design, these drawings are reasonable for use. Revisions and clarifications to these drawings are shown in Section 4.6.

4.2 The system architecture for the FHF primary confinement HVAC system is established by *Fuel Handling Facility Primary Confinement HVAC System Block Flow Diagram* (BSC 2004g), *Fuel Handling Facility Primary Confinement HVAC System Air Handling Unit Ventilation Flow Diagram* (BSC 2004h), *Fuel Handling Facility Primary Confinement HVAC System Remote HEPA Filters Ventilation Flow Diagram* (BSC 2004i), and *Fuel Handling Facility Primary Confinement HVAC System Exhaust HEPA Filter & Exhaust Fan Ventilation Flow Diagram* (BSC 2004j). These inputs contain the best design information available to proceed with a meaningful analysis of the system reliability. Because this calculation is a preliminary estimate of the reliability, to ensure feasibility of the design, these drawings are reasonable for use. Revisions and clarifications to these drawings are shown in Section 4.6.

4.3 Sources used for failure rate data are "Generic Component Failure Data Base" (Eide and Calley 1993, Tables 1 and 2), *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)), and *Nonelectronic Parts Reliability Data* (Denson 1991). These sources have compiled failure rate data for use in probabilistic risk assessment.

4.4 The threshold failure probability to ensure that a Category 1 initiating event, followed by a failure of the HVAC, is a Category 2 event sequence is established in *Categorization of Event Sequences for License Application* (BSC 2005, Sections 5.1.1.48 and 6.3.1.3).

4.5 The failure rates for a loss of electric power to the nuclear HVAC systems in the primary confinement areas of the DTFs and the FHF are established in *Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System* (BSC 2004a, Section 7.3).

4.6 For the inputs of Sections 4.1 and 4.2, the following changes are adopted in the Fault Tree Analysis (FTA), in accordance with (Demetria 2005):

- All air-operated isolation dampers shown as "NO/FC" (normally open/fail close) should be changed to "NO/FO" (normally open/fail open) and all air operated modulating dampers should be "FL" (fail last position). This ensures that the flow paths cannot be inadvertently closed by loss of the air supply to the dampers.

- Any exhaust fan running will result in automatic opening of inlet dampers to all operating HEPA filters. This change eliminates a potential one-to-one dependency between a given exhaust fan and a given HEPA filter plenum. (Applies to DTF)

- A dedicated programmable logic controller (PLC) located locally in the facility will perform all the control functions. Detailed design will further evaluate the control functions.

5. ASSUMPTIONS

5.1 Assumption: No credit is given for human operator interaction with the HVAC systems and thus no human failure is analyzed in the FTA.

Basis: The HVAC system is started and verified to be operating properly before any operations with nuclear fuel or nuclear waste are initiated (Assumption 5.4). Once this action is complete, which may require some operator interaction, the need for operator actions is no longer present. This part of the FTA is therefore modeled with undeveloped events, without operator interaction and without human failure, and will be further developed at a later time (when operator requirements are identified) to include human failures as warranted.

Used in: Section 6.3.3.

5.2 Assumption: Routine maintenance on redundant components will be performed with a staggered schedule.

Basis: This is a recommended practice 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.

5.3 Assumption: The release of airborne contamination inventory is instantaneous and no settling or plateout occurs.

Basis: In order to maximize the required HVAC flow rates for the 4-h mission time, the airborne contamination inventory after a postulated CSNF drop event is maximized by assuming that the release is instantaneous and that no settling or plateout occurs.

Used in: Section 6.3, Equation 4

5.4 Assumption: An operational requirement will ensure that (1) the HVAC system is working properly before normal operations begin, (2) that the HVAC system is monitored for proper operation during normal operations, and (3) that normal operations are suspended if the HVAC system becomes unavailable. Additionally no credit is taken for the standby HVAC equipment.

Basis: This operational requirement is from *Categorization of Event Sequences for License Application* (BSC 2005 , Section 5.1.1.48). Taking no credit for the standby HVAC equipment is conservative; neither the standby equipment nor the components required to sense the need for the standby equipment and start it are modeled in the analysis.

Used in: Throughout the report.

5.5 Assumption: Fiber optic and electrical cables are not considered as a potential failure to the operation of the HVAC system.

Basis: The fiber optic and electrical cables are highly reliable passive components and thus excluded from this evaluation.

Used in: Throughout the report.

5.6 Assumption: The operation and efficiency of the HEPA filters during the event sequence are unchanged from prior to the event.

Basis: Before the event sequence, the HVAC system is operating properly and accommodates the loading on the filters. The event sequence does not include a fire or other occurrence that would significantly increase the loading on the filters. Thus, the operation and efficiency of the HEPA filters during the event sequence are unchanged from prior to the event.

Used in: Throughout the report.

5.7 Assumption: The bird screen and intake grill are not considered as a potential failure to the operation of the HVAC system.

Basis: The bird screen and intake grill are highly reliable passive components and thus excluded from this evaluation.

Used in: Throughout the report.

5.8 Assumption: Only the equipment shown on the ventilation flow diagrams will be analyzed in this report. No attempt will be made to analyze control equipment not shown (relays, PLC, etc.).

Basis: The reliability of control equipment that is not shown cannot be estimated without detailed design. This analysis is preliminary; detailed design will produce the information needed for more detailed analysis and confirm that the equipment can be controlled in accordance with the design requirements used here.

Used in: Throughout the report.

5.9 Assumption: The control system and instruments, including solenoid valves, are powered from uninterruptible power supplies (UPSs) or batteries. The loss of power to these instruments and the control system is assumed to be included in the failure rates for these components or enveloped by the loss of power events considered explicitly for the fans.

Basis: Control systems and instruments are traditionally powered from UPSs. Upon loss of the normal AC power feed to a UPS, batteries provide the necessary power through the inverter in the UPS. DC solenoid valves are battery powered. Loss of power to the fans could also result in loss of the AC power feed to the UPS or battery charger, but the control system, instrument or solenoid valve is unaffected by that power loss (until the batteries are drained). Loss of AC power to the UPS or battery charger is alarmed to the operator, and movement of fuel would be terminated in accordance with Assumption 5.4.

Used: Throughout the report.

5.10 Assumption: The primary confinement and the HVAC system function such that leakage will be only into the primary confinement and all releases from the primary confinement will be filtered by the HEPA filter plenums prior to release through the exhaust stack.

Basis: These design conditions are considered effective for the first four hours after a Category 1 fuel drop event (BSC 2005; BSC 2004l). Detailed design must therefore ensure that the primary confinement and the HVAC system are designed so that leakage will be only into the primary confinement and all releases from the primary confinement will be filtered by the HEPA filter plenums prior to release through the exhaust stack.

Used in: Throughout the report.

5.11 Assumption: Dependent and common-cause failures among systems and components are treated by the techniques developed for probabilistic risk assessment of nuclear reactor systems, namely explicit modeling and parametric modeling (NRC 1983, Section 3.7.3). Explicit modeling uses gates, transfers, and basic events in the fault tree logic based on the physical “hard-wired” interdependence between HVAC mechanical components and their power sources, control elements, and human error (where applicable). Parametric modeling is used to introduce “pseudo” failure events into a FT model to account for the potential multiple failures of redundant, identical components due to non-specific generic causes. In particular, this analysis employs the Alpha Factor method of parametric CCF analysis. Values of the Alpha Factor parameters are shown in Section 6.3.4.

Basis: Methods are discussed in NUREG/CR-2300 (NRC 1983, Section 3.7.3) for modeling of dependent failures in fault tree analysis. One method identified is the “explicit” method where causes of failures of front-line system components are identified and built into the fault tree logic. Such dependencies may include loss of AC power to multiple components, failure to actuate multiple components due to the failure of a common control element, or failure of one or more components because of maintenance errors. Explicit modeling may also include earthquakes, fires, and floods, but such external-event causes are beyond the purpose of this HVAC reliability analysis. In general, if an explicit dependent cause can be identified and can be quantified for its effect on the probability of failure of one or more components of a front-line system, then explicit modeling is the preferable analytic approach.

It is common practice in PRA modeling of systems having redundant components to provide for uncertainty in the initial evaluation, and to allow for a certain probability for CCF to occur between like components without trying to identify the explicit causes. This approach ensures that an overly optimistic result is not obtained by assuming complete independence between redundant, identical components. Such parametric modeling implicitly accounts for errors such as design flaws, manufacturing defects, maintenance errors, and environmental and usage factors. Based on a compilation of many years of data, the NRC has established the Alpha Factor method as the means to evaluate the implicit CCFs and has developed a database to support it.

Used in: Sections 6.3.4 and 6.4.

6. ANALYSIS

6.1 OBJECTIVE

The objective of this report is to perform an FTA on the mechanical equipment that supports the function of the nuclear primary confinement HVAC systems in the DTFs and FHF to determine the reliability. This analysis also gives the overall reliability of the nuclear HVAC systems in the primary confinement areas of the DTFs and the FHF based on loss of electrical power and mechanical equipment failure.

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. FTA also helps to improve the understanding of the system in question, to identify components that may need further testing or redundancy, and to identify root causes of equipment failure. This analysis is performed using the methods in *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 the Top Event to be Analyzed

An undesirable event for the system in question is termed top event. The top event is logically broken down into all credible ways that it can occur. Because the lower level breakdown of the top event includes only those faults that contribute to the top event, it is important to identify the specific top event that corresponds to a particular system failure mode. The top event for this analysis is “Failure of HVAC system, in the DTF 1 primary confinement, to continue operation for 4 hours.”

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 to maintain the system in working order. For example, the nuclear HVAC system in the DTF primary confinement area is successful as long as two out of its three normally operating supply and exhaust fans continue to operate properly (Section 6.3). This means that less than two supply and two exhaust fans operating properly results in the top event.

6.2.2 Step Two: Understand the System

It is necessary to have a good understanding of the system being analyzed to identify the events that directly contribute to the top event. Research must be done to understand how the system works as a whole, the direct interface between its subsystems, and the functions performed by each component in all subsystems 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 the breakdown of a fault tree (FT) and can represent the failure of an individual component, a particular human action, a CCF event, or an undeveloped event.

In the study of the HVAC systems, it is important to understand the function of each subsystem (e.g., air handling system and exhaust system), to identify the specific path of ventilation from the outside air to the exhaust fans, and to know in detail the function and control of each component along that path to accomplish the proper HVAC operation.

6.2.3 Step Three: Make a Logic Model

The FT model is created by breaking down the top event into combinations of events that lead to it. This is done with the use of Boolean logic gates. Logic gates show the relationships of events that are needed for the occurrence of a higher event. The higher event is the output of the gate; the lower events are 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). (See Figures 1 and 2 for gate symbols.)

Boolean logic analysis consists of binary inputs and outputs to a gate. The inputs and outputs of logic gates are termed binary because they can take only one of two states, either TRUE or FALSE that an event exists. Although FTA uses several specialized logic gates the two basic types of logic gates are AND and OR. One specialized gate, used in this analysis, is the N/M-gate. The types of logic gates and other event symbols used in this analysis are defined in the following paragraphs:

The OR-gate is used to show that the output event occurs only if one or more of the input events occur (Vesely et al. 1981, p. IV-4). That is, the output state is TRUE if one or more of the input events is (are) TRUE. There may be any number of input events to an OR-gate.

For example, the OR-gate is used to represent a system or subsystem when every component in the system is essential for the successful operation of the system. To quantify the probability of the output event represented by an OR-gate, the probabilities of input events are added.

The AND-gate is used to show that the output event occurs only if all of the input events occur (Vesely et al. 1981, p. IV-6). That is, the output state is TRUE only if every one of the input events are TRUE. There may be any number of input events to an AND-gate.

For example, the AND-gate is used to represent a system or subsystem when the failure of all components in the system is required to cause failure of the system. The AND-gate is used, therefore, to represent failure of a system consisting of two or more redundant components in parallel where the successful operation of any one of the components is sufficient for successful execution of the function of the system. Similarly, the AND-gate is used to represent cases where failure of a primary signal or control element is backed up by an alternative signal or control element. To quantify the probability of the event represented by an AND-gate, the probabilities of input events are multiplied.

The N/M-gate is used to represent the case where a system is comprised of a number M identical components or subsystems, but where failure of a subset N of the components or subsystems is necessary and sufficient to cause failure of the overall system. A fault tree for an N/M logic can be built by hand by the fault tree analyst using a combination of AND and OR gates, but the logic model becomes complex for cases where n is greater than 3 or 4. However, the fault tree program SAPHIRE, used in this analysis, provides a shortcut where the analyst can simply select the N/M-gate from the program gate list. This simplifies the analysis as well as the graphical display of the fault tree.

A circle shape is used in an FT to represent basic events that have been developed. A diamond shape is used in an FT to represent events that are undeveloped. Undeveloped events are events that could be developed in further detail in FT modeling but are not because, (1) it is unnecessary to include such detail, or (2) there is not enough information available. Undeveloped events are included in the logic model for completeness of the FT and can be developed at a later time. Undeveloped events are treated as basic events in the FTA.

With the use of logic gates, fault tree logic is developed downward from the top event to determine the intermediate events that lead to the top event. The logic development process continues until the basic events are identified, usually at the component level. The final FT can be constructed and analyzed with the use of a computer program software such as SAPHIRE (BSC 2002).

6.2.4 Step Four: Assess the Probability of Basic Events

Once an FT model has been made, the basic events are quantified using reliability data resources and probability calculations. The process includes gathering and assembling component failure rate data from reliability databases for the basic events. Such databases include "Generic Component Failure Data Base" (Eide and Calley 1993, Tables 1 and 2), *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)), and *Nonelectronic Parts Reliability Data* (Denson 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 performed using 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:

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

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:

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

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

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

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. The design requirement in *Categorization of Events Sequences for License Application* (BSC 2005, Sections 5.1.1.48) identifies this time to be four hours.

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

6.2.5 Step Five: Perform Common-Cause Failure Analysis

A CCF is a failure that occurs simultaneously in two or more structures, systems, or components due to a single specific event or cause (Assumption 5.11).

Examples of CCFs include, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a man-induced event including ineffective maintenance, or some kind of system interaction or domino effect. Such domino effects occur when failure of one component leads to failure of one or more other components through some coupling mechanism such as a physical interaction like a missile or oil spray generated by the initial component failure. Another kind of domino effect occurs when the first component failure leads to a condition beyond the design capacity of one or more dependent components, such as an over-demand, over-voltage, or over-temperature.

The potential CCFs and their coupling mechanisms that can be specifically identified, evaluated, or prevented through design or operational controls are termed "explicit" CCFs because they can be explicitly modeled in FT logic. For example, two pressure controllers could fail to perform their redundant safety function due to a miscalibration error by a technician. The coupling mechanism could be an incorrect procedure or common maintenance personnel. Such CCFs can be modeled explicitly in a fault tree by including a basic event for miscalibration error (i.e., a human error) when sufficient information exists on the design, operations, and maintenance schedules. CCF defenses for this example include measures to validate and verify procedures and to ensure proper training of maintenance personnel. At present, there is insufficient design and operational information to evaluate explicit CCFs associated with the HVAC systems

Even after evaluation and prevention of explicit CCFs, however, experience with highly reliable systems has demonstrated that there remains a finite probability of CCFs of multiple, similar components. The data that has been evaluated for CCF rates, e.g., Marshall (1998 [DIRS 167710] cannot, with certainty, identify the specific causes of a given CCF in the historical records in most cases. However, the undefined cause of a recorded CCF could be due to one of the causes discussed for explicit CCFs. That is, the database may indicate that two pressure controllers failed concurrently in some plant but a specific cause cannot be determined. The cause could have been due to a miscalibration error by a technician or other maintenance error, but could have been some other cause like a common design or manufacturing defect that was not prevented by programmatic defenses. Therefore, to capture the probability of such CCFs when insufficient information is available to permit explicit CCF modeling, one or more CCF basic events are included in the FT model. This process is termed “implicit” CCF modeling. The quantification of the probabilities of the basic events that represent the implicit CCFs is obtained using “parametric” methods. The implicit CCF modeling is used in this analysis of the HVAC.

There are several parametric methods for quantification of the implicit CCF probability, such as the Beta Factor, the Multiple Greek Letter, and the Alpha Factor. Guidelines and parameters for application of the Alpha Factor method have been presented by the U.S. Nuclear Regulatory Commission (NRC) in NUREG/CR-5497 (Marshall 1998, and NUREG/CR-5485 (Mosleh 1998). These sources show that maintenance errors are one contributor to CCFs represented in the NRC’s database and that staggered maintenance leads to fewer CCFs than non-staggered maintenance. Therefore, Mosleh (1998 [DIRS 167711]) presents Alpha Factor parameters for the alternative cases of staggered and non-staggered maintenance. Section 6.3.4 provides a guideline for using the Alpha Factor method in CCF analyses assuming staggered maintenance on redundant components (Assumption 5.2).

The assessment of a CCF event (Section 6.2.2) is done by multiplying the total failure probability of a redundant component by a CCF factor (based on the Alpha Factor method) that considers how many components are in the redundant group, termed n, and how many are needed for success, termed k. It is important to note that although the Alpha Factor method for CCF analyses is based on a success configuration, it is meant to be applied to a failure structured FT.

The fundamental modeling of a CCF in an OR-gate is shown in Figure 1. Logic analysis shows that when redundant events are the inputs to an OR-gate, the success criterion for the CCF basic event is always n-of-n, where n is the number of redundant events in the system. The CCF basic event is then quantified by multiplying the total failure probability of the redundant basic event by the CCF factor for n-of-n (Section 6.3.4).

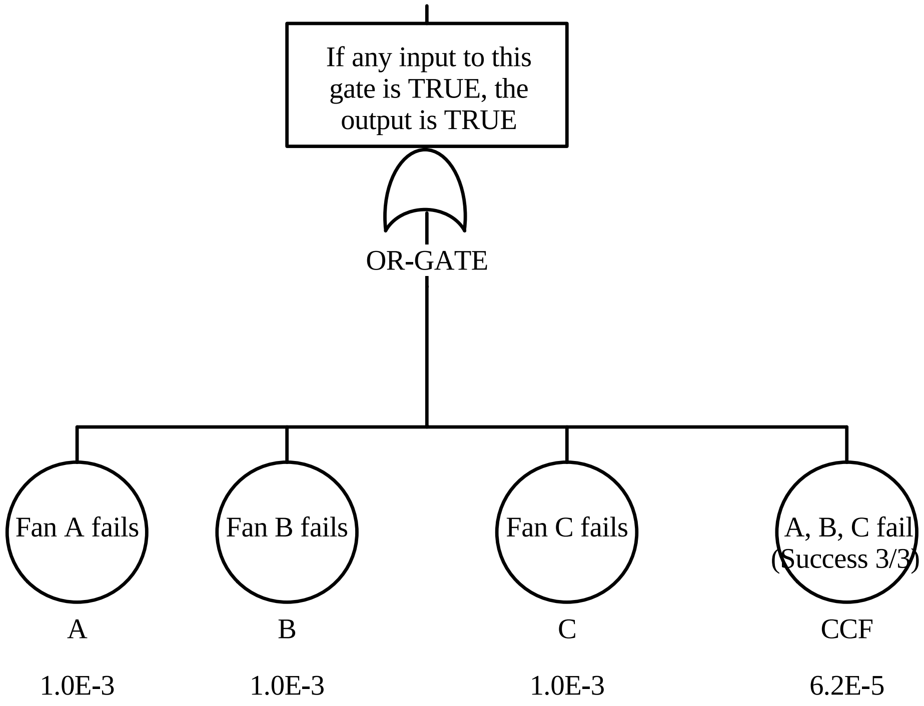

If any input to this gate is TRUE, the output is TRUE
OR-GATE
Fan A fails
Fan B fails
Fan C fails
A, B, C fail (Success 3/3)
A
B
C
CCF
1.0E-3
1.0E-3
1.0E-3
6.2E-5

Figure 1. Common-Cause Failure 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 to the FT because quantitatively, it does not contribute significantly to the output. In this case, the output without CCF is 3.0E-3 whereas with CCF, it is 3.1E-3. Note that the CCF failure probability of 6.2E-5 is equal to the total component failure probability of 1.0E-3 multiplied by the CCF factor of 0.062 for a three-out-of-three success ratio (Section 6.3.4).

The fundamental modeling of a CCF in an AND-gate is shown in Figure 2. Logic analysis shows that when redundant events are the inputs to an AND-gate, the success criterion 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 CCF factor for 1-of-n (Section 6.3.4).

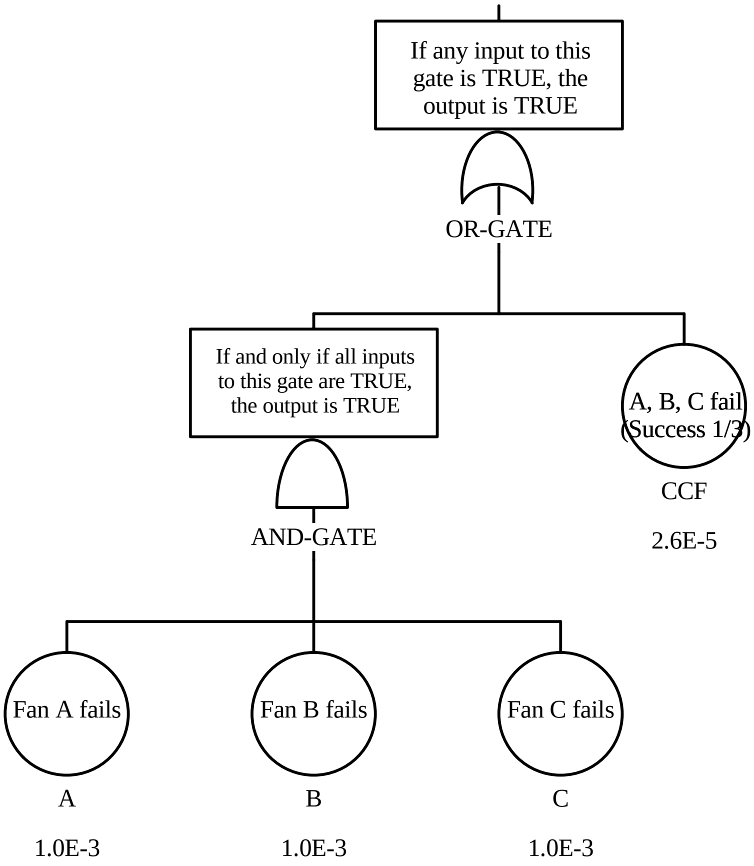

If any input to this gate is TRUE, the output is TRUE
OR-GATE
If and only if all inputs to this gate are TRUE, the output is TRUE
AND-GATE
A, B, C fail (Success 1/3)
CCF
2.6E-5
Fan A fails
A
1.0E-3
Fan B fails
B
1.0E-3
Fan C fails
C
1.0E-3

Figure 2. Common-Cause Failure 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. The CCF event is qualitatively and quantitatively important to the output of the FT. In this case, the output without CCF is 1.0E-9, whereas with CCF, it is 2.6E-5, which is the value of the CCF and dominates the total output. Note that the CCF failure probability of 2.6E-5 is equal to the total component failure probability of 1.0E-3 multiplied by the CCF factor of 0.026 for a one-out-of-three success ratio (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 an FT has been modeled and failure probabilities have been assigned to each basic event, then the FT is ready to be evaluated. With the aid of SAPHIRE, the appropriate Boolean algebra is performed and the result is output in a report that contains the minimal cut sets. A minimal cut set is the smallest combination of component failures that, if they all occur, will cause the top event to occur. If one of the failures in the minimal 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 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 events, depending on the complexity of the FT. The cut set 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 listed at the top of the cut set report because it takes fewer component failures to make the top event occur. The higher the number of events in a cut set, the more component failures it takes to make the top event occur.

A quantitative cut set report shows the same arrangement of minimal cut sets as does a qualitative cut set report, but the quantitative cut set report also 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 to the major contributors of the top event.

Analysis of a cut set report can improve the reliability of a system by identifying the main contributing events and by either adding redundancy to those components or using more reliable ones.

6.3 FAULT TREE ANALYSIS

The FTAs discussed in Sections 6.3 through 6.4 analyze the equipment of the nuclear HVAC systems in the primary confinement areas of the DTFs and the FHF.

There are two identical DTF buildings, DTF 1 and DTF 2. Although this analysis refers to DTF 1, the results are also applicable to DTF 2. Therefore, only two FTAs are performed in this analysis, one for DTF 1 and one for FHF. Also, because the architecture of DTF 1 and the FHF primary confinement HVAC systems are similar, the FTAs are similarly structured. The drawings used for this analysis are in Attachment A for DTF 1 and Attachment B for the FHF.

Top Event

The top event of both FTAs (Attachment C, Figure C-1 and Attachment D, Figure D-1) is described as: failure of HVAC system in the DTF 1/FHF primary confinement to continue operation for four hours (post-event). The top event is represented by an OR-gate called DTF_HVAC for the DTF 1 (Figure C-1) and an OR-gate called FHF_HVAC for the FHF (Figure D-1).

Success Criteria

Success criteria determine the type of logic gate for top events DTF_HVAC and FHF_HVAC. In this case, DTF 1 and the FHF primary confinement nuclear HVAC system is successful as long as:

1. All of its subsystems operate in unison to maintain required negative differential pressures, and

2. A minimum flow rate is achieved throughout the four hour mission time following the drop event, to significantly reduce the amount of airborne contamination remaining in the primary confinement.

A series of subsystems (the air handling, primary confinement zones, remote HEPA filter trains, and exhaust subsystems) in concert with one another are needed to maintain negative differential pressure. Top event DTF_HVAC is represented with an OR-gate with all subsystems as inputs because if one subsystem fails, then the function of the HVAC system fails.

A minimum airflow rate must also be achieved throughout the four hour mission time following a CSNF drop event, to significantly reduce the amount of airborne contamination remaining in the primary confinement zones. The airflow rate calculation is performed with the use of the concentration ratio formula (Equation 4) using the mission time (t), and the primary confinement area volumes of the DTFs and the FHF. This formula is used for predicting the airflow rate needed to reduce the original airborne radionuclide concentration after a CSNF drop event.

$$C(t) / C_0 = \exp [-Q t /V] \qquad \text{(Eq. 4)}$$

where:

$C(t)/C_0$ = radionuclide concentration ratio
Q = volumetric flow rate (ft^3/m)
t = mission time (m)
V = primary confinement area volume (ft^3)

Equation 4 is obtained using Equation 4.31 in NUREG/CR-6410 (SAIC 1998, p. 4-23) by taking the deposition velocity, (Vp), as zero (Assumption 5.3) and M_0/V as the initial concentration (C_0).

Table 1 shows airflow rates for different concentration ratios given a mission time (t) of four hours (Section 6.2.4) and a DTF 1 primary confinement area volume (V) of 1,598,691 ft^3. The primary confinement area volume for the DTF 1 was derived from BSC (2004k, Table 7.1-1) by multiplying the area by the height of each room in the primary confinement of the DTF 1 and adding them together.

Table 1. Flow Rate Calculation Table for Dry Transfer Facility 1

Concentration Ratio **$C(t) / C_0$**	**Volumetric Flow Rate, Q** **(cfm)**
0.50	4,617
0.10	15,338
0.010	30.676
0.0010	46,014

NOTE: The last row is the adopted concentration ratio with its corresponding flow rate.

cfm = cubic feet per minute

To provide significant concentration reduction, the last row of Table 1 gives the adopted concentration ratio and volumetric flow rate for this analysis of 0.0010 (or 0.1 percent) and 46,014 cfm, respectively. The *Preclosure Consequence Analyses for License Application* (BSC 2004l, Section 6.3) analyzes normal operation and a Category 1 drop event sequence (MACCS2 computer Run No. 1 for normal operation, and Run No. 16 for Category 1 drop event sequence), with reduction factor of 10^4 for HEPA filtration, and determines that the dose will not exceed the dose limits of 10 CFR Part 63 to an adjacent worker onsite and a member of the public at the site boundary. After four hours, with ventilation reducing the original concentration to below 0.1 percent of the original concentration, the remaining inventory, if released unfiltered, would not result in doses exceeding the 10 CFR Part 63 limits, and thus this concentration reduction is considered acceptable.

Each supply and exhaust fan in the primary confinement HVAC system of DTF 1 is rated at 35,000 cfm, which means that in order to meet the volumetric flow rate of 46,014 cfm, at least two supply fans and two exhaust fans are necessary.

Table 2 shows airflow rates for different concentration ratios given a mission time (t) of four hours (Section 6.2.4) and a FHF primary confinement volume (V) of 156,048 ft^3. The primary confinement area volume for the FHF was derived from BSC (2004m, Table 1) by multiplying the area by the height of each room in the primary confinement of the FHF and adding them together.

Table 2. Flow Rate Calculation Table for Fuel Handling Facility

Concentration Ratio **$C(t) / C_0$**	**Volumetric Flow Rate, Q** **(cfm)**
0.50	451
0.10	1,497
0.010	2,994
0.0010	4,491

NOTE: The last row is the adopted concentration ratio with its corresponding flow rate.

cfm = cubic feet per minute

To provide significant concentration reduction, the last row of Table 2 gives the adopted concentration ratio and volumetric flow rate for this analysis of 0.001 (or 0.1 percent) and 4,491 cfm, respectively. The *Preclosure Consequence Analyses for License Application* (BSC 2004l, Section 6.3) analyzes normal operation and a Category 1 drop event sequence (MACCS2 computer Run No. 1 for normal operation, and Run No. 16 for Category 1 drop event sequence), with reduction factor of 10^4 for HEPA filtration, and determines that the dose will not exceed the dose limits of 10 CFR Part 63 to an adjacent worker onsite and a member of the public at the site boundary. After four hours, with ventilation reducing the original concentration to below 0.1 percent of the original concentration, the remaining inventory, if released unfiltered, would not result in doses exceeding the 10 CFR Part 63 limits, and thus this concentration reduction is considered acceptable.

Each supply and exhaust fan in the primary confinement HVAC system of FHF is rated at 12,000 cfm, which means that in order to meet the volumetric flow rate of 4,491 cfm, only one supply fan and one exhaust fan are necessary.

6.3.1 Nuclear Primary Confinement HVAC System Description

Block diagrams of the primary confinement HVAC systems are provided in Attachment A, Figure A-1, for DTF 1, and Attachment B, Figure B-1 for the FHF. For practical purposes of this analysis each HVAC system is broken down into four subsystems that provide a flow of air throughout the facility from the outside air intake through the primary confinement zones and HEPA filters to the exhaust air stack. The four subsystems working in concert are: air-handling, primary confinement zones, remote HEPA filter trains, and exhaust air subsystems. Sections 6.3.1.1 through 6.3.1.4 describe the function of each subsystem.

Note that the design is conceptual in nature and the drawings in Attachments A and B contain enough information to proceed with a meaningful analysis of the system reliability (Assumption 5.8). Slight modifications to the drawings appear in Section 4.6.

6.3.1.1 Air-Handling Subsystem

As shown in Figures A-2 and B-2, each air-handling subsystem consists of a louvered air intake, which directs outside air into the HVAC system, a supply air distribution network, and air-handling units (AHUs), which draw air from the intake plenum, condition the air, and direct it to the primary confinement zones and to the remote HEPA filter room. The AHU supply fans are equipped with adjustable speed drives and speed controllers to provide adjustment in the system airflow to maintain the required negative differential pressures in the confinement zones. The supply air distribution network includes ductwork, and isolation dampers. Isolation dampers are two position (open/closed) parallel blade dampers that are actuated to either isolate or include a particular AHU to the flow path.

The DTF 1 air-handling subsystem consists of four AHUs, three typically operating and one on standby, and delivers 99,000 cfm (Attachment A, Figure A-2) to the primary confinement zones. The FHF air-handling subsystem consists of two AHUs, of which one is typically in operation and one is on standby, and delivers 10,500 cfm (Attachment B, Figure B-2) to the primary confinement zone.

6.3.1.2 Primary Confinement Zones

The primary confinement zones are those areas where radioactive materials are processed and that are normally contaminated with airborne radioactive particulates. The primary confinement zones (DTF, two zones, Attachment A, Figure A-3, and FHF, one zone, Attachment B, Figure B-3) receive air from the air-handling subsystem through air ducts. Differential pressure-transmitters, situated in the primary confinement zones, transmit information to a differential pressure controller that controls the speed of the AHU supply fans via a speed controller. From the primary confinement zones, the air is directed by ductwork to the remote HEPA filter trains. The DTF 1 has two primary confinement zones, while the FHF has only one.

6.3.1.3 Remote High Efficiency Particulate Air Filter Trains Subsystem

The remote HEPA filter trains subsystem, located in the remote HEPA filter room, includes HEPA filters to remove particulate radioactive contaminants from the primary confinement zones exhaust air, as shown in Attachment A, Figure A-4 and Attachment B, Figure B-3. After the air has been filtered by the remote HEPA filter trains subsystem, it is directed to the exhaust air subsystem. These remote HEPA filters act as prefilters to the exhaust subsystem HEPA filter plenums.

A control damper in the bypass duct coming from the air-handling subsystem to the remote HEPA filter room modulates the air coming into the remote HEPA filter room to maintain negative differential pressure. A differential pressure transmitter and a differential pressure controller controls the modulation of the bypass damper.

The remote HEPA filter trains subsystem for DTF 1, and likewise for the FHF, consists of five HEPA filter trains, four typically operating and one on standby. After the air has been prefiltered by the remote HEPA filter trains subsystem, it is directed to the exhaust air subsystem.

6.3.1.4 Exhaust Air Subsystem

The exhaust air subsystem is shown in Attachment A, Figure A-5 and Attachment B, Figure B-4. The exhaust air subsystem consists of HEPA filter plenums, exhaust fans, and an exhaust collection network. The exhaust collection network directs the air into the HEPA filter plenums for filtration and then to the exhaust fans. The exhaust fans direct the filtered air into the exhaust air stack, where it is monitored for radioactivity and discharged to the outside.

Each HEPA filter plenum includes two stages of HEPA filters. The exhaust fans are equipped with adjustable speed drives used to adjust system airflow to maintain the required differential pressure. The adjustable speed drives are modulated by a speed controller fed from a differential pressure transmitter. The exhaust collection network includes ductwork, and dampers. Isolation dampers are provided for the HEPA filter plenum units and exhaust fans; these are two-position (open/closed) parallel blade dampers that are actuated to either isolate or include a particular HEPA filter plenum or fan to the flow path.

DTF 1 has five HEPA filter plenum units, four typically operating and one on standby, and four exhaust fans, three typically operating and one on standby. The FHF has one HEPA filter plenum unit, of which half is typically operating and half is on standby, and two exhaust fans, of which one is typically operating and one is on standby.

6.3.2 Fault Tree Logic Model

After the top events DTF_HVAC and FHF_HVAC, and their success criteria have been defined for DTF 1 and the FHF (Section 6.3), the FT logic models can be made.

Maintaining negative differential pressure is the first part of the success criteria described in Section 6.3. The HVAC systems in the primary confinement areas of DTF 1 and the FHF have four subsystems in series (Section 6.3.1) that must work together to accomplish a negative differential pressure. Failure of any subsystem results in the occurrence of the top event by not meeting the first part of the success criteria. The second part of the success criteria, to maintain a minimum flow rate of 46,014 cfm (Table 1) for DTF 1 and 4,491 cfm (Table 2) for the FHF, must be met by the individual subsystems. For this analysis, the exhaust air subsystem was broken down into the HEPA filter plenum subsystem and the exhaust fan subsystem. The top events and the first level of breakdown for the DTF 1 FT model and the FHF FT model are shown in Attachment C, Figure C-1, and Attachment D, Figure D-1, respectively. In order for each top event represented by OR-gates DTF_HVAC and FHF_HVAC to occur, any one of the following five inputs must occur, representing the failure of five subsystems:

- TRANSFER-gate AIR_HANDL: Failure of Air Handling Subsystem to maintain HVAC function
- TRANSFER-gate PRIMARY_ZONES: Failure of Primary Confinement Zones to maintain HVAC function
- TRANSFER-gate HEPA_TRAINS: Failure of HEPA Trains Subsystem to maintain HVAC function
- TRANSFER-gate FILTR_PLENM: Failure of HEPA Filter Plenum Subsystem to maintain HVAC function
- TRANSFER-gate EXHAUST_SYSTM: Failure of Exhaust Fan Subsystem to maintain HVAC function

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

The FT models of DTF 1 and the FHF are provided in Attachments C and D, respectively, and are explained in Sections 6.3.2.1 through 6.3.2.5. Different types of bullets are used throughout this analysis to emphasize the hierarchy of events in the FT. CCF events are explained in Section 6.3.4.

All normally operating units described in Sections 6.3.2.1 through 6.3.2.5 are credited for being in service up to the time of failure and evaluation of standby units is excluded from this analysis (Assumption 5.4).

6.3.2.1 Air-Handling Subsystem

DTF 1

Attachment C, Figure C-2, shows subtree AIR_HANDL, which is a subtop event defined as "Failure of Air Handling Subsystem to maintain HVAC function." This is an input that if TRUE, can make the top event occur (Section 6.3.2) and it is the expansion of TRANSFER-gate AIR_HANDL in Attachment C, Figure C-1.

The air-handling subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the air-handling subsystem if less than two supply fans are operating successfully, which will not meet the airflow requirement (i.e., 33,000 cfm is less than 46,014 cfm), or if the pressure modulation system fails to maintain negative differential pressure in the primary confinement zones. This is represented by the following events, which are inputs to OR-gate AIR_HANDL:

- ➢ Basic Event AIRHANLD_HDUCT1: Failure of header air duct 1. Duct 1 represents the upstream duct.Basic Event AIRHANDL_HDUCT2: Failure of header air duct 2. Duct 2 represents the downstream duct.
- ➢ OR-gate AIRHANDL_NORML: Failure of 2 normal operating air handling units
- ➢ OR-gate AIRHANDL_PRESS: Failure of pressure modulation system to maintain negative differential pressure.

Based on the description of the operation of the air-handling subsystem (Section 6.3.1), it is known that three AHUs are normally operating and one is on standby. However, for conservatism, the standby unit is not considered in this evaluation at this time. Subtree AIRHANDL_NORML models the loss of HVAC function due to the failure of two normally operating AHUs. This is represented by the following three events, which are inputs to OR-gate AIRHANDL_NORML:

- ⇒ OR-gate AIRHANDL_1: Normal operating air handling unit 1 fails.
- ⇒ OR-gate AIRHANDL_2: Normal operating air handling unit 2 fails.
- ⇒ OR-gate AIRHANDL_3: Normal operating air handling unit 3 fails.

AIRHANDL_NORML occurs if two of its three inputs are TRUE. Each input is an OR-gate termed AIRHANDL_X, where X represents unit numbers 1 through 3. All normally operating AHUs are identical and thus fail in the same manner. Each AHU can fail due to mechanical equipment failure or the loss of power to the motored fans.

The system description and a portion of the reliability evaluation of the electrical power distribution to the primary confinement HVAC systems in DTF 1 and the FHF are presented in *Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System* (BSC 2004a, Section 7.3). It is necessary that at least two supply and two exhaust fans be successfully operating in the DTF 1 (Section 6.3). The electrical power distribution system distributes power symmetrically to DTF 1. This means that Side A of the power distribution grid as described in BSC (2004a) provides power to the first two supply and the first two exhaust fans for DTF 1. Also, Side B of the power distribution grid as described in BSC (2004a) provides power to the remaining two supply and the remaining two exhaust fans for the DTF 1. Side A of the power distribution grid cannot supply power to the fans on Side B and vice versa.

The following two events are inputs to AIRHANDL_1, and represent the failure of two essential systems for its successful operation:

- → OR-gate AIRHANDL_1_MECH: Failure of mechanical equipment in air handling unit 1.
- → Undeveloped event LOSP_SIDEA: Loss of power to motored fan in air handling unit 1.

The following two events are inputs to AIRHANDL_2, and represent the failure of two essential systems for its successful operation:

- → OR-gate AIRHANDL_2_MECH: Failure of mechanical equipment in air handling unit 2.
- → Undeveloped event LOSP_SIDEA: Loss of power to motored fan in air handling unit 2.

The following two events are inputs to AIRHANDL_3, and represent the failure of two essential systems for its successful operation:

- → OR-gate AIRHANDL_3_MECH: Failure of mechanical equipment in air handling unit 3.
- → Undeveloped event LOSP_SIDEB: Loss of power to motored fan in air handling unit 3.

Each OR-gate input termed AIRHANDL_X_MECH, where X represents unit numbers 1 through 3 occurs in the same manner. The following 14 events are inputs to AIRHANDL_X_MECH, and represent the failure of 14 key components essential for the successful operation of one AHU:

- ✧ Basic event AIRHANDL_X_SPEED: Fan speed controller failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_FAN: Motored fan failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_HINTLOCK: Hardwired interlock failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_DAMPR1: Parallel blade damper 1 failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_DAMPR2: Parallel blade damper 2 failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_3WYVAL1: Solenoid valve 1 failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_3WYVAL2: Solenoid valve 2 failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_PLUG: Air handling unit X plugs.
- ✧ Basic event AIRHANDL_X_DUCT: Air duct failure – air handling unit X. Note that only one duct is modeled for each AHU although there are two duct pieces, one before and one after the unit. The modeling of one duct complies with the idempotent law (X+X=X) of Boolean algebra, which reduces two or more identical events to one when joined by an OR-gate.
- ✧ Undeveloped event AIRHANDL_X_SWITCH: Local Start/Stop switch failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_SMOKE: Smoke detector failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_INTLOCK: Logic interlock failure – air handling unit X.
- ✧ Basic event AIRHANDL_X_TRANS: Speed transmitter failure – air handling unit X.

- ✧ Basic event AIRHANDL_X_SENSR: Speed sensor failure – air handling unit X.

OR-gate AIRHANDL_PRESS is the second input to subtree AIR_HANDL describing the failure of the pressure modulation system to maintain negative differential pressure in the primary confinement zones. The following four events, which are inputs to OR-gate AIRHANDL_PRESS, represent the failure of four key components essential for the successful operation of the pressure modulation system:

- ⇒ Basic event AIRHANDL_PRESS_CONT: Differential pressure controller (PDIC102) fails.

- ⇒ Basic event AIRHANDL_PRESS_COMP: Differential pressure computing device (PDY112) fails.

- ⇒ Basic event AIRHANDL_PRESS_Z1: Differential pressure transmitter (PDIT112) fails – zone 1.

- ⇒ Basic event AIRHANDL_PRESS_Z2: Differential pressure transmitter (PDIT113) fails – zone 2.

CCF will be explained in Section 6.3.4.1

FHF

The subtree (Attachment D, Figure D-2) that describes the failure of the air-handling subsystem in the FHF (Attachment B, Figure B-2) is similar to the one just described for DTF 1 with one difference being that there is only one normally operating AHU and it is needed to meet the airflow requirement according to part two of the success criteria for the FHF (Table 2).

6.3.2.2 Primary Confinement Zones

DTF 1

Attachment C, Figure C-3, shows subtree PRIMARY_ZONES, which is a subtop event defined as “Failure of Primary Confinement Zones to maintain HVAC function.” This is an input that if TRUE, can make the top event occur (Section 6.3.2) and it is the expansion of TRANSFER-gate PRIMARY_ZONES in Attachment C, Figure C-1.

The primary confinement zones must meet part one of the success criteria: maintain negative differential pressure (Section 6.3). Thus, the loss of HVAC function can occur in the primary confinement zones if the ducts and dampers fail to maintain negative differential pressure. This is represented by the following events, which are inputs to OR-gate PRIMARY_ZONES:

- ➢ OR-gate PRIMARY_ZONE1: Failure of Primary Confinement Zone 1.

- ➢ Basic event PRIM_ZONES_99KDUCT: Air duct failure – Primary Confinement Zones 99,000 cfm line.

- ➢ OR-gate PRIMARY_ZONE2: Failure of Primary Confinement Zone 2.

Primary confinement zones 1 and 2 can fail to maintain negative pressure if there is a failure in the duct or if the opposed blade damper fails. This is represented by the following two basic events, which are inputs to OR-gates PRIMARY_ZONE1 and PRIMARY_ZONE2:

- ⇒ Basic event ZONEX_DUCT: Air duct failure - Primary Confinement Zone X. (X represents zone numbers 1 and 2) Note that one duct is modeled for each primary confinement zone, although there are two duct pieces, one before and one after the primary confinement zone. The modeling of one duct complies with the idempotent law (X+X=X) of Boolean algebra, which reduces two or more identical events to one when joined by an OR-gate.

- ⇒ Basic event ZONEX_OBDAMPR: Opposed blade damper failure – Primary Confinement Zone X (X represents zone numbers 1 and 2).

FHF

The subtree (Attachment D, Figure D-3) that describes the failure of the primary confinement zones in the FHF (Attachment B, Figure B-3) is similar to the one just described for DTF 1 with one difference being that there is only one primary confinement zone with two parallel blade dampers.

6.3.2.3 Remote High Efficiency Particulate Air Trains Subsystem

DTF 1

Attachment C, Figure C-4, shows subtree HEPA_TRAINS, which is a subtop event defined as "Failure of Remote HEPA Trains Subsystem to maintain HVAC function." This is an input that if TRUE, can make the top event occur (Section 6.3.2) and it is the expansion of TRANSFER-gate HEPA_TRAINS in Attachment C, Figure C-1.

The remote HEPA trains subsystem must meet part one of the success criteria: maintain negative differential pressure. Thus, the loss of HVAC function can occur in the remote HEPA trains subsystem if less than four HEPA trains successfully maintain a flow path, or if the pressure modulation system fails to maintain negative differential pressure. This is represented by the following events, which are inputs to OR-gate HEPA_TRAINS:

- ➢ OR-gate HEPTRAIN_PRESS: Failure of pressure modulation system to maintain differential pressure.

- ➢ OR-gate HEPTRAIN_93KCFM: Failure of 93,000 cfm air supply – HEPA trains.

- ➢ Basic Event HEP_105K_DUCT: Air duct failure – HEPA trains 105k line.

- ➢ OR-gate HEPTRAIN_NORML: Failure of 1 normal operating HEPA filter train.

HEPTRAIN_PRESS is an input to subtree HEPA_TRAINS that describes the failure of the pressure modulation system to maintain negative differential pressure. This can occur if either the 10,000 cfm air supply fails or the 12,000 cfm air return fails. This is represented by the following events, which are inputs to OR-gate HEPTRAIN_PRESS:

- ⇒ OR-gate HEPTRAIN_10KCFM: Failure of 10,000 cfm air supply – HEPA trains.
- ⇒ OR-gate HEPTRAIN_12KCFM: Failure of 12,000 cfm air backup – HEPA trains.

HEPTRAIN_10KCFM represents the failure of the 10,000 cfm air supply to the HEPA filter room, which can occur if any of six key components fail. The following five events are inputs to OR-gate HEPTRAIN_10KCFM:

- → Basic event HEPTRAIN_10K_SOBDMPR: Spring actuated opposed blade damper (115) failure – HEPA trains 10k line.
- → Basic event HEPTRAIN_10K_DUCT: Air duct failure – HEPA trains 10k line.
- → Basic event HEPTRAIN_10K_PTRANS: Differential pressure transmitter (PDIT115) failure – HEPA trains 10k line.
- → Basic event HEPTRAIN_10_REL: Differential pressure relay (PDY115) failure – HEPA trains 10k line.
- → Basic event HEPTRAIN_10K_PCONT: Differential pressure controller (PDIC115) failure – HEPA trains 10k line.

HEPTRAIN_12KCFM represents the failure of the 12,000 cfm air return to the HEPA trains, which can occur if any of two key components fail. The following two events are inputs to OR-gate HEPTRAIN_12KCFM:

- → Basic event HEPTRN_12K_DUCT: Air duct failure – HEPA trains 12k line.
- → Basic event HEPTRN_12K_OBDMPR: Opposed blade damper failure – HEPA trains 12k line.

HEPTRAIN_93KCFM is another input to subtree HEPA_TRAINS that describes the failure of the 93,000 cfm air supply because of the air duct failure or the modulating opposed blade damper failure. This is represented by the following events, which are inputs to OR-gate HEPTRAIN_93KCFM:

- ⇒ Basic event HEP_93K_DUCT: Air duct failure – HEPA trains 93k line.
- ⇒ Basic event HEP_93K_OBDAMPR: Opposed blade damper failure – HEPA trains 93k line.

HEPTRAIN_NORML is one more input to subtree HEPA_TRAINS that describes the failure of the normally operating HEPA trains to maintain a flow path for the success of the negative differential pressure. This occurs when less than four trains are successfully operating, which occurs when one of the normal operating HEPA trains fails. This is represented by the following events, which are inputs to OR-gate HEPTRAIN_NORML:

⇒ OR-gate HEPTRAIN_1: Normal operating HEPA filter train 1 fails.

⇒ OR-gate HEPTRAIN_2: Normal operating HEPA filter train 2 fails.

⇒ OR-gate HEPTRAIN_3: Normal operating HEPA filter train 3 fails.

⇒ OR-gate HEPTRAIN_4: Normal operating HEPA filter train 4 fails.

HEPTRAIN_NORML occurs if any of its four inputs is TRUE. Each input is an OR-gate termed HEPTRAIN_X, where X represents train numbers 1 through 4. All normally operating HEPA trains are identical and thus fail in the same manner. The following four events are inputs to HEPTRAIN_X and represent the failure of four key components essential for the successful operation of one normal operating HEPA train:

→ Basic event TRAIN_X_HEPA: HEPA filter clogs – HEPA filter train X.

→ Undeveloped event TRAIN_X_VDAMP1: Slide gate damper 1 fails – HEPA filter train X.

→ Undeveloped event TRAIN_X_VDAMP2: Slide gate damper 2 fails – HEPA filter train X.

→ Basic event TRAIN_X_DUCT: Air duct failure – HEPA filter train X.

Note that only one duct is modeled for each HEPA filter train although there are two duct pieces, one before and one after the unit. The modeling of one duct complies with the idempotent law (X+X=X) of Boolean algebra, which reduces two or more identical events to one when joined by an OR-gate.

CCF will be explained in Section 6.3.4.3.

FHF

The subtree (Attachment D, Figure D-4) that describes the failure of the remote HEPA trains subsystem in the FHF (Attachment B, Figure B-3) is similar to the one just described for DTF 1.

6.3.2.4 High Efficiency Particulate Air Filter Plenum Subsystem

DTF 1

Attachment C, Figure C-5, shows subtree FILTR_PLENM, which is a subtop event defined as "Failure of HEPA Filter Plenum Subsystem to maintain HVAC function." This is an input that if TRUE, can make the top event occur (Section 6.3.2) and it is the expansion of TRANSFER-gate FILTR_PLENM in Attachment C, Figure C-1.

The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate of 70,000 cfm to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, rated at 27,000 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. This is represented by the following events, which are inputs to OR-gate FILTR_PLENM:

- ➢ Basic event FILTR_HDUCT1: Failure of header duct 1.
- ➢ Basic event FILTR_HDUCT2: Failure of header duct 2.
- ➢ OR-gate NORML_FILTR: Failure of 2 normal operating HEPA filter plenum units.

Based on the description of the operation of the exhaust air subsystem (Section 6.3.1), it is known that four HEPA filter plenum units are normally operating and one is on standby. However, the standby unit is not considered in this evaluation. Subtree NORML_FILTR models the loss of HVAC function due to the failure of two normally operating HEPA filter plenum units. This means that with three successful normal operating HEPA filter plenum units, the HEPA filter plenum subsystem will meet the 70,000 cfm air-flow requirement. This is represented by the following events, which are inputs to OR-gate NORML_FILTR:

- ⇒ OR-gate FILTR_1: Normal operating filter plenum unit 1 fails.
- ⇒ OR-gate FILTR_2: Normal operating filter plenum unit 2 fails.
- ⇒ OR-gate FILTR_3: Normal operating filter plenum unit 3 fails.
- ⇒ OR-gate FILTR_4: Normal operating filter plenum unit 4 fails.

NORML_FILTR has four inputs, each representing the failure of a normally operating HEPA filter plenum unit. NORML_FILTR occurs if two of its four inputs are TRUE. Each input is an OR-gate termed FILTR_X, where X represents unit numbers 1 through 4. All normally operating HEPA filter plenum units are identical and thus fail in the same manner. The following nine events are inputs to FILTR_X and represent the failure of nine key components essential for the successful operation of one normal operating HEPA filter plenum unit:

- → Basic event FILTR_X_DUCT: Air duct failure – filter unit X. Note that only one duct is modeled for each filter unit although there are several duct pieces in the unit. The modeling of one duct complies with the idempotent law (X+X=X) of Boolean algebra, which reduces two or more identical events to one when joined by an OR-gate.
- → Basic event FILTR_X_HEPA: HEPA filter 1 clogs – filter unit X.
- → Basic event FILTR_X_HEPA2: HEPA filter 2 clogs – filter unit X.
- → Basic event FILTR_X_3WYVAL: Solenoid valve failure – filter unit X.

- → Basic event FILTR_X_DAMPR1: Parallel blade damper 1 failure – filter unit X.
- → Basic event FILTR_X_DAMPR2: Parallel blade damper 2 failure – filter unit X.
- → Basic event FILTR_X_OBDAMP1: Opposed blade damper 1 failure – filter unit X.
- → Basic event FILTR_X_OBDAMP2: Opposed blade damper 2 failure – filter unit X.
- → Basic event FILTR_X_OBDAMP3: Opposed blade damper 3 failure – filter unit X.

CCF will be explained in Section 6.3.4.4.

FHF

The subtree (Attachment D, Figure D-5) that describes the failure of the HEPA filter plenum subsystem in the FHF (Attachment B, Figure B-4) is similar to the one just described for DTF 1 with one difference being that there is only one normally operating HEPA filter plenum unit and it is needed to meet the air-flow requirement according to part two of the success criteria for the FHF (Table 2).

6.3.2.5 Exhaust Fan Subsystem

DTF 1

Attachment C, Figure C-6, shows subtree EXHAUST_SYSTM, which is a subtop event defined as “Failure of Exhaust Fan Subsystem to maintain HVAC function.” This is an input that if TRUE, can make the top event occur (Section 6.3.2) and it is the expansion of TRANSFER-gate EXHAUST_SYSTM in Attachment C, Figure C-1.

The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two exhaust fans are operating successfully, which will not meet the airflow requirement, or if the pressure modulation system fails to maintain negative differential pressure. This is represented by the following events, which are inputs to OR-gate EXHAUST_SYSTM:

- ➢ Basic event EX_HDUCT: Failure of outlet header duct.
- ➢ OR-gate EX_NORML: Failure of 2 normal operating exhaust fan units.
- ➢ OR-gate EX_PRESS_MODU: Failure of pressure modulation system to maintain negative differential pressure.

Based on the description of the operation of the exhaust air subsystem (Section 6.3.1), it is known that three exhaust fans are normally operating and one is on standby. However, the standby unit is not considered in this evaluation. Subtree EX_NORML models the loss of HVAC function due to the failure of two normally operating exhaust fan units. This is represented by the following three events, which are inputs to OR-gate EX_NORML:

⇒ OR-gate EXHAUST_1: Normal operating exhaust fan unit 1 fails.

⇒ OR-gate EXHAUST_2: Normal operating exhaust fan unit 2 fails.

⇒ OR-gate EXHAUST_3: Normal operating exhaust fans unit 3 fails.

EX_NORML occurs if two of its three inputs are TRUE. Each input is an OR-gate termed EXHAUST_X, where X represents unit numbers 1 through 3. All normally operating exhaust fan units are identical and thus fail in the same manner. Each exhaust fan unit can fail due to mechanical equipment failure or the loss of power to the motored fan.

The system description and a portion of the reliability evaluation of the electrical power distribution to the primary confinement HVAC systems in the DTF 1 and the FHF is presented in *Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System* (BSC 2004a, Section 7.3). It is necessary that at least two supply and two exhaust fans be successfully operating in DTF 1 (Section 6.3). The electrical power distribution system distributes power symmetrically to DTF 1. This means that Side A of the power distribution grid as described in BSC (2004a) provides power to the first two supply and the first two exhaust fans for DTF 1. Also, Side B of the power distribution grid as described in (BSC 2004a) provides power to the remaining two supply and the remaining two exhaust fans for DTF 1.

The following two events are inputs to EXHAUST_1 and represent the failure of two essential systems for its successful operation:

→ OR-gate EXHAUST_1_MECH: Failure of mechanical equipment in exhaust fan unit 1.

→ Undeveloped event LOSP_SIDEA: Loss of power to motored fan in exhaust fan unit 1.

The following two events are inputs to EXHAUST_2 and represent the failure of two essential systems for its successful operation:

→ OR-gate EXHAUST_2_MECH: Failure of mechanical equipment in exhaust fan unit 2.

→ Undeveloped event LOSP_SIDEA: Loss of power to motored fan in exhaust fan unit 2.

The following two events are inputs to EXHAUST_3 and represent the failure of two essential systems for its successful operation:

→ OR-gate EXHAUST_3_MECH: Failure of mechanical equipment in exhaust fan unit 3.

→ Undeveloped event LOSP_SIDEB: Loss of power to motored fan in exhaust fan unit 3.

Each OR-gate input termed EXHAUST_X_MECH, where X represents unit numbers 1 through 3, occurs in the same manner. The following eleven events are inputs to EXHAUST_X_MECH, and represent the failure of eleven key components essential for the successful operation of one exhaust fan unit:

- ✧ Basic event EXHAUST_X_HINTLOCK: Hardwired interlock failure - exhaust fan unit X.
- ✧ Basic event EXHAUST_X_SPEED: Fan speed controller failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_FAN: Motored fan failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_3WYVAL: Solenoid valve failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_OBDAMPR: Opposed blade damper failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_DAMPR: Parallel blade damper failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_DUCT: Air duct failure – exhaust fan unit X. Note that only one duct is modeled for each exhaust fan unit although there are two duct pieces, one before and one after the unit. The modeling of one duct complies with the idempotent law (X+X=X) of Boolean algebra, which reduces two or more identical events to one when joined by an OR-gate.
- ✧ Basic event EXHAUST_X_INTLOCK: Logic interlock failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_SWITCH: Local Start/Stop switch failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_SENSR: Speed sensor failure – exhaust fan unit X.
- ✧ Basic event EXHAUST_X_TRANS: Speed transmitter failure – exhaust fan unit X.

OR-gate EX_PRESS_MODU is the second input to subtree EXHAUST_SYSTM, describing the failure of the pressure modulation system to maintain negative differential pressure. The following two events, which are inputs to OR-gate EX_PRESS_MODU, represent the failure of two key components essential for the successful operation of the pressure modulation system:

- ⇒ Basic event EX_PRESS_TRANS: Differential pressure transmitter (PDIT101) fails.
- ⇒ Basic event EX_PRESS_CONT: Differential pressure transmitter controller (PDIC101) fails.

CCF will be explained in Section 6.3.4.5.

FHF

The subtree (Attachment D, Figure D-6) that describes the failure of the exhaust fan subsystem in the FHF (Attachment B, Figure B-4) is similar to the one just described for DTF 1, with one difference being that there is only one normally operating exhaust fan unit and it is needed to meet the airflow requirement according to part two of the success criteria for the FHF (Section 6.3).

6.3.3 Basic Events Quantification

Once the FT logic model is completed (Section 6.3.2.1 through 6.3.2.5), probabilities of the basic events are assessed (Section 6.2.4). Component failure rate data for this FTA were gathered from three main component reliability information sources: "Generic Component Failure Data Base" (Eide and Calley 1993, Tables 1 and 2), *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations* (IEEE Std 500-1984 (Reaffirmed 1991)), and *Nonelectronic Parts Reliability Data* (Denson 1991). These sources have compiled failure rate data for use in probabilistic risk assessment for commercial nuclear power plants (Eide and Calley 1993, Tables 1 and 2; IEEE Std 500-1984 (Reaffirmed 1991)), or for reliability analyses for U.S. military equipment (Denson 1991). IEEE Std 500-1984 (Reaffirmed1991) is the base document from which most of the failure data are selected. Eide and Calley (1993, Tables 1 and 2) and Denson (1991) are used to select failure rates for most of the nonelectrical components.

IEEE Std 500-1984 (Reaffirmed 1991) compiled failure rate data from nuclear facilities, fossil-fired generating stations, chemical industries, transmission grids and industrial plants. Denson (1991) compiled failure rate data from published reports and papers, government sponsored studies, military systems and commercial systems. Data in Eide and Calley (1993, Tables 1 and 2) are mostly based on nuclear power plant standards. It should be stressed that none of these data bases distinguish between failure rates for safety-related and non safety-related components.

Collected data represent the failure rate of generic components in failure per million hours (λ) or per demand (q). The failure rates collected represent point estimate values, which are generally mean values. Eide and Calley (1993, Tables 1 and 2) shows two modes per component, failure to start and failure to continue operation. 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. Denson (1991) provides a name or category of component, but no description of the failure modes represented by a given component data entry. Also, many failure rates are presented for each component to designate the military application from which the data were derived, such as "ground mobile" or "ground fixed."

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 probability form. All generic components used for basic events are compiled in Table 3.

The first column in Table 3 contains the generic component name as listed in the database used. The second column describes the failure mode(s) used in the FT for each component. The failure rates for each component failure mode and their units are found in columns three and four, respectively. The Data Source column identifies the source where the data were taken for each component. The column entitled Basis for Probability gives the basis for obtaining the failure probability for each component. The failure probability is derived in the next column to be input into SAPHIRE. Lastly, the Comment column 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, which are explained in Section 6.3.4.1 through 6.3.4.5. Note that the failure rate for the air-handling unit filter was gathered from CRWMS (1999, p. IV-2) and the failure rate for loss of electric power from BSC (2004a, Section 7.3).

Subsystems such as air-handling, remote HEPA filter trains, HEPA filter plenum, and exhaust fans have normal operating units as well as standby units. Active components (i.e. dampers, solenoid valves, fans, etc.) found in normal operating units must have “per hour” failure rates describing the failure of the component to continue operation. There may be several failure modes that will prevent the successful operation of a component, so instead of making several different basic events for the same component in an FT, the “all modes” failure rate is used for the component whenever it is provided by the source. This number is conservative because it includes failure of component to start operation, which is not needed for the analysis of normal operating components because these are already in operation.

Passive components are found throughout the HVAC system. These include filters, pneumatic lines, ducts, wires and cables. All these passive components fail on a “per hour” basis, describing the failure of the component to continue passive operation.

Table 3. Basic Event Failure Rates and Probability Calculations

Component/ Subsystem Type	Failure Mode	Failure Rate	Unit:	Data Source	Basis for Probability	Probability of Basic Event in FT Model	Comment
Electric Power	Loss	6.388×10^{-05}	h	BSC 2004a, Section 7.3	λt	2.555×10^{-04}	Used for loss of power to motored fans in air-handling and exhaust subsystems
Spring Diaphragm Actuator	Fails to operate	0.36×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 487	λt	1.44×10^{-06}	Used to find failure prob. of Spring Actuated Opposed Blade Damper
Opposed Blade Damper	Fails to operate	1.75×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 1228	λt	7.00×10^{-06}	Used for Opposed Blade Damper and Spring Actuated Opposed Blade Damper
Pressure Transducer	Spurious operation	3.92×10^{-06}	h	Eide and Calley 1993, p. 1179	λt	1.57×10^{-05}	Used for Differential Pressure Relay
Computation Module - Averager	Fails to operate	1.00×10^{-05}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 713	λt	4.00×10^{-05}	Differential Pressure Computing Device
Shut-off 2-Position Parallel Blade Damper	Fails to operate	1.21×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 1227	λt	4.84×10^{-06}	Used to find failure prob. of Parallel Blade Damper
Damper Actuator, Pneumatic, piston type	Fails to operate	1.73×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 823	λt	6.92×10^{-06}	
Valve, Pneumatic Solenoid	Fails to operate	9.62×10^{-06}	h	Denson et al. 1991 Mil, GF p. 2-159	λt	3.85×10^{-05}	Used for Solenoid Valve
Centrifugal Air Intake Fan	Fails to operate	$7.61x10^{-06}$	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 1254	λt	3.04×10^{-05}	Used to find failure probability of Motored Fan in Air Handling Units
460 AC Motor 30-60 HP	Fails to operate	$5.70x10^{-06}$	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 225	λt	2.28×10^{-05}	Used to find failure probability of Motored Fan in Exhaust and Air Handling Units.
Exhaust Fan	Fails to operate	2.71×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 1256	λt	1.08×10^{-05}	Used to find failure probability of Motored Fan in Exhaust Fan Units
Electronic Controller	Fail to operate	1.19×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 735	λt	4.76×10^{-06}	Used for Fan Speed Controller
Solid State Logic Module	Fail to operate	3.00×10^{-06}	h	Eide & Calley 1993, p. 1180	λt	1.20×10^{-05}	Used for Logic Interlock and Hardwired Interlock

Table 3. Basic Event Failure Rates and Probability Calculations (Continued)

Component/ Subsystem Type	Failure Mode	Failure Rate	Unit:	Data Source	Basis for Probability	Probability of Basic Event in FT Model	Comment
Pressure Sensor Transmitter	Fail to operate	3.43×10^{-06}	h	Denson et al. 1991 G, p. 2-122	λt	1.37×10^{-05}	Used for Differential Pressure Transmitter
Pneumatic Differential Pressure Controller	Fail to operate	1.21×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 572	λt	4.84×10^{-06}	Used for Differential Pressure Controller
Control Box	Fail to operate	3.56×10^{-05}	h	Denson et al. 1991 Mil, A, p. 2-43	λt	1.42×10^{-04}	Control Start/Stop Signal
Electro-pneumatic Actuator	Fail to operate	0.28×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 498	λt	1.12×10^{-06}	Used to find failure probability for Slide Gate Damper
Damper	Spurious operation	3.00×10^{-07}	h	Eide & Calley 1993, p. 1178	λt	1.20×10^{-06}	
Switch, general	Spurious operation	1.00×10^{-06}	h	Eide & Calley 1993, p. 1179	λt	4.00×10^{-06}	Used for Start/ Stop Switch and Local Switch
	Fails to open/close	1.00×10^{-05}	d		q	1.00×10^{-05}	
Air Filter	Plugs	1.00×10^{-05}	h	Eide & Calley 1993, p. 1178	λt	4.00×10^{-05}	Used for Clogged HEPA Filter
Pipes/fittings ≥ 16” long	Fail to operate	1.81×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 1318	λt	7.24×10^{-06}	Used for Air Ducts
Heat Exchanger	Plugs	3.40×10^{-06}	h	CRWMS 1999, p. IV-2	λt	1.36×10^{-05}	Used for Clogged Air Handling Unit
Speed Transducer	Fail to operate	1.86×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 596	λt	7.44×10^{-06}	Used for Speed sensors
Transmitter	Fail to operate	1.22×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 686	λt	4.88×10^{-06}	Used for Speed transmitters
Temperature Transducer	Spurious operation	1.73×10^{-06}	h	IEEE Std 500-1984 (Reaffirmed 1991), p. 527	λt	6.92×10^{-06}	Used for smoke detector

NOTES: Mission time = 4 h (Section 6.2.4)

h hour

d demand

q Failure on demand of in-service component

λt Unavailability of in-service components during mission time = 1 - exp (Failure rate x Mission Time) ≅ Failure rate x Mission Time (NRC 1983, Section 5.3.1.1 Eq. 5.1).

The failure probability of the spring-actuated opposed blade damper, parallel blade damper, and slide gate damper were found by adding the failure probability of the actuating device and the damper. The failure probability of the spring-actuated, opposed blade damper is 8.44E-6, which includes the failure of the spring diaphragm actuator and the opposed blade damper. The failure probability of the parallel blade damper is 1.18E-5, which includes the failure of the pneumatic damper actuator and the shut-off two-position parallel blade damper. The failure probability of the slide gate damper is 2.32E-6, which includes the failure of the electro-pneumatic actuator and a generic damper. It is important to note that electro-pneumatic actuation was chosen in this analysis for the slide gate damper to represent the as-yet-undefined remote machine to be used with these dampers. Thus, it is left as an undeveloped event.

The failure probabilities of motored fans in the AHUs and in the exhaust fan units were found by adding the failure probability of the motor and of the respective fan. The failure probability of the motored fan in the AHUs is 5.32E-5. The failure probability of the motored fan in the exhaust fan units is 3.36E-5. Note that these numbers already include failure of the drive mechanism of the fans (IEEE Std 500-1984 (Reaffirmed 1991)) and therefore the ASD or adjustable speed drive does not have to be modeled in the FT.

The quantification of the undeveloped events that involve local switches and control signals with manual control capability in subtrees AIR_HANDL, HEPA_TRAINS, FILTR_PLENM, and EXHAUST_SYSTM, is solely based on the failure of the component (Assumption 5.1). These events will be developed at a later time to include human failure as necessary.

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. As noted in Section 6.2.5, the present analysis includes the category of CCFs that are termed implicit CCFs.

The first step in implicit CCF analysis is to identify which components are identical and redundant in a subsystem, and subject to a CCF (Section 6.2.5). Redundant components in a subsystem subject to a CCF are those that are the same type, that are in parallel with each other, and that perform the same function under the same operating conditions. Next, the probability of the identified CCF events is derived by multiplying the failure probability of the basic event by the CCF factor based on the Alpha Factor Method found in column four of Table 4. In the same way, the independent failure probability of a component that is treated in the Alpha Factor CCF modeling is derived by multiplying the total failure probability of the basic event by the α_1 symbol. However, since this factor is close to 1.0 for all cases (i.e., 0.9 or greater), this analysis conservatively ignores this reduction factor and uses the total failure probability as the probability of an independent failure.

The first column of Table 4 identifies common-cause component group (CCCG) size or the number of redundant components subject to CCF in a system. The second column defines how many components out of the group are needed for success. The third column contains the formulas used to derive the CCF factors, which are in the fourth column. These factors are based on a staggered maintenance schedule for the components (Assumption 5.2).

Table 4. Alpha Factor Expressions for Common Cause Failure (Staggered Maintenance)

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

CCCG = common-cause component group; CCF = common-cause failure

Source: (BSC 2004n, Table II-2)

Attachment C, Figures C-2 through C-6, and Attachment D, Figures D-2 through D-6, show subtrees that represent subsystems of the HVAC system in the primary confinement areas of DTF 1 and the FHF, respectively. Each subtree is scoped for redundant components subject to CCF, starting with subtree AIR_HANDL in Attachment C, Figure C-2, for DTF 1.

6.3.4.1 Air-Handling Subsystem

DTF 1

Subtree AIR_HANDL (Attachment C, Figure C-2) for DTF 1 has an input called CCF_AIRHANDL (not described in Section 6.3.2.1) that if TRUE, can cause the failure of the air-handling subsystem in DTF 1. OR-gate CCF_AIRHANDL is composed of 14 inputs that identify 14 redundant events found in all normally operating AHUs. These are represented by the following basic events:

- CCF_AIRHANDL_HINTLOCK: CCF Hardwired Interlock (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three hardwired interlocks in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three hardwired interlocks, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.2E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.44E-7 for CCF_ AIRHANDL_HINTLOCK.

- CCF_AIRHANDL_SPEED: CCF Fan Speed Controller (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three normally operating fan speed controllers in the air-handling subsystem, one for each AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three fan speed controllers, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.76E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.95E-7 for CCF_ AIRHANDL_SPEED.

- CCF_AIRHANDL_FAN: CCF Motored Fan (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three normally operating motored fans in the air-handling subsystem, one for each AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three motored fans are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 5.32E-6 from Section 6.3.3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 3.30E-6 for CCF_ AIRHANDL_FAN.

- CCF_AIRHANDL_DAMPR: CCF Parallel Blade Damper one (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three parallel blade dampers upstream of the AHUs in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three parallel blade dampers, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.18E-5 from Section 6.3.3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.32E-7 for CCF_ AIRHANDL_DAMPR.

- CCF_AIRHANDL_DAMPR2: CCF Parallel Blade Damper two (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three parallel blade dampers downstream of the AHUs in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three parallel blade dampers, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.18E-5 from Section 6.3.3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.32E-7 for CCF_ AIRHANDL_DAMPR2.

- CCF_AIRHANDL_3WYVAL: CCF Solenoid Valve one (2/3) Air Handling Subsystem.

This event was derived by observing that there is a total of three solenoid valves upstream of the AHUs in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three solenoid valves, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 3.85E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.39E-6 for CCF_ AIRHANDL_3WYVAL.

- CCF_AIRHANDL_3WYVAL2: CCF Solenoid Valve two (2/3) Air Handling Subsystem.

This event was derived by observing that there is a total of three solenoid valves downstream of the AHUs in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three solenoid valves, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 3.85E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.39E-6 for CCF_ AIRHANDL_3WYVAL2.

- CCF_AIRHANDL_DUCT: CCF Air Duct (2/3) - Air Handling Subsystem.

This event was derived by observing that there is a total of three air ducts in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three air ducts, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.24E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.49E-7 for CCF_ AIRHANDL_DUCT.

- CCF_AIRHANDL_PLUG: CCF Air Handling Unit (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three air filters in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three air filters, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.36E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 8.43E-7 for CCF_ AIRHANDL_PLUG.

- CCF_AIRHANDL_SWITCH: CCF Local Start/Stop Switch (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three local start/stop switches in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three local start/stop switches, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.00E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.48E-7 for CCF_ AIRHANDL_SWITCH.

- CCF_AIRHANDL_SMOKE: CCF Smoke Detector (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three smoke detectors in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three smoke detectors, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 6.92E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.29E-7 for CCF_ AIRHANDL_SMOKE.

- CCF_AIRHANDL_INTLOCK: CCF Logic Interlock (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three logic interlocks in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three logic interlock, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.2E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.44E-7 for CCF_ AIRHANDL_INTLOCK.

- CCF_AIRHANDL_SENSR: CCF Speed Sensor (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three speed sensors in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three speed sensors, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.44E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.61E-7 for CCF_ AIRHANDL_SENSR.

- CCF_AIRHANDL_TRANS: CCF Speed Transmitter (2/3) – Air Handling Subsystem.

This event was derived by observing that there is a total of three speed transmitters in the air-handling subsystem, one for each normally operating AHU. From Part 2 of the success criteria (Section 6.3), it is known that two fans are required for successful operation. Thus, two out of three speed transmitters, which are supporting equipment to two fans, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.88E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 3.03E-7 for CCF_ AIRHANDL_TRANS.

FHF

There is only one normally operating unit in the FHF of which one is needed for success (Section 6.3). Thus , there is no CCF input in Subtree AIR_HANDL (Attachment D, Figure D-2).

6.3.4.2 Primary Confinement Zones

DTF 1

Subtree PRIMARY_ZONES (Attachment C, Figure C-3) for DTF 1 has no CCF inputs because there are no redundant components.

FHF

Subtree PRIMARY_ZONES (Attachment D, Figure D-3) for FHF has no CCF inputs because there are no redundant components.

6.3.4.3 Remote High Efficiency Particulate Air Trains Subsystem

DTF 1

Subtree HEPA_TRAINS (Attachment C, Figure C-4) for DTF 1 has an input called CCF_TRAINS (not described in Section 6.3.2.3) that if TRUE, can cause the failure of the remote HEPA trains subsystem in DTF 1. OR-gate CCF_TRAINS is composed of four inputs that identify four redundant events found in all normally operating HEPA filter trains. These are represented by the following basic events:

- CCF_TRAINS_DUCT: CCF Air Duct (4/4) –HEPA Trains Subsystem.

This event was derived by observing that there is a total of four air ducts in the remote HEPA trains subsystem, one for each normally operating HEPA filter train. The remote HEPA trains subsystem must meet part one of the success criteria: maintain negative differential pressure. Thus, the loss of HVAC function can occur in the remote HEPA trains subsystem if less than all four HEPA filter trains successfully maintain a flow path. Thus, four out of four air ducts that support four HEPA filter trains are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.24E-6 from Table 3 by a factor of 0.075 from Table 4 that represents a four-out-of-four success configuration. This results in a failure probability of 5.43E-7 for CCF_ TRAINS_DUCT.

- CCF_TRAINS_HEPA: CCF HEPA Filter (4/4) – HEPA Trains Subsystem.

This event was derived by observing that there are a total of four HEPA filters in the remote HEPA trains subsystem, one for each normally operating HEPA filter train. The remote HEPA trains subsystem must meet part one of the success criteria: maintain negative differential pressure. Thus, the loss of HVAC function can occur in the remote HEPA trains subsystem if less than all four HEPA filter trains successfully maintain a flow path. Thus, four out of four HEPA filters are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.00E-5 from Table 3 by a factor of 0.075 from Table 4 that represents a four-out-of-four success configuration. This results in a failure probability of 3.00E-6 for CCF_ TRAINS_HEPA.

- CCF_TRAINS_VDAMPR: CCF Slide Gate Damper one (4/4) – HEPA Trains Subsystem.

This event was derived by observing that there is a total of four slide gate dampers upstream of the HEPA filters in the remote HEPA trains subsystem, one for each normally operating HEPA filter train. The remote HEPA trains subsystem must meet part one of the success criteria: maintain negative differential pressure. Thus, the loss of HVAC function can occur in the remote HEPA trains subsystem if less than all four HEPA filter trains successfully maintain a flow path. Thus, four out of four upstream slide gate dampers are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 2.32E-6 from Section 6.3.3 by a factor of 0.075 from Table 4 that represents a four-out-of-four success configuration. This results in a failure probability of 1.74E-7 for CCF_ TRAINS_VDAMPR.

- CCF_TRAINS_VDAMPR2: CCF Slide Gate Damper two (4/4) – HEPA Trains Subsystem.

This event was derived by observing that there is a total of four slide gate dampers downstream of the HEPA filters in the remote HEPA trains subsystem, one for each normally operating HEPA filter train. The remote HEPA trains subsystem must meet part one of the success criteria: maintain negative differential pressure. Thus, the loss of HVAC function can occur in the remote HEPA trains subsystem if less than all four HEPA filter trains successfully maintain a flow path. Thus, four out of four upstream slide gate dampers are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 2.32E-6 from Section 6.3.3 by a factor of 0.075 from Table 4 that represents a four-out-of-four success configuration. This results in a failure probability of 1.74E-7 for CCF_ TRAINS_VDAMPR2.

FHF

Subtree HEPA_TRAINS (Attachment D, Figure D-4) for FHF is derived in the same fashion as that explained above for DTF 1.

6.3.4.4 High Efficiency Particulate Air Filter Plenum Subsystem

DTF 1

Subtree FILTR_PLENM (Attachment C, Figure C-5) for DTF 1 has an input called CCF_FILTR (not described in Section 6.3.2.4) that if TRUE, can cause the failure of the HEPA filter plenum subsystem in DTF 1. OR-gate CCF_FILTR is composed of nine inputs that identify nine redundant events found in all normally operating HEPA filter units. These are represented by the following basic events:

- CCF_FILTR_3WYVAL: CCF Solenoid Valve (3/4): HEPA Filter Plenum Subsystem.

This event was derived by observing that there is a total of four solenoid valves in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four solenoid valves that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 3.85E-5 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 2.89E-6 for CCF_ FILTR_3WYVAL.

- CCF_FILTR_HEPA: CCF HEPA Filter one (3/4): HEPA Filter Plenum Subsystem.

This event was derived by observing that there is a total of four HEPA-1 filters in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four HEPA filters that support three normally operating HEPA filter units, rated at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.00E-5 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 3.00E-6 for CCF_ FILTR_HEPA.

- CCF_FILTR_HEPA2: CCF HEPA Filter two (3/4): HEPA Filter Plenum Subsystem.

This event was derived by observing that there is a total of four HEPA-2 filters in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four HEPA filters that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.00E-5 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 3.00E-6 for CCF_ FILTR_HEPA2.

- CCF_FILTR_DAMPR: CCF Parallel Blade Damper one (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there is a total of four parallel blade-1 dampers in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four parallel blade dampers that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.18E-5 from Section 6.3.3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 8.85E-7 for CCF_ FILTR_DAMPR.

- CCF_FILTR_DAMPR2: CCF Parallel Blade Damper two (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there is a total of four parallel blade-2 dampers in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four parallel blade dampers that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.18E-5 from Section 6.3.3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 8.85E-7 for CCF_ FILTR_DAMPR2.

- CCF_FILTR_DUCT: CCF Air Duct (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there are a total of four air ducts in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four air ducts that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.24E-6 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 5.43E-7 for CCF_ FILTR_DUCT.

- CCF_FILTR_OBDAMPR: CCF Opposed Blade Damper one (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there are a total of four opposed blade-1 dampers in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three normally operating HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four opposed blade dampers that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.00E-6 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 5.25E-7 for CCF_ FILTR_OBDAMPR.

- CCF_FILTR_OBDAMPR2: CCF Opposed Blade Damper two (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there are a total of four opposed blade-2 dampers in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three normally operating HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four opposed blade dampers that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.00E-6 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 5.25E-7 for CCF_ FILTR_OBDAMPR2.

- CCF_FILTR_OBDAMPR3: CCF Opposed Blade Damper three (3/4) – HEPA Filter Plenum Subsystem.

This event was derived by observing that there are a total of four opposed blade-3 dampers in the HEPA filter plenum subsystem, one for each normally operating HEPA filter unit leakage collection line. The HEPA filter plenum subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a volumetric flow rate to support the air capacity of two exhaust fans (Section 6.3). Thus, the loss of HVAC function can occur in the HEPA filter plenum subsystem if less than three normally operating HEPA filter plenum units, operating at 26,250 cfm, successfully maintain a flow path for the success of negative differential pressure and the airflow requirement. Thus, three out of four opposed blade dampers that support three normally operating HEPA filter units, operating at 26,250 cfm, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.00E-6 from Table 3 by a factor of 0.075 from Table 4 that represents a three-out-of-four success configuration. This results in a failure probability of 5.25E-7 for CCF_ FILTR_OBDAMPR3.

FHF

There is only one normally operating HEPA filter plenum unit in FHF and it is needed for success. Thus , there is no CCF input in Subtree FILTR_PLENM (Attachment D, Figure D-5).

6.3.4.5 Exhaust Fan Subsystem

DTF 1

Subtree EXHAUST_SYSTM (Attachment C, Figure C-6) for DTF 1 has an input called CCF_EXSYS (not described in Section 6.3.2.5) that if TRUE, can cause the failure of the exhaust fan subsystem in DTF 1. OR-gate CCF_EXSYS is composed of 11 inputs that identify 11 redundant events found in all normally operating exhaust fan units. These are represented by the following basic events:

- CCF_EXSYS_OBDAMPR: CCF Opposed Blade Damper (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three opposed blade dampers in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the air-flow requirement. Thus, two out of three opposed blade dampers, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.00E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.34E-7 for CCF_ EXSYS_OBDAMPR.

- CCF_EXSYS_DAMPR: CCF Parallel Blade Damper (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three parallel blade dampers in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three parallel blade dampers, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.18E-5 from Section 6.3.3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.32E-7 for CCF_ EXSYS_DAMPR.

- CCF_EXSYS_DUCT: CCF Air Duct (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three air ducts in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three air ducts, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.24E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.49E-7 for CCF_ EXSYS_DUCT.

- CCF_EXSYS_FAN: CCF Motored Fan (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three motored fans in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three motored fans are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 3.36E-5 from Section 6.3.3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.08E-6 for CCF_ EXSYS_FAN.

- CCF_EXSYS_SENSR: CCF Speed Sensor (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three speed sensors in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three speed sensors, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 7.44E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 4.61E-7 for CCF_ EXSYS_SENSR.

- CCF_EXSYS_TRANS: CCF Speed Transmitter (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three speed transmitters in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three speed transmitters, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.88E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 3.03E-7 for CCF_ EXSYS_TRANS.

- CCF_EXSYS_HINTLOCK: CCF Hardwired Interlock (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three hardwired interlocks in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three hardwired interlocks, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.2E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.44E-7 for CCF_ EXSYS_HINTLOCK.

- CCF_EXSYS_SPEED: CCF Fan Speed Controller (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three fan speed controllers in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three fan speed controllers, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.76E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.95E-7 for CCF_ EXSYS_SPEED.

- CCF_EXSYS_3WYVAL: CCF Solenoid Valve (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three solenoid valves in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the air-flow requirement. Thus, two out of three solenoid valves, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 3.85E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a 2-out-of-3 success configuration. This results in a failure probability of 2.39E-6 for CCF_ EXSYS_3WYVAL.

- CCF_EXSYS_INTLOCK: CCF Logic Interlock (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three logic interlocks in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three logic interlocks, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 1.2E-5 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 7.44E-7 for CCF_ EXSYS_INTLOCK.

- CCF_EXSYS_SWITCH: CCF Start/Stop Switch (2/3) – Exhaust Fan Subsystem.

This event was derived by observing that there is a total of three local start/stop switches in the exhaust fan subsystem, one for each normally operating exhaust fan unit. The exhaust fan subsystem must meet both parts of the success criteria: maintain negative differential pressure and meet a minimum volumetric flow rate of 46,014 cfm (Table 1). Thus, the loss of HVAC function can occur in the exhaust fan subsystem if less than two normally operating exhaust fans successfully operate, which will not meet the airflow requirement. Thus, two out of three local start/stop switches, which are supporting equipment to two exhaust fan units, are required to be successful in this CCF event.

This event is then quantified by multiplying the event failure probability of 4.00E-6 from Table 3 by a factor of 0.062 from Table 4 that represents a two-out-of-three success configuration. This results in a failure probability of 2.48E-7 for CCF_ EXSYS_SWITCH.

FHF

There is only one normally operating exhaust fan unit in FHF and it is needed for success (Section 6.3). Thus, there is no CCF input in Subtree EXHAUST_SYSTM (Attachment D, Figure D-6).

6.4 FAULT TREE ANALYSIS RESULTS

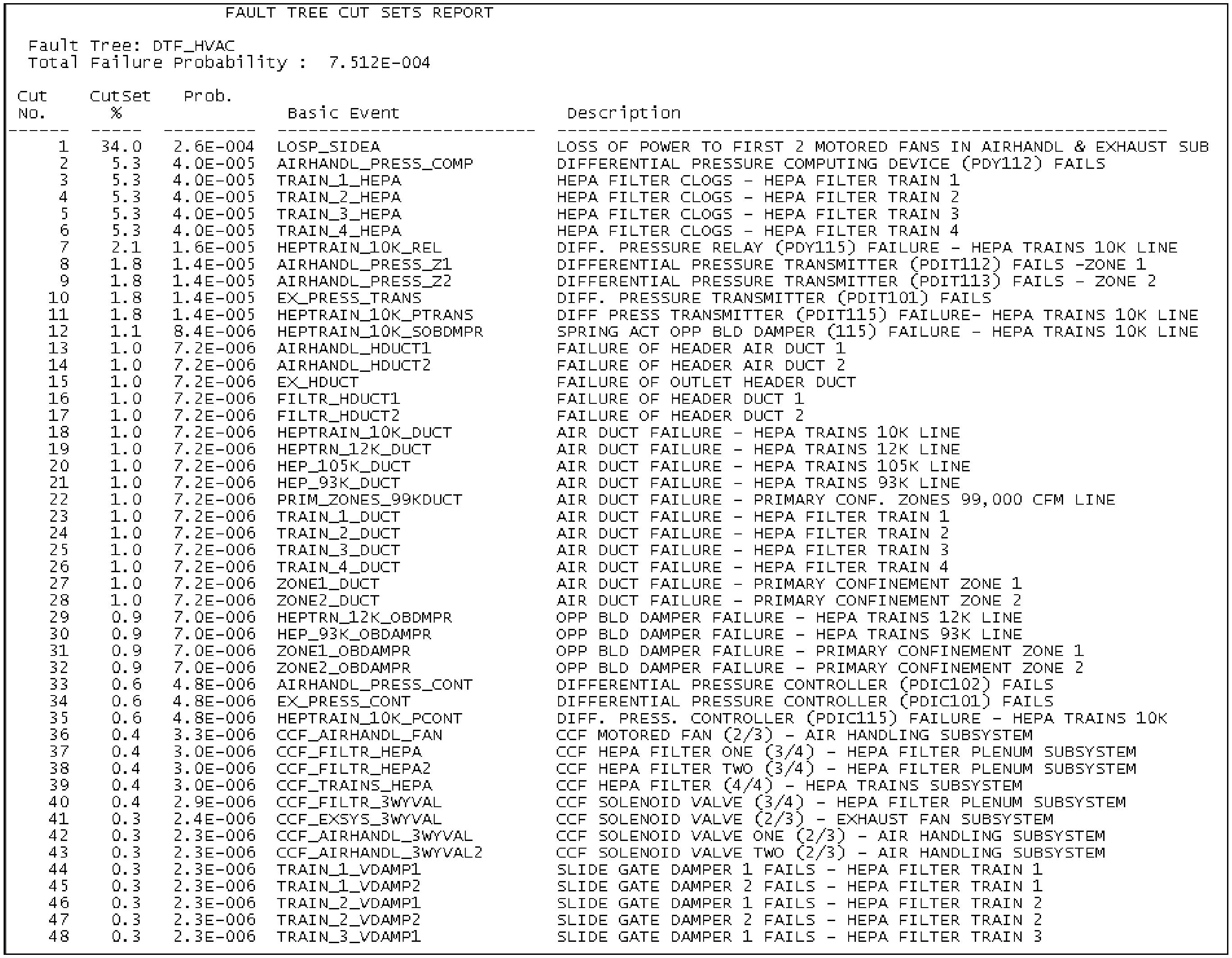
Once the FTs for the DTF 1 and FHF have been modeled and failure probabilities have been input into all basic events, the FTs are solved with the aid of SAPHIRE to identify and quantify the minimal cut sets (Section 6.2.6). The result is output in a quantitative Cut Set Report (Tables 5 and 6).

DTF 1

A detailed quantitative cut set list of the top 48 cut sets is shown on 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 60.5 percent of the total probability, are six “singles” that represent the loss of power to the first two motored fans in the air-handling and exhaust subsystems, the failure of the differential pressure computing device in the air-handling subsystem, and the blockage of the HEPA filters in the remote HEPA trains subsystem. These events are found in subtree AIR_HANDL (Attachment C, Figure C-2), EXHAUST_SYSTM (Attachment C, Figure C-6), and subtree HEPA_TRAINS (Attachment C, Figure C-4). The seventh cut set represents the failure of the differential pressure relay in the remote HEPA trains subsystem and is found in subtree HEPA_TRAINS (Attachment C, Figure C-4). Cut sets eight through ten are “singles” that represent the failure of the differential pressure transmitter in the primary confinement zones and HEPA filter plenum subsystem, and are found in subtrees AIR_HANDL (Attachment C, Figure C-2) and EXHAUST_SYSTM (Attachment C, Figure C-6). Cut sets 11 and 12 represent the failure of the differential pressure transmitter and the spring actuated opposed blade damper in the remote HEPA trains subsystem and are found in subtree HEPA _TRAINS (Attachment C, Figure C-4). Cut sets 13 through 28 are “singles” that represent the failure of air ducts throughout the DTF 1 primary confinement HVAC system and together make 16 percent of the total failure probability.

The complete cut set report for DTF 1 shows that the top event can occur from any one of 81 “singles” that combine to give a probability of 7.506E-4, and any one of 1,487 “doubles” that combine to give a probability of 5.787E-7. All cut sets are added together and result in a final probability of 7.512E-4 for the occurrence of the top event in a 4-h mission time (Section 6.2.4) or 1.878E-4 failures per hour. This result is also applicable for DTF 2.

Table 5. SAPHIRE Cut Sets Report for Dry Transfer Facility 1



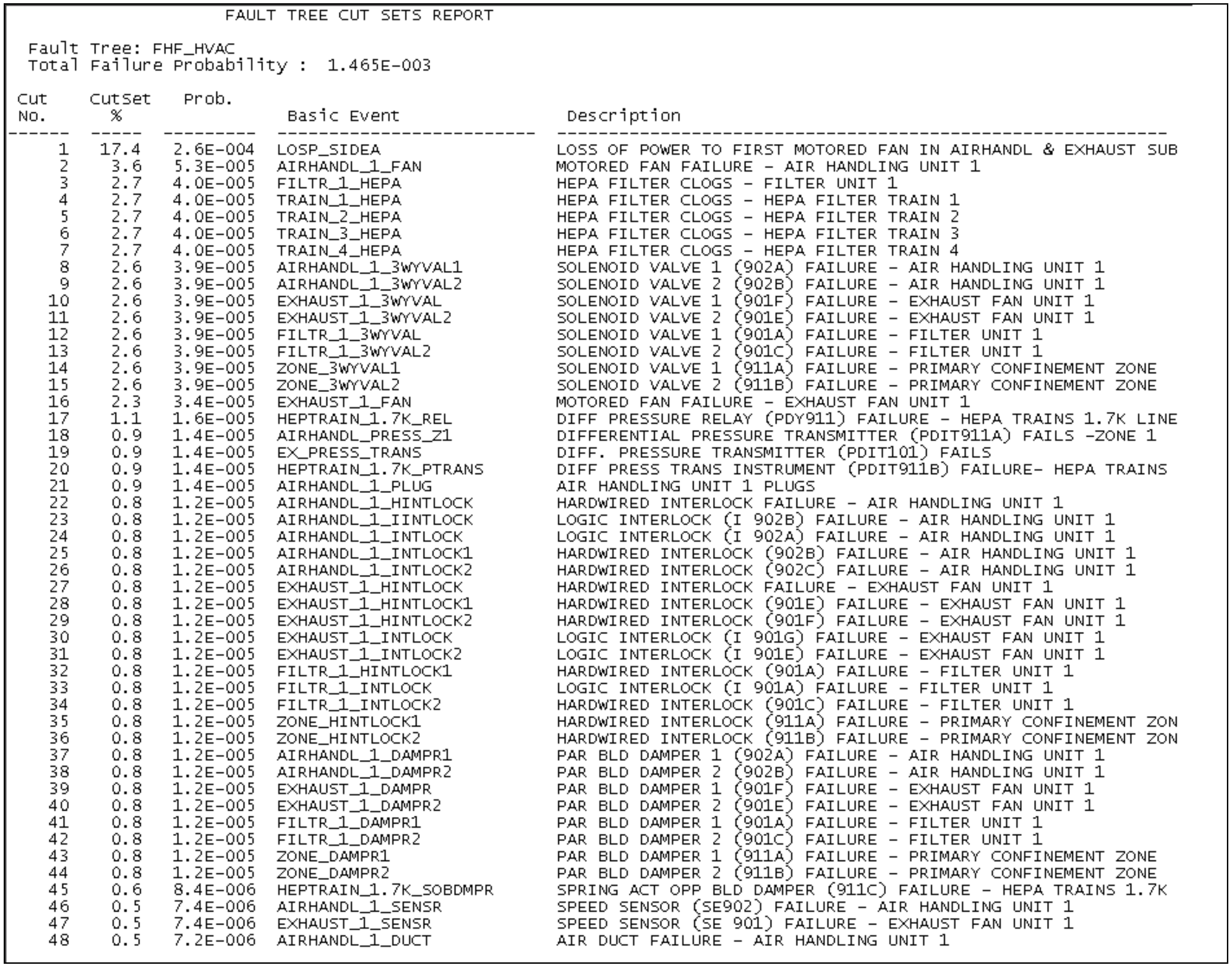
```
                      FAULT TREE CUT SETS REPORT

  Fault Tree: DTF_HVAC
  Total Failure Probability :  7.512E-004

 Cut    CutSet   Prob.
 No.      %                Basic Event                Description
------  -----  ---------  -------------------------  ------------------------------------------------------------
     1   34.0  2.6E-004   LOSP_SIDEA                 LOSS OF POWER TO FIRST 2 MOTORED FANS IN AIRHANDL & EXHAUST SUB
     2    5.3  4.0E-005   AIRHANDL_PRESS_COMP        DIFFERENTIAL PRESSURE COMPUTING DEVICE (PDY112) FAILS
     3    5.3  4.0E-005   TRAIN_1_HEPA               HEPA FILTER CLOGS - HEPA FILTER TRAIN 1
     4    5.3  4.0E-005   TRAIN_2_HEPA               HEPA FILTER CLOGS - HEPA FILTER TRAIN 2
     5    5.3  4.0E-005   TRAIN_3_HEPA               HEPA FILTER CLOGS - HEPA FILTER TRAIN 3
     6    5.3  4.0E-005   TRAIN_4_HEPA               HEPA FILTER CLOGS - HEPA FILTER TRAIN 4
     7    2.1  1.6E-005   HEPTRAIN_10K_REL           DIFF. PRESSURE RELAY (PDY115) FAILURE - HEPA TRAINS 10K LINE
     8    1.8  1.4E-005   AIRHANDL_PRESS_Z1          DIFFERENTIAL PRESSURE TRANSMITTER (PDIT112) FAILS -ZONE 1
     9    1.8  1.4E-005   AIRHANDL_PRESS_Z2          DIFFERENTIAL PRESSURE TRANSMITTER (PDIT113) FAILS - ZONE 2
    10    1.8  1.4E-005   EX_PRESS_TRANS             DIFF. PRESSURE TRANSMITTER (PDIT101) FAILS
    11    1.8  1.4E-005   HEPTRAIN_10K_PTRANS        DIFF PRESS TRANSMITTER (PDIT115) FAILURE- HEPA TRAINS 10K LINE
    12    1.1  8.4E-006   HEPTRAIN_10K_SOBDMPR       SPRING ACT OPP BLD DAMPER (115) FAILURE - HEPA TRAINS 10K LINE
    13    1.0  7.2E-006   AIRHANDL_HDUCT1            FAILURE OF HEADER AIR DUCT 1
    14    1.0  7.2E-006   AIRHANDL_HDUCT2            FAILURE OF HEADER AIR DUCT 2
    15    1.0  7.2E-006   EX_HDUCT                   FAILURE OF OUTLET HEADER DUCT
    16    1.0  7.2E-006   FILTR_HDUCT1               FAILURE OF HEADER DUCT 1
    17    1.0  7.2E-006   FILTR_HDUCT2               FAILURE OF HEADER DUCT 2
    18    1.0  7.2E-006   HEPTRAIN_10K_DUCT          AIR DUCT FAILURE - HEPA TRAINS 10K LINE
    19    1.0  7.2E-006   HEPTRN_12K_DUCT            AIR DUCT FAILURE - HEPA TRAINS 12K LINE
    20    1.0  7.2E-006   HEP_105K_DUCT              AIR DUCT FAILURE - HEPA TRAINS 105K LINE
    21    1.0  7.2E-006   HEP_93K_DUCT               AIR DUCT FAILURE - HEPA TRAINS 93K LINE
    22    1.0  7.2E-006   PRIM_ZONES_99KDUCT         AIR DUCT FAILURE - PRIMARY CONF. ZONES 99,000 CFM LINE
    23    1.0  7.2E-006   TRAIN_1_DUCT               AIR DUCT FAILURE - HEPA FILTER TRAIN 1
    24    1.0  7.2E-006   TRAIN_2_DUCT               AIR DUCT FAILURE - HEPA FILTER TRAIN 2
    25    1.0  7.2E-006   TRAIN_3_DUCT               AIR DUCT FAILURE - HEPA FILTER TRAIN 3
    26    1.0  7.2E-006   TRAIN_4_DUCT               AIR DUCT FAILURE - HEPA FILTER TRAIN 4
    27    1.0  7.2E-006   ZONE1_DUCT                 AIR DUCT FAILURE - PRIMARY CONFINEMENT ZONE 1
    28    1.0  7.2E-006   ZONE2_DUCT                 AIR DUCT FAILURE - PRIMARY CONFINEMENT ZONE 2
    29    0.9  7.0E-006   HEPTRN_12K_OBDMPR          OPP BLD DAMPER FAILURE - HEPA TRAINS 12K LINE
    30    0.9  7.0E-006   HEP_93K_OBDAMPR            OPP BLD DAMPER FAILURE - HEPA TRAINS 93K LINE
    31    0.9  7.0E-006   ZONE1_OBDAMPR              OPP BLD DAMPER FAILURE - PRIMARY CONFINEMENT ZONE 1
    32    0.9  7.0E-006   ZONE2_OBDAMPR              OPP BLD DAMPER FAILURE - PRIMARY CONFINEMENT ZONE 2
    33    0.6  4.8E-006   AIRHANDL_PRESS_CONT        DIFFERENTIAL PRESSURE CONTROLLER (PDIC102) FAILS
    34    0.6  4.8E-006   EX_PRESS_CONT              DIFFERENTIAL PRESSURE CONTROLLER (PDIC101) FAILS
    35    0.6  4.8E-006   HEPTRAIN_10K_PCONT         DIFF. PRESS. CONTROLLER (PDIC115) FAILURE - HEPA TRAINS 10K
    36    0.4  3.3E-006   CCF_AIRHANDL_FAN           CCF MOTORED FAN (2/3) - AIR HANDLING SUBSYSTEM
    37    0.4  3.0E-006   CCF_FILTR_HEPA             CCF HEPA FILTER ONE (3/4) - HEPA FILTER PLENUM SUBSYSTEM
    38    0.4  3.0E-006   CCF_FILTR_HEPA2            CCF HEPA FILTER TWO (3/4) - HEPA FILTER PLENUM SUBSYSTEM
    39    0.4  3.0E-006   CCF_TRAINS_HEPA            CCF HEPA FILTER (4/4) - HEPA TRAINS SUBSYSTEM
    40    0.4  2.9E-006   CCF_FILTR_3WYVAL           CCF SOLENOID VALVE (3/4) - HEPA FILTER PLENUM SUBSYSTEM
    41    0.3  2.4E-006   CCF_EXSYS_3WYVAL           CCF SOLENOID VALVE (2/3) - EXHAUST FAN SUBSYSTEM
    42    0.3  2.3E-006   CCF_AIRHANDL_3WYVAL        CCF SOLENOID VALVE ONE (2/3) - AIR HANDLING SUBSYSTEM
    43    0.3  2.3E-006   CCF_AIRHANDL_3WYVAL2       CCF SOLENOID VALVE TWO (2/3) - AIR HANDLING SUBSYSTEM
    44    0.3  2.3E-006   TRAIN_1_VDAMP1             SLIDE GATE DAMPER 1 FAILS - HEPA FILTER TRAIN 1
    45    0.3  2.3E-006   TRAIN_1_VDAMP2             SLIDE GATE DAMPER 2 FAILS - HEPA FILTER TRAIN 1
    46    0.3  2.3E-006   TRAIN_2_VDAMP1             SLIDE GATE DAMPER 1 FAILS - HEPA FILTER TRAIN 2
    47    0.3  2.3E-006   TRAIN_2_VDAMP2             SLIDE GATE DAMPER 2 FAILS - HEPA FILTER TRAIN 2
    48    0.3  2.3E-006   TRAIN_3_VDAMP1             SLIDE GATE DAMPER 1 FAILS - HEPA FILTER TRAIN 3
```

FHF

A detailed quantitative cut set list of the top 48 cut sets is shown on 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 34.5 percent of the total probability, are seven “singles” that represent the loss of power to the first motored fans in the air-handling and exhaust subsystems, the failure of the motored fan in the air-handling subsystem, and the blockage of the HEPA filters in the HEPA filter plenum subsystem and remote HEPA trains subsystem. These events are found in subtrees AIR_HANDL (Attachment D, Figure D-2), HEPA_TRAINS (Attachment D, Figure D-4), and FILTR_PLENM (Attachment D, Figure D-5) and EXHAUST_SYSTM (Attachment D, Figure D-6). Cut sets eight through fifteen are “singles” that represent the failure of solenoid valves throughout the FHF primary confinement HVAC system. Cut set 16 is a “single” that represents the failure of the motored fan in the exhaust fan subsystem and is found in subtree EXHAUST_SYSTM (Attachment D, Figure D-6).

The complete cut set report for FHF shows that the top event can occur from any one of 97 “singles” that combine to give a probability of 1.465E-3. All cut sets are added together and result in a final probability of 1.465E-3 for the occurrence of the top event in a 4-h mission time (Section 6.2.4), or 3.663E-4 failures per hour.

Table 6. SAPHIRE Cut Sets Report for Fuel Handling Facility



```
                    FAULT TREE CUT SETS REPORT

 Fault Tree: FHF_HVAC
 Total Failure Probability :  1.465E-003

Cut    CutSet   Prob.
No.      %                Basic Event                 Description
------ -----  ---------  -------------------------   -------------------------------------------------------------
     1  17.4  2.6E-004   LOSP_SIDEA                  LOSS OF POWER TO FIRST MOTORED FAN IN AIRHANDL & EXHAUST SUB
     2   3.6  5.3E-005   AIRHANDL_1_FAN              MOTORED FAN FAILURE - AIR HANDLING UNIT 1
     3   2.7  4.0E-005   FILTR_1_HEPA                HEPA FILTER CLOGS - FILTER UNIT 1
     4   2.7  4.0E-005   TRAIN_1_HEPA                HEPA FILTER CLOGS - HEPA FILTER TRAIN 1
     5   2.7  4.0E-005   TRAIN_2_HEPA                HEPA FILTER CLOGS - HEPA FILTER TRAIN 2
     6   2.7  4.0E-005   TRAIN_3_HEPA                HEPA FILTER CLOGS - HEPA FILTER TRAIN 3
     7   2.7  4.0E-005   TRAIN_4_HEPA                HEPA FILTER CLOGS - HEPA FILTER TRAIN 4
     8   2.6  3.9E-005   AIRHANDL_1_3WYVAL1          SOLENOID VALVE 1 (902A) FAILURE - AIR HANDLING UNIT 1
     9   2.6  3.9E-005   AIRHANDL_1_3WYVAL2          SOLENOID VALVE 2 (902B) FAILURE - AIR HANDLING UNIT 1
    10   2.6  3.9E-005   EXHAUST_1_3WYVAL            SOLENOID VALVE 1 (901F) FAILURE - EXHAUST FAN UNIT 1
    11   2.6  3.9E-005   EXHAUST_1_3WYVAL2           SOLENOID VALVE 2 (901E) FAILURE - EXHAUST FAN UNIT 1
    12   2.6  3.9E-005   FILTR_1_3WYVAL              SOLENOID VALVE 1 (901A) FAILURE - FILTER UNIT 1
    13   2.6  3.9E-005   FILTR_1_3WYVAL2             SOLENOID VALVE 2 (901C) FAILURE - FILTER UNIT 1
    14   2.6  3.9E-005   ZONE_3WYVAL1                SOLENOID VALVE 1 (911A) FAILURE - PRIMARY CONFINEMENT ZONE
    15   2.6  3.9E-005   ZONE_3WYVAL2                SOLENOID VALVE 2 (911B) FAILURE - PRIMARY CONFINEMENT ZONE
    16   2.3  3.4E-005   EXHAUST_1_FAN               MOTORED FAN FAILURE - EXHAUST FAN UNIT 1
    17   1.1  1.6E-005   HEPTRAIN_1.7K_REL           DIFF PRESSURE RELAY (PDY911) FAILURE - HEPA TRAINS 1.7K LINE
    18   0.9  1.4E-005   AIRHANDL_PRESS_Z1           DIFFERENTIAL PRESSURE TRANSMITTER (PDIT911A) FAILS -ZONE 1
    19   0.9  1.4E-005   EX_PRESS_TRANS              DIFF. PRESSURE TRANSMITTER (PDIT101) FAILS
    20   0.9  1.4E-005   HEPTRAIN_1.7K_PTRANS        DIFF PRESS TRANS INSTRUMENT (PDIT911B) FAILURE- HEPA TRAINS
    21   0.9  1.4E-005   AIRHANDL_1_PLUG             AIR HANDLING UNIT 1 PLUGS
    22   0.8  1.2E-005   AIRHANDL_1_HINTLOCK         HARDWIRED INTERLOCK FAILURE - AIR HANDLING UNIT 1
    23   0.8  1.2E-005   AIRHANDL_1_IINTLOCK         LOGIC INTERLOCK (I 902B) FAILURE - AIR HANDLING UNIT 1
    24   0.8  1.2E-005   AIRHANDL_1_INTLOCK          LOGIC INTERLOCK (I 902A) FAILURE - AIR HANDLING UNIT 1
    25   0.8  1.2E-005   AIRHANDL_1_INTLOCK1         HARDWIRED INTERLOCK (902B) FAILURE - AIR HANDLING UNIT 1
    26   0.8  1.2E-005   AIRHANDL_1_INTLOCK2         HARDWIRED INTERLOCK (902C) FAILURE - AIR HANDLING UNIT 1
    27   0.8  1.2E-005   EXHAUST_1_HINTLOCK          HARDWIRED INTERLOCK FAILURE - EXHAUST FAN UNIT 1
    28   0.8  1.2E-005   EXHAUST_1_HINTLOCK1         HARDWIRED INTERLOCK (901E) FAILURE - EXHAUST FAN UNIT 1
    29   0.8  1.2E-005   EXHAUST_1_HINTLOCK2         HARDWIRED INTERLOCK (901F) FAILURE - EXHAUST FAN UNIT 1
    30   0.8  1.2E-005   EXHAUST_1_INTLOCK           LOGIC INTERLOCK (I 901G) FAILURE - EXHAUST FAN UNIT 1
    31   0.8  1.2E-005   EXHAUST_1_INTLOCK2          LOGIC INTERLOCK (I 901E) FAILURE - EXHAUST FAN UNIT 1
    32   0.8  1.2E-005   FILTR_1_HINTLOCK1           HARDWIRED INTERLOCK (901A) FAILURE - FILTER UNIT 1
    33   0.8  1.2E-005   FILTR_1_INTLOCK             LOGIC INTERLOCK (I 901A) FAILURE - FILTER UNIT 1
    34   0.8  1.2E-005   FILTR_1_INTLOCK2            HARDWIRED INTERLOCK (901C) FAILURE - FILTER UNIT 1
    35   0.8  1.2E-005   ZONE_HINTLOCK1              HARDWIRED INTERLOCK (911A) FAILURE - PRIMARY CONFINEMENT ZON
    36   0.8  1.2E-005   ZONE_HINTLOCK2              HARDWIRED INTERLOCK (911B) FAILURE - PRIMARY CONFINEMENT ZON
    37   0.8  1.2E-005   AIRHANDL_1_DAMPR1           PAR BLD DAMPER 1 (902A) FAILURE - AIR HANDLING UNIT 1
    38   0.8  1.2E-005   AIRHANDL_1_DAMPR2           PAR BLD DAMPER 2 (902B) FAILURE - AIR HANDLING UNIT 1
    39   0.8  1.2E-005   EXHAUST_1_DAMPR             PAR BLD DAMPER 1 (901F) FAILURE - EXHAUST FAN UNIT 1
    40   0.8  1.2E-005   EXHAUST_1_DAMPR2            PAR BLD DAMPER 2 (901E) FAILURE - EXHAUST FAN UNIT 1
    41   0.8  1.2E-005   FILTR_1_DAMPR1              PAR BLD DAMPER 1 (901A) FAILURE - FILTER UNIT 1
    42   0.8  1.2E-005   FILTR_1_DAMPR2              PAR BLD DAMPER 2 (901C) FAILURE - FILTER UNIT 1
    43   0.8  1.2E-005   ZONE_DAMPR1                 PAR BLD DAMPER 1 (911A) FAILURE - PRIMARY CONFINEMENT ZONE
    44   0.8  1.2E-005   ZONE_DAMPR2                 PAR BLD DAMPER 2 (911B) FAILURE - PRIMARY CONFINEMENT ZONE
    45   0.6  8.4E-006   HEPTRAIN_1.7K_SOBDMPR       SPRING ACT OPP BLD DAMPER (911C) FAILURE - HEPA TRAINS 1.7K
    46   0.5  7.4E-006   AIRHANDL_1_SENSR            SPEED SENSOR (SE902) FAILURE - AIR HANDLING UNIT 1
    47   0.5  7.4E-006   EXHAUST_1_SENSR             SPEED SENSOR (SE 901) FAILURE - EXHAUST FAN UNIT 1
    48   0.5  7.2E-006   AIRHANDL_1_DUCT             AIR DUCT FAILURE - AIR HANDLING UNIT 1
```

7. CONCLUSION

This analysis is preliminary and is intended to develop and demonstrate the methodology to be followed for a reliability assessment, as well as to determine a numerical result. Since the HVAC design has not been developed in sufficient detail to allow evaluation of supporting systems, a more complete analysis will be required in the future. The present results provide an indication of the order of magnitude of the system reliability that meets the required goals. The present analysis also identified some design areas that will need to be addressed (e.g. air operated devices, items in section 4.6) as the design of the HVAC systems progresses.

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.

A failure rate of 2.5E-3 per hour for the DTFs and FHF primary confinement HVAC systems ensures that a Category 1 initiating event followed by a failure of the HVAC system is a Category 2 event sequence (BSC 2005, Section 6.3.1.3). Two dominant causes contribute to the failure of the HVAC system: equipment failure and loss of electrical power. Thus, the combined probability of mechanical equipment failure and loss of electrical power must be less than or equal to 2.5E-3 per hour for DTF 1, for DTF 2 and for the FHF.

DTF 1

The FTA results presented in Section 6.4 demonstrate that the failure rate of the nuclear HVAC system in the primary confinement of DTF 1, due to mechanical equipment failure and loss of electrical power, is 1.878E-4 failures per hour, which meets the design requirement of 2.5E-3 per hour. Based on the results of this analysis (Table 5), the contribution of mechanical equipment failure to the total HVAC failure rate is 66 percent, while the contribution of loss of electrical power to the total HVAC failure rate is 34 percent.

DTF 2

Because DTF 1 and DTF 2 are identical, the reliability of the HVAC system in the primary confinement of DTF 2 is the same as that for DTF 1 of 1.878E-4 failures per hour, which meets the design requirement of 2.5E-3 per hour.

FHF

The FTA results presented in Section 6.4 demonstrate that the failure rate of the nuclear HVAC system in the primary confinement of the FHF, due to mechanical equipment failure and loss of electrical power, is 3.663E-4 failures per hour, which meets the design requirement of 2.5E-3 per hour. Based on the results of this analysis (Table 6), the contribution of mechanical equipment failure to the total HVAC failure rate is of 82.6 percent, while the contribution of loss of electrical power to the total HVAC failure rate is of 17.4 percent.

8. REFERENCES

8.1 DOCUMENTS CITED

BSC (Bechtel SAIC Company) 2002. *Software Code: SAPHIRE.* V7.18. PC - Windows 2000/NT 4.0. 10325-7.18-00.

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.

BSC (Bechtel SAIC Company) 2004a. *Reliability Analysis of the Electrical Power Distribution System to Selected Portions of the Nuclear HVAC System.* 100-PSA-EE00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20041216.0029.

BSC (Bechtel SAIC Company) 2004b. *Dry Transfer Facility #1 Primary Confinement HVAC System Block Flow Diagram.* 110-M50-VNP0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040318.0020.

BSC (Bechtel SAIC Company) 2004c. *Dry Transfer Facility #1 Primary Supply HVAC System Air Handling Unit Ventilation Flow Diagram.* 110-M50-VNP0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040318.0021.

BSC (Bechtel SAIC Company) 2004d. *Dry Transfer Facility #1 Primary Confinement HVAC System Air Distribution Ventilation Flow Diagram.* 110-M50-VNP0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040318.0023.

BSC (Bechtel SAIC Company) 2004e. *Dry Transfer Facility #1 Primary Confinement HVAC Sys Remote HEPA Filters Ventilation Flow Diagram.* 110-M50-VNP0-00302-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040318.0024.

BSC (Bechtel SAIC Company) 2004f. *Dry Transfer Facility #1 Primary Confinement HVAC System Exhaust Ventilation Flow Diagram.* 110-M50-VNP0-00401-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040318.0025.

BSC (Bechtel SAIC Company) 2004g. *Fuel Handling Facility Primary Confinement HVAC System Block Flow Diagram.* 210-M50-VNP0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040621.0009.

BSC (Bechtel SAIC Company) 2004h. *Fuel Handling Facility Primary Confinement HVAC Sys Air Handling Unit Ventilation Flow Diagram.* 210-M50-VNP0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040621.0010.

BSC (Bechtel SAIC Company) 2004i. *Fuel Handling Facility Primary Confinement HVAC Sys Remote HEPA Filters Ventilation Flow Diagram.* 210-M50-VNP0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040621.0011.

BSC (Bechtel SAIC Company) 2004j. *Fuel Handling Facility Primary Confinement HVAC Sys Exhaust HEPA Filter & Exh Fan Ventilation Flow Diagram.* 210-M50-VNP0-00401-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040621.0012.

BSC (Bechtel SAIC Company) 2004k. *Dry Transfer Facility #1 - Ventilation Air Calculation.* 110-MAC-VN00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040223.0008.

BSC (Bechtel SAIC Company) 2004l. *Preclosure Consequence Analyses for License Application.* 000-00C-MGR0-00900-000-00B. Las Vegas, Nevada: Bechtel SAIC Company.

BSC (Bechtel SAIC Company) 2004m. *Fuel Handling Facility Ventilation Air Calculation.* 210-MAC-VN00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040616.0006.

BSC (Bechtel SAIC Company) 2004n. *Waste Package Transporter Preclosure Safety Analysis.* 800-MQC-HET0-00200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20040623.0002.

BSC (Bechtel SAIC Company) 2005. *Categorization of Event Sequences for License Application.* 000-00C-MGR0-00800-000-00B. Las Vegas, Nevada: Bechtel SAIC Company.

CRWMS M&O (Civilian Radiological Waste Management System Management & Operations Contractor) 1999. *Reliability Assessment of Waste Handling Building HVAC System.* BCBD00000-01717-0210-00008 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990621.0155.

Demetria, M. 2005. "HVAC Design Features to Include in Reliability Analysis - MM-05-067." Interoffice memorandum from M. Demetria (BSC) to T. Dunn, February 17, 2005, 0217054784. ACC: MOL.20050306.0365.

Denson, W.; Chandler, G.; Crowell, W.; and Wanner, R. 1991. *Nonelectronic Parts Reliability Data 1991.* NPRD-91. Rome, New York: Reliability Analysis Center. TIC: 245475.

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.

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.

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.

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.

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.

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.

SAIC (Science Applications International Corporation) 1998. *Nuclear Fuel Cycle Facility Accident Analysis Handbook.* NUREG/CR-6410. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010726.0069.

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.

8.2 CODES, STANDARDS, REGULATIONS AND PROCEDURES

10 CFR 63. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. Readily available.

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

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

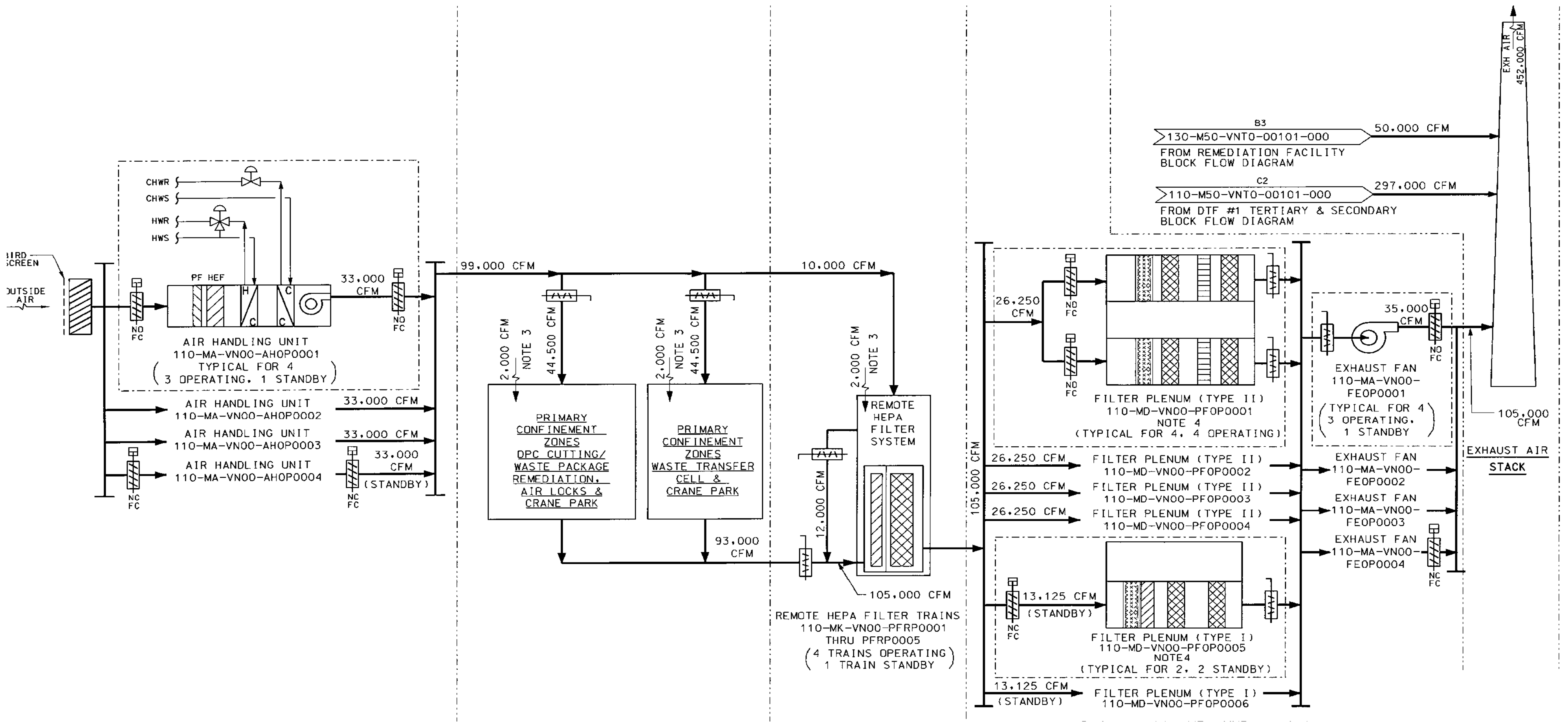
LP-SI.11Q-BSC. *Software Management.*

INTENTIONALLY LEFT BLANK

ATTACHMENT A

ARCHITECTURE OF THE DTF 1 PRIMARY CONFINEMENT NUCLEAR HVAC SYSTEM

INTENTIONALLY LEFT BLANK

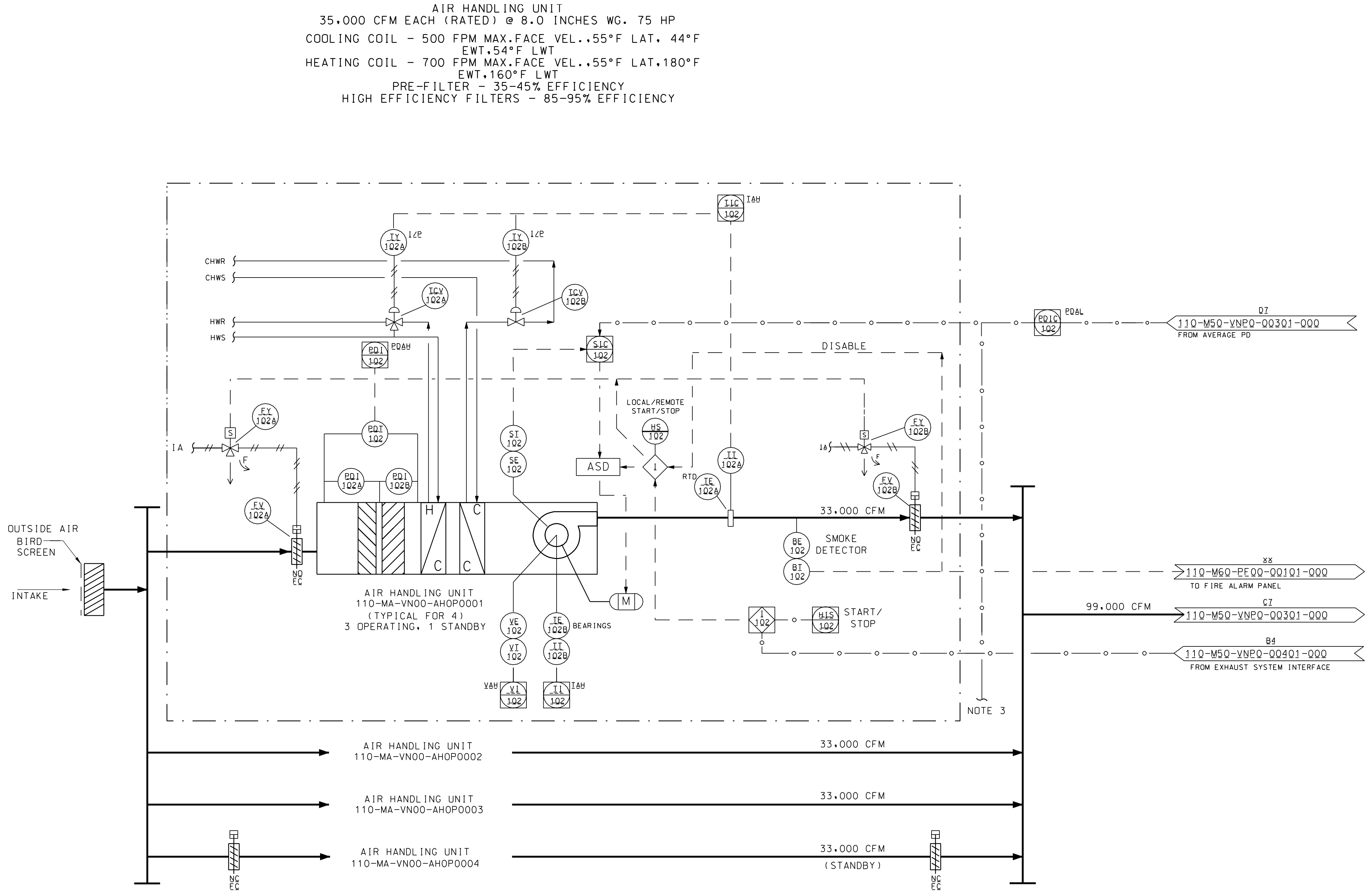

BIRD SCREEN
OUTSIDE AIR
CHWR
CHWS
HWR
HWS
PF HEF
H
C
NO FC
33,000 CFM
AIR HANDLING UNIT 110-MA-VN00-AHOP0001 TYPICAL FOR 4 (3 OPERATING, 1 STANDBY)
AIR HANDLING UNIT 110-MA-VN00-AHOP0002
33,000 CFM
AIR HANDLING UNIT 110-MA-VN00-AHOP0003
33,000 CFM
AIR HANDLING UNIT 110-MA-VN00-AHOP0004
33,000 CFM (STANDBY)
NC FC
99,000 CFM
2,000 CFM NOTE 3
44,500 CFM
PRIMARY CONFINEMENT ZONES
DPC CUTTING/ WASTE PACKAGE REMEDIATION, AIR LOCKS & CRANE PARK
PRIMARY CONFINEMENT ZONES
WASTE TRANSFER CELL & CRANE PARK
93,000 CFM
10,000 CFM
REMOTE HEPA FILTER SYSTEM
12,000 CFM
105,000 CFM
REMOTE HEPA FILTER TRAINS 110-MK-VN00-PFRP0001 THRU PFRP0005 (4 TRAINS OPERATING 1 TRAIN STANDBY)
105,000 CFM
26,250 CFM
FILTER PLENUM (TYPE II) 110-MD-VN00-PFOP0001 NOTE 4 (TYPICAL FOR 4, 4 OPERATING)
26,250 CFM
FILTER PLENUM (TYPE II) 110-MD-VN00-PFOP0002
26,250 CFM
FILTER PLENUM (TYPE II) 110-MD-VN00-PFOP0003
26,250 CFM
FILTER PLENUM (TYPE II) 110-MD-VN00-PFOP0004
13,125 CFM (STANDBY)
FILTER PLENUM (TYPE I) 110-MD-VN00-PFOP0005 NOTE4 (TYPICAL FOR 2, 2 STANDBY)
13,125 CFM (STANDBY)
FILTER PLENUM (TYPE I) 110-MD-VN00-PFOP0006
35,000 CFM
EXHAUST FAN 110-MA-VN00-FEOP0001 (TYPICAL FOR 4 3 OPERATING, 1 STANDBY)
EXHAUST FAN 110-MA-VN00-FEOP0002
EXHAUST FAN 110-MA-VN00-FEOP0003
EXHAUST FAN 110-MA-VN00-FEOP0004
B3
130-M50-VNT0-00101-000
FROM REMEDIATION FACILITY BLOCK FLOW DIAGRAM
50,000 CFM
C2
110-M50-VNT0-00101-000
FROM DTF #1 TERTIARY & SECONDARY BLOCK FLOW DIAGRAM
297,000 CFM
105,000 CFM
EXH AIR 452,000 CFM
EXHAUST AIR STACK

Note 3: Infiltration is from secondary confinement zone.
(The design was modified slightly per Input 4.6)

Source: BSC 2004b [DIRS 167666]

Figure A-1. DTF1 Primary Confinement HVAC System

INTENTIONALLY LEFT BLANK

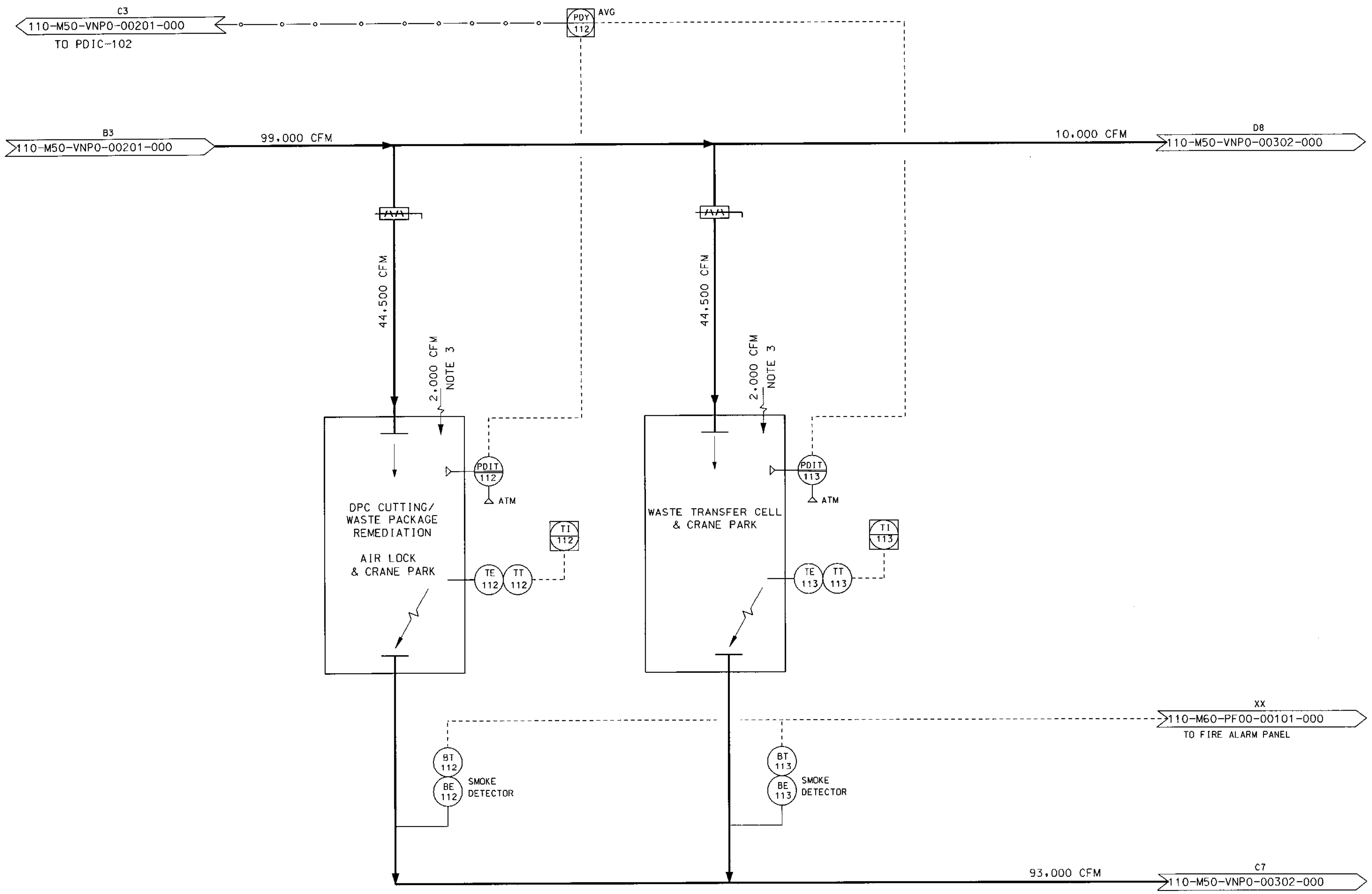


Note 3: Signal to other air handling unit controllers.
(The design was modified slightly per Input 4.6)

Source: BSC2004c [DIRS 172046]

Figure A-2. DTF1 Primary Confinement Air Handling Subsystem

INTENTIONALLY LEFT BLANK

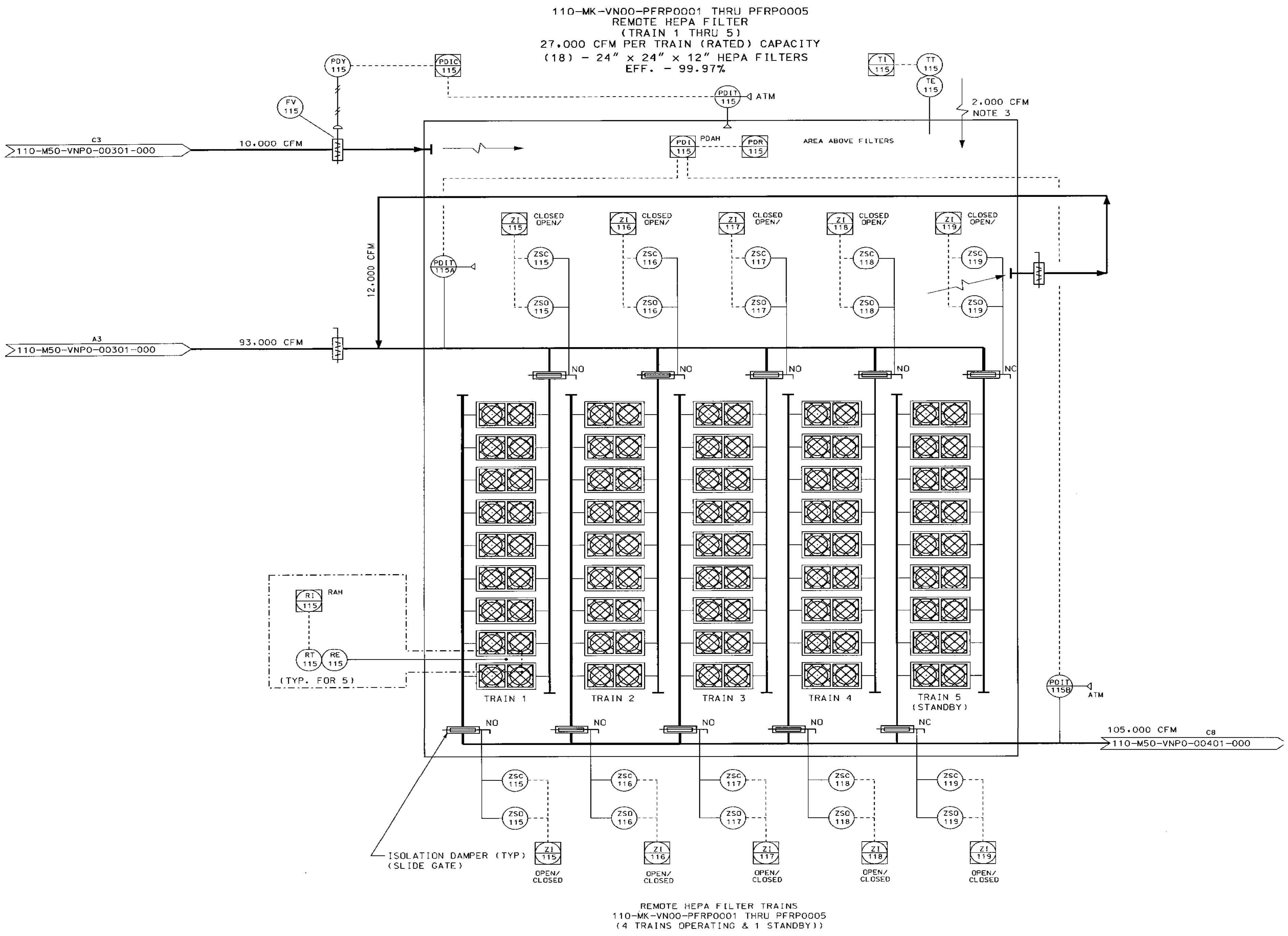


Note 3: Infiltration is from secondary confinement zone.
(The design was modified slightly per Input 4.6)

Source: BSC 2004d [DIRS 167673]

Figure A-3. DTF1 Primary Confinement Zones

INTENTIONALLY LEFT BLANK

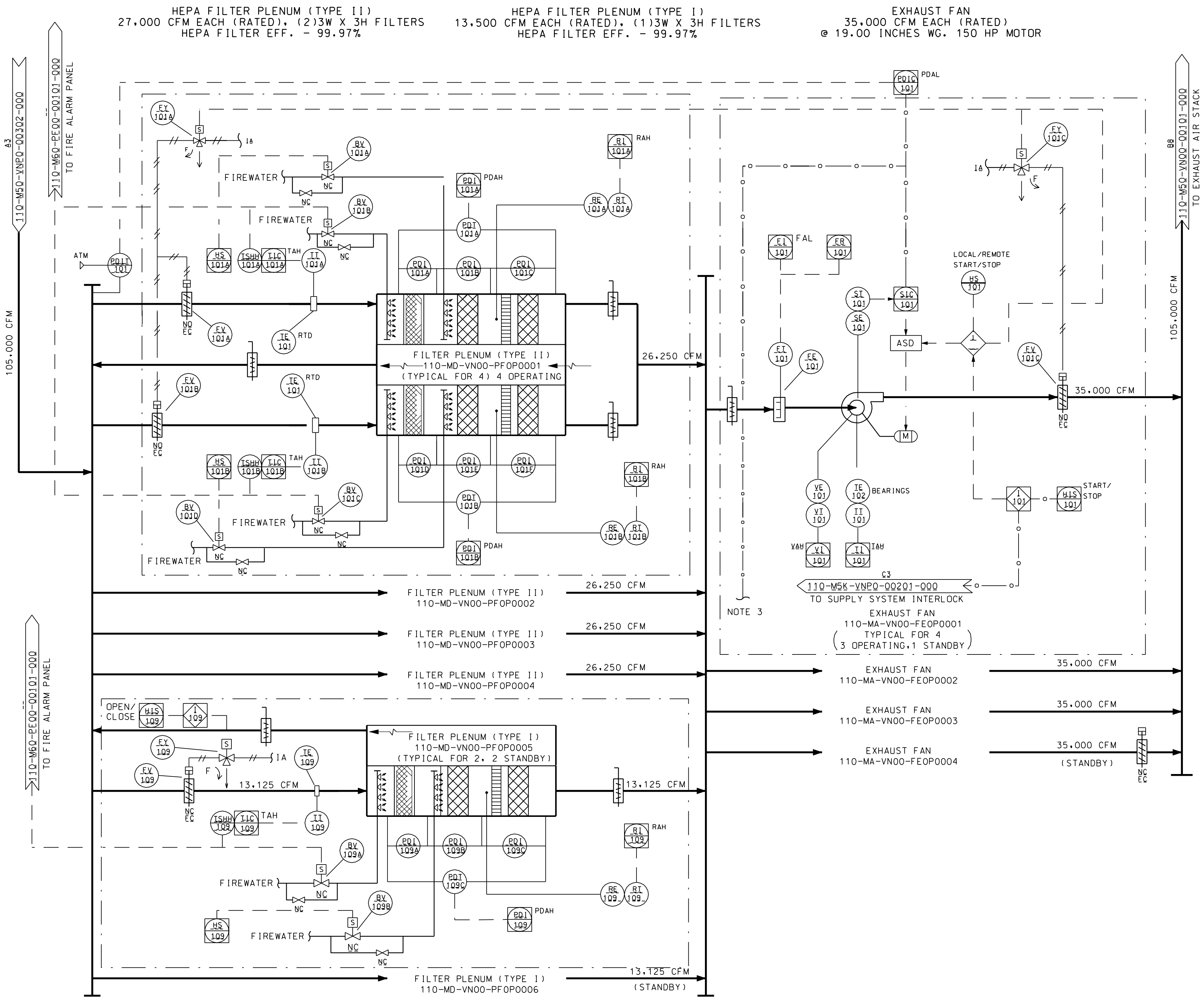


Note 3: Infiltration is from secondary confinement zone.
(The design was modified slightly per Input 4.6)

Source: BSC 2004e [DIRS 167674]

Figure A-4. DTF1 Primary Confinement HEPA Trains Subsystem

INTENTIONALLY LEFT BLANK



Note 3: Signal to other exhaust fan speed controllers.
(The design was modified slightly per Input 4.6)

Source: BSC 2004f [DIRS 171241]

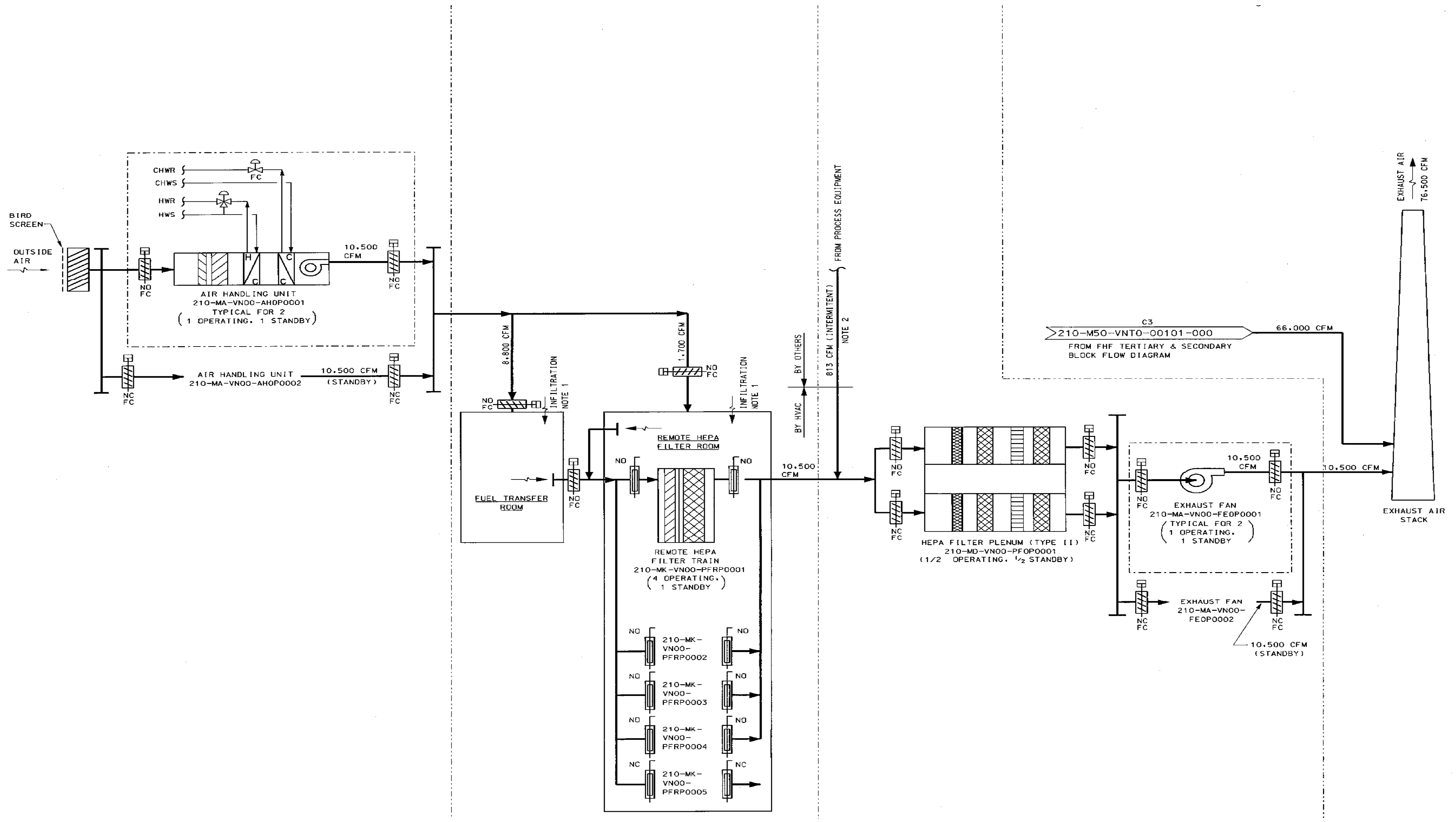
Figure A-5. DTF1 Primary Confinement HEPA Filter Plenum and Exhaust Fan Subsystem

INTENTIONALLY LEFT BLANK

ATTACHMENT B

ARCHITECTURE OF THE FHF PRIMARY CONFINEMENT NUCLEAR HVAC SYSTEM

INTENTIONALLY LEFT BLANK



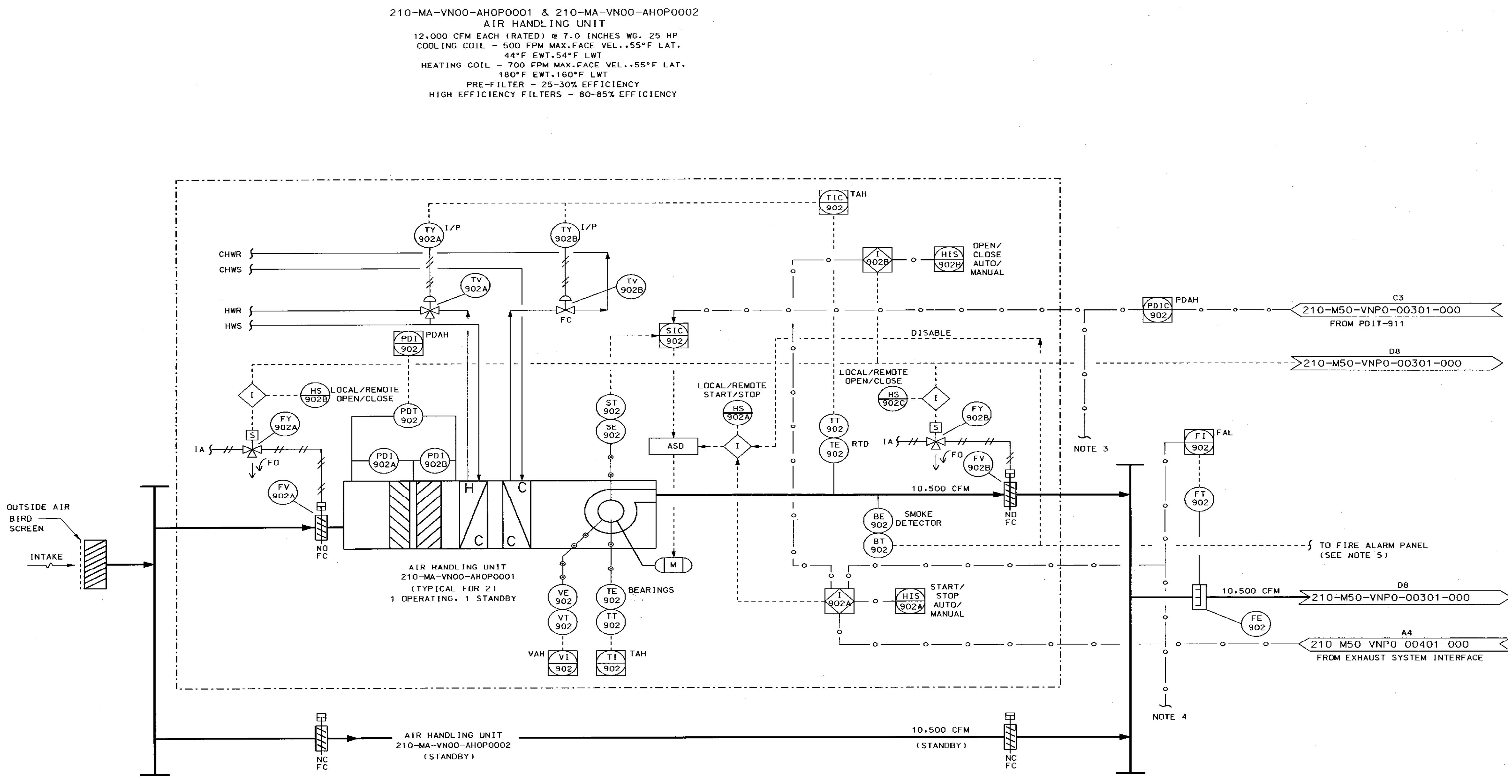
Note 1: Infiltration air flow will be determined in detail design. Supply and exhaust air flow will be adjusted accordingly.
Note 2: Exhaust from process equipment includes air flows from cask, waste package inerting systems, and gas sampling system. Process piping provided by others.

(The design was modified slightly per Input 4.6)

Source: BSC 2004g [DIRS 169225]

Figure B-1. FHF Primary Confinement HVAC System

INTENTIONALLY LEFT BLANK



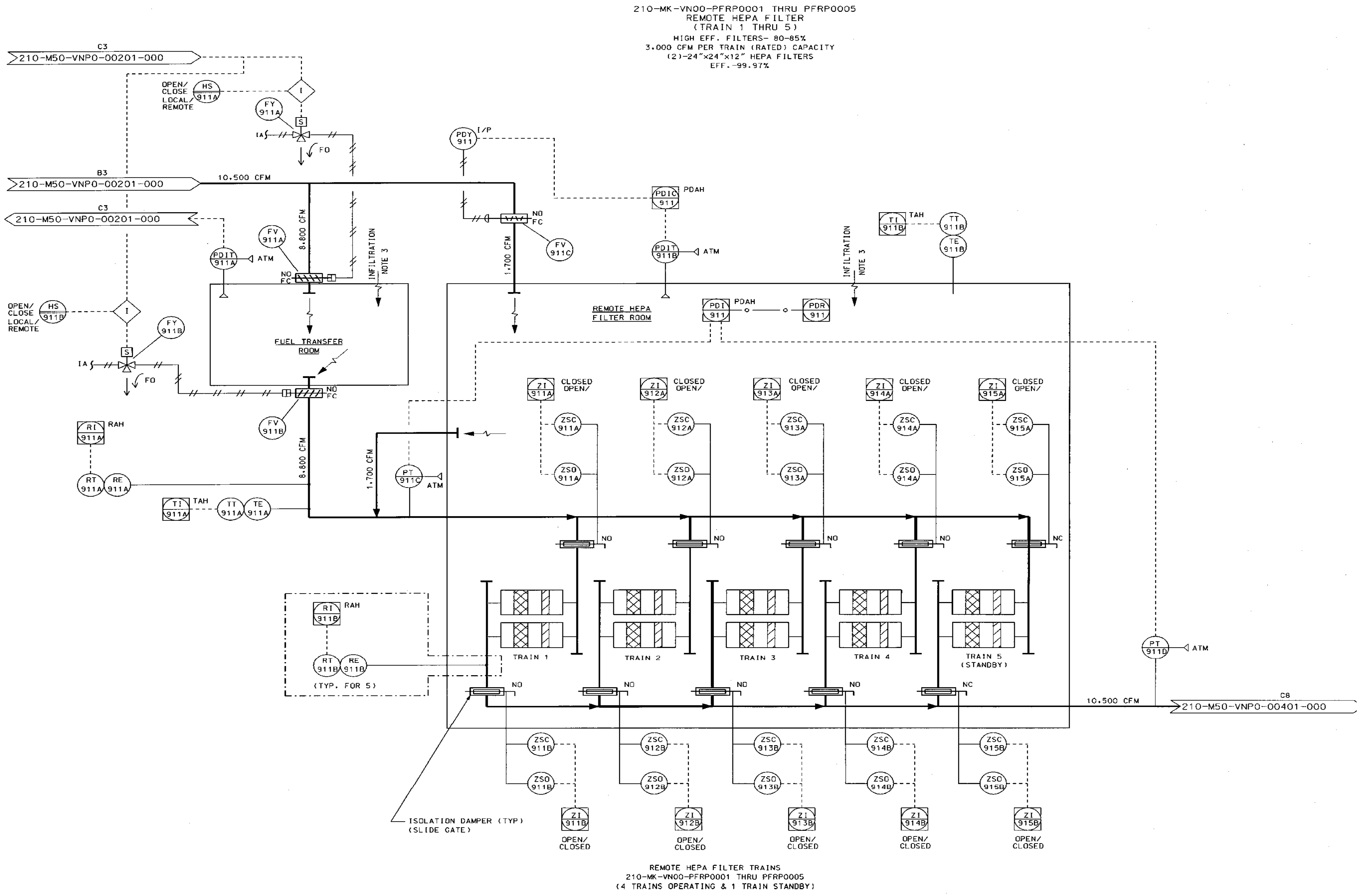
Note 3: Set point signal to standby air handling unit speed controller.
Note 4: Interface signal to standby AHU logic interlock to start
standby unit automatically upon detection of low flow.

(The design was modified slightly per Input 4.6)

Source: BSC2004h [DIRS 172047]

Figure B-2. FHF Primary Confinement Air Handling Subsystem

INTENTIONALLY LEFT BLANK



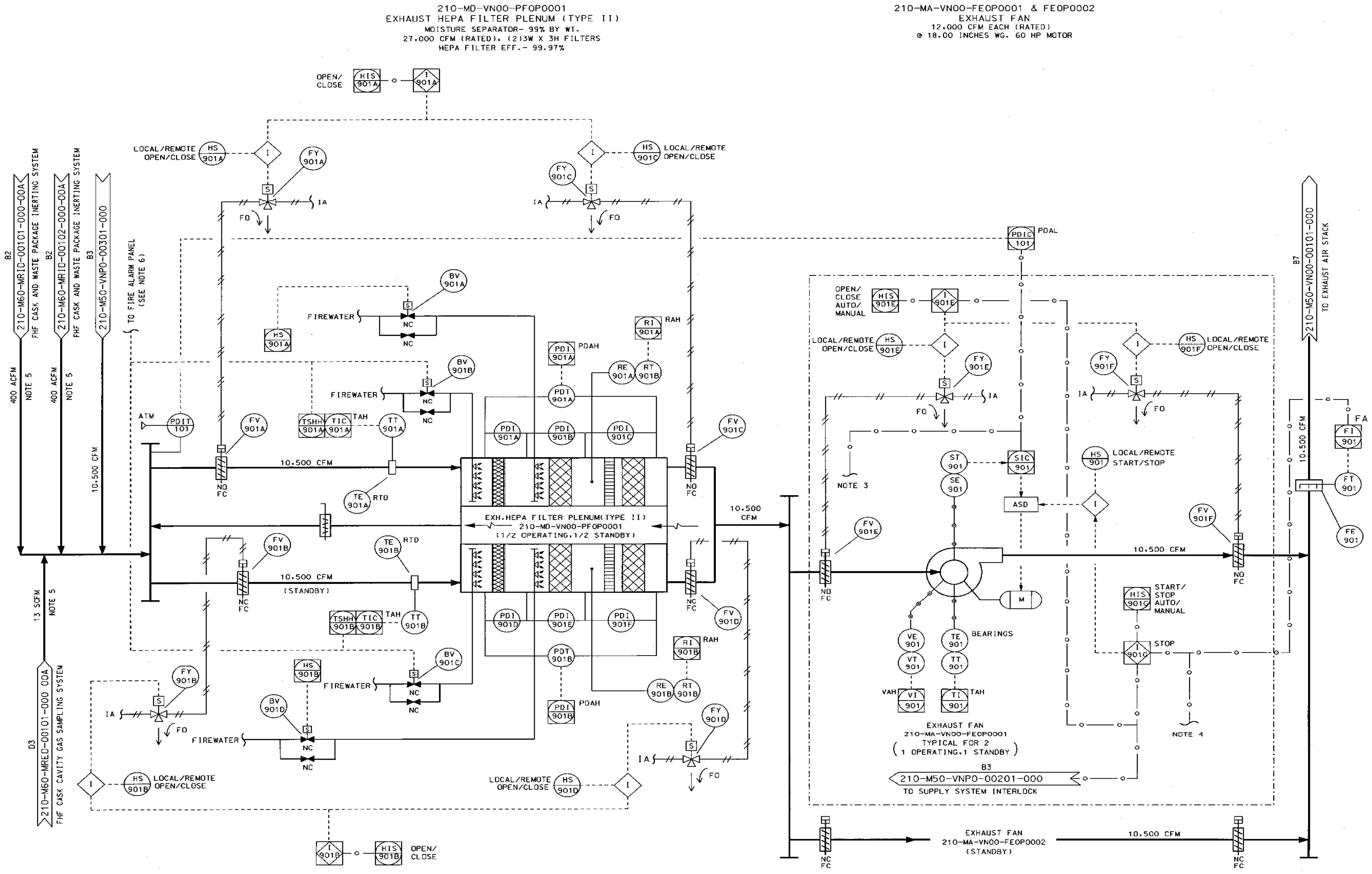
Note 3: Infiltration air flow will be determined in detail design.
Supply and exhaust air flows will be adjusted accordingly.

(The design was modified slightly per Input 4.6)

Source: BSC 2004i [DIRS 172048]

Figure B-3. FHF Primary Confinement Zone and HEPA Trains Subsystem

INTENTIONALLY LEFT BLANK



Note 3: Set point signal to other exhaust fan speed controller.
Note 4: Interface signal to standby exhaust fan logic interlock to start standby exhaust fan automatically upon detection of low flow on operating exhaust fan.
Note 5: Flow rate shown is intermittent, process piping provided by others.

(The design was modified slightly per Input 4.6)

Source: BSC 2004j [DIRS 171243]

Figure B-4. FHF Primary Confinement HEPA Filter Plenum and Exhaust Fan Subsystem

INTENTIONALLY LEFT BLANK

ATTACHMENT C

FAULT TREE MODEL FOR THE DTF 1 PRIMARY CONFINEMENT NUCLEAR HVAC SYSTEM

INTENTIONALLY LEFT BLANK

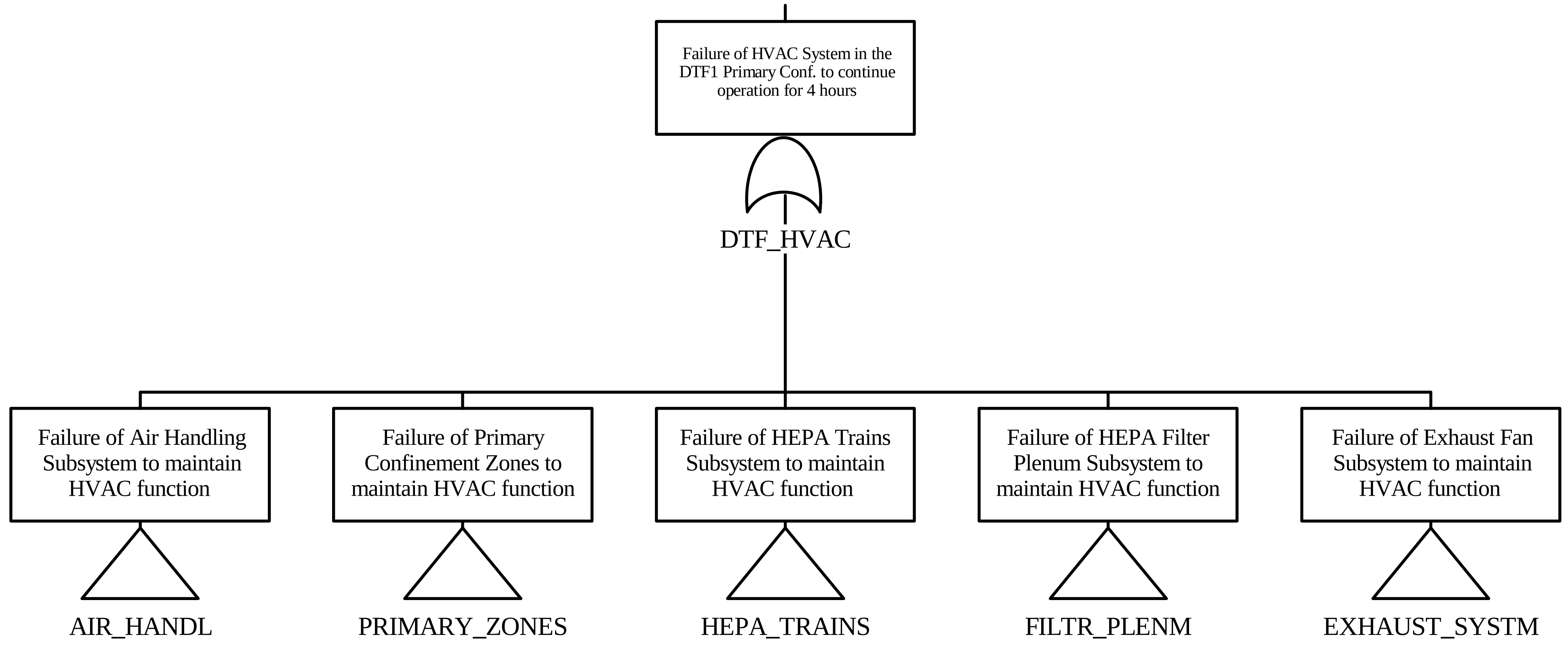

Failure of HVAC System in the DTF1 Primary Conf. to continue operation for 4 hours
DTF_HVAC
Failure of Air Handling Subsystem to maintain HVAC function
AIR_HANDL
Failure of Primary Confinement Zones to maintain HVAC function
PRIMARY_ZONES
Failure of HEPA Trains Subsystem to maintain HVAC function
HEPA_TRAINS
Failure of HEPA Filter Plenum Subsystem to maintain HVAC function
FILTR_PLENM
Failure of Exhaust Fan Subsystem to maintain HVAC function
EXHAUST_SYSTM

Figure C-1. FT Model for the DTF1 Primary Confinement HVAC System

INTENTIONALLY LEFT BLANK

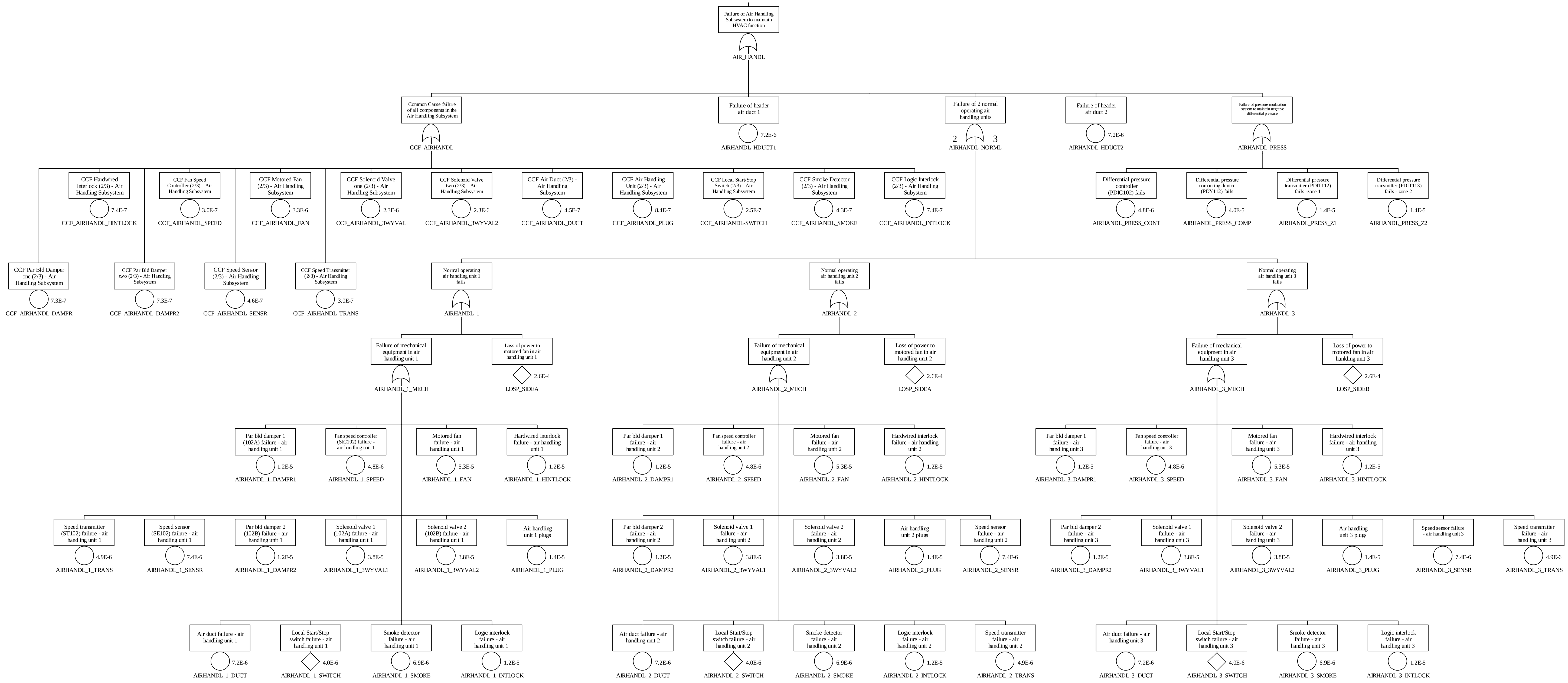

Failure of Air Handling Subsystem to maintain HVAC function
AIR_HANDL
Common Cause failure of all components in the Air Handling Subsystem
CCF_AIRHANDL
Failure of header air duct 1
7.2E-6
AIRHANDL_HDUCT1
Failure of 2 normal operating air handling units
2
3
AIRHANDL_NORML
Failure of header air duct 2
7.2E-6
AIRHANDL_HDUCT2
Failure of pressure modulation system to maintain negative differential pressure
AIRHANDL_PRESS
CCF Hardwired Interlock (2/3) - Air Handling Subsystem
7.4E-7
CCF_AIRHANDL_HINTLOCK
CCF Fan Speed Controller (2/3) - Air Handling Subsystem
3.0E-7
CCF_AIRHANDL_SPEED
CCF Motored Fan (2/3) - Air Handling Subsystem
3.3E-6
CCF_AIRHANDL_FAN
CCF Solenoid Valve one (2/3) - Air Handling Subsystem
2.3E-6
CCF_AIRHANDL_3WYVAL
CCF Solenoid Valve two (2/3) - Air Handling Subsystem
2.3E-6
CCF_AIRHANDL_3WYVAL2
CCF Air Duct (2/3) - Air Handling Subsystem
4.5E-7
CCF_AIRHANDL_DUCT
CCF Air Handling Unit (2/3) - Air Handling Subsystem
8.4E-7
CCF_AIRHANDL_PLUG
CCF Local Start/Stop Switch (2/3) - Air Handling Subsystem
2.5E-7
CCF_AIRHANDL-SWITCH
CCF Smoke Detector (2/3) - Air Handling Subsystem
4.3E-7
CCF_AIRHANDL_SMOKE
CCF Logic Interlock (2/3) - Air Handling Subsytem
7.4E-7
CCF_AIRHANDL_INTLOCK
Differential pressure controller (PDIC102) fails
4.8E-6
AIRHANDL_PRESS_CONT
Differential pressure computing device (PDY112) fails
4.0E-5
AIRHANDL_PRESS_COMP
Differential pressure transmitter (PDIT112) fails -zone 1
1.4E-5
AIRHANDL_PRESS_Z1
Differential pressure transmitter (PDIT113) fails - zone 2
1.4E-5
AIRHANDL_PRESS_Z2
CCF Par Bld Damper one (2/3) - Air Handling Subsystem
7.3E-7
CCF_AIRHANDL_DAMPR
CCF Par Bld Damper two (2/3) - Air Handling Subsystem
7.3E-7
CCF_AIRHANDL_DAMPR2
CCF Speed Sensor (2/3) - Air Handling Subsystem
4.6E-7
CCF_AIRHANDL_SENSR
CCF Speed Transmitter (2/3) - Air Handling Subsystem
3.0E-7
CCF_AIRHANDL_TRANS
Normal operating air handling unit 1 fails
AIRHANDL_1
Normal operating air handling unit 2 fails
AIRHANDL_2
Normal operating air handling unit 3 fails
AIRHANDL_3
Failure of mechanical equipment in air handling unit 1
AIRHANDL_1_MECH
Loss of power to motored fan in air handling unit 1
2.6E-4
LOSP_SIDEA
Failure of mechanical equipment in air handling unit 2
AIRHANDL_2_MECH
Loss of power to motored fan in air handling unit 2
2.6E-4
LOSP_SIDEA
Failure of mechanical equipment in air handling unit 3
AIRHANDL_3_MECH
Loss of power to motored fan in air handling unit 3
2.6E-4
LOSP_SIDEB
Par bld damper 1 (102A) failure - air handling unit 1
1.2E-5
AIRHANDL_1_DAMPR1
Fan speed controller (SIC102) failure - air handling unit 1
4.8E-6
AIRHANDL_1_SPEED
Motored fan failure - air handling unit 1
5.3E-5
AIRHANDL_1_FAN
Hardwired interlock failure - air handling unit 1
1.2E-5
AIRHANDL_1_HINTLOCK
Speed transmitter (ST102) failure - air handling unit 1
4.9E-6
AIRHANDL_1_TRANS
Speed sensor (SE102) failure - air handling unit 1
7.4E-6
AIRHANDL_1_SENSR
Par bld damper 2 (102B) failure - air handling unit 1
1.2E-5
AIRHANDL_1_DAMPR2
Solenoid valve 1 (102A) failure - air handling unit 1
3.8E-5
AIRHANDL_1_3WYVAL1
Solenoid valve 2 (102B) failure - air handling unit 1
3.8E-5
AIRHANDL_1_3WYVAL2
Air handling unit 1 plugs
1.4E-5
AIRHANDL_1_PLUG
Air duct failure - air handling unit 1
7.2E-6
AIRHANDL_1_DUCT
Local Start/Stop switch failure - air handling unit 1
4.0E-6
AIRHANDL_1_SWITCH
Smoke detector failure - air handling unit 1
6.9E-6
AIRHANDL_1_SMOKE
Logic interlock failure - air handling unit 1
1.2E-5
AIRHANDL_1_INTLOCK
Par bld damper 1 failure - air handling unit 2
1.2E-5
AIRHANDL_2_DAMPR1
Fan speed controller failure - air handling unit 2
4.8E-6
AIRHANDL_2_SPEED
Motored fan failure - air handling unit 2
5.3E-5
AIRHANDL_2_FAN
Hardwired interlock failure - air handling unit 2
1.2E-5
AIRHANDL_2_HINTLOCK
Par bld damper 2 failure - air handling unit 2
1.2E-5
AIRHANDL_2_DAMPR2
Solenoid valve 1 failure - air handling unit 2
3.8E-5
AIRHANDL_2_3WYVAL1
Solenoid valve 2 failure - air handling unit 2
3.8E-5
AIRHANDL_2_3WYVAL2
Air handling unit 2 plugs
1.4E-5
AIRHANDL_2_PLUG
Speed sensor failure - air handling unit 2
7.4E-6
AIRHANDL_2_SENSR
Air duct failure - air handling unit 2
7.2E-6
AIRHANDL_2_DUCT
Local Start/Stop switch failure - air handling unit 2
4.0E-6
AIRHANDL_2_SWITCH
Smoke detector failure - air handling unit 2
6.9E-6
AIRHANDL_2_SMOKE
Logic interlock failure - air handling unit 2
1.2E-5
AIRHANDL_2_INTLOCK
Speed transmitter failure - air handling unit 2
4.9E-6
AIRHANDL_2_TRANS
Par bld damper 1 failure - air handling unit 3
1.2E-5
AIRHANDL_3_DAMPR1
Fan speed controller failure - air handling unit 3
4.8E-6
AIRHANDL_3_SPEED
Motored fan failure - air handling unit 3
5.3E-5
AIRHANDL_3_FAN
Hardwired interlock failure - air handling unit 3
1.2E-5
AIRHANDL_3_HINTLOCK
Par bld damper 2 failure - air handling unit 3
1.2E-5
AIRHANDL_3_DAMPR2
Solenoid valve 1 failure - air handling unit 3
3.8E-5
AIRHANDL_3_3WYVAL1
Solenoid valve 2 failure - air handling unit 3
3.8E-5
AIRHANDL_3_3WYVAL2
Air handling unit 3 plugs
1.4E-5
AIRHANDL_3_PLUG
Speed sensor failure - air handling unit 3
7.4E-6
AIRHANDL_3_SENSR
Speed transmitter failure - air handling unit 3
4.9E-6
AIRHANDL_3_TRANS
Air duct failure - air handling unit 3
7.2E-6
AIRHANDL_3_DUCT
Local Start/Stop switch failure - air handling unit 3
4.0E-6
AIRHANDL_3_SWITCH
Smoke detector failure - air handling unit 3
6.9E-6
AIRHANDL_3_SMOKE
Logic interlock failure - air handling unit 3
1.2E-5
AIRHANDL_3_INTLOCK

Figure C-2. Subtree AIR_HANDL

INTENTIONALLY LEFT BLANK

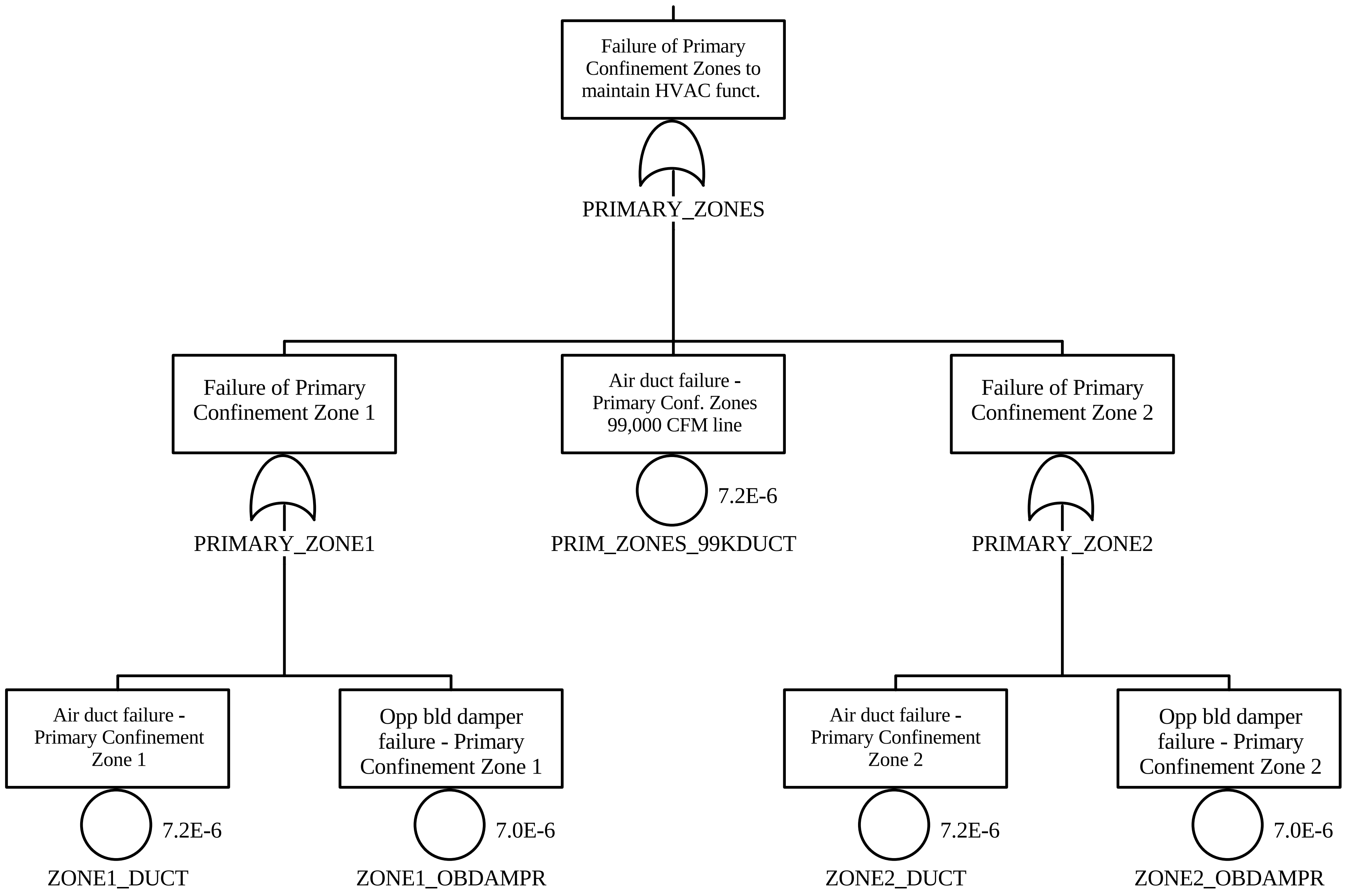

Failure of Primary Confinement Zones to maintain HVAC funct.
PRIMARY_ZONES
Failure of Primary Confinement Zone 1
PRIMARY_ZONE1
Air duct failure - Primary Conf. Zones 99,000 CFM line
7.2E-6
PRIM_ZONES_99KDUCT
Failure of Primary Confinement Zone 2
PRIMARY_ZONE2
Air duct failure - Primary Confinement Zone 1
7.2E-6
ZONE1_DUCT
Opp bld damper failure - Primary Confinement Zone 1
7.0E-6
ZONE1_OBDAMPR
Air duct failure - Primary Confinement Zone 2
7.2E-6
ZONE2_DUCT
Opp bld damper failure - Primary Confinement Zone 2
7.0E-6
ZONE2_OBDAMPR

Figure C-3. Subtree PRIMARY_ZONES

INTENTIONALLY LEFT BLANK

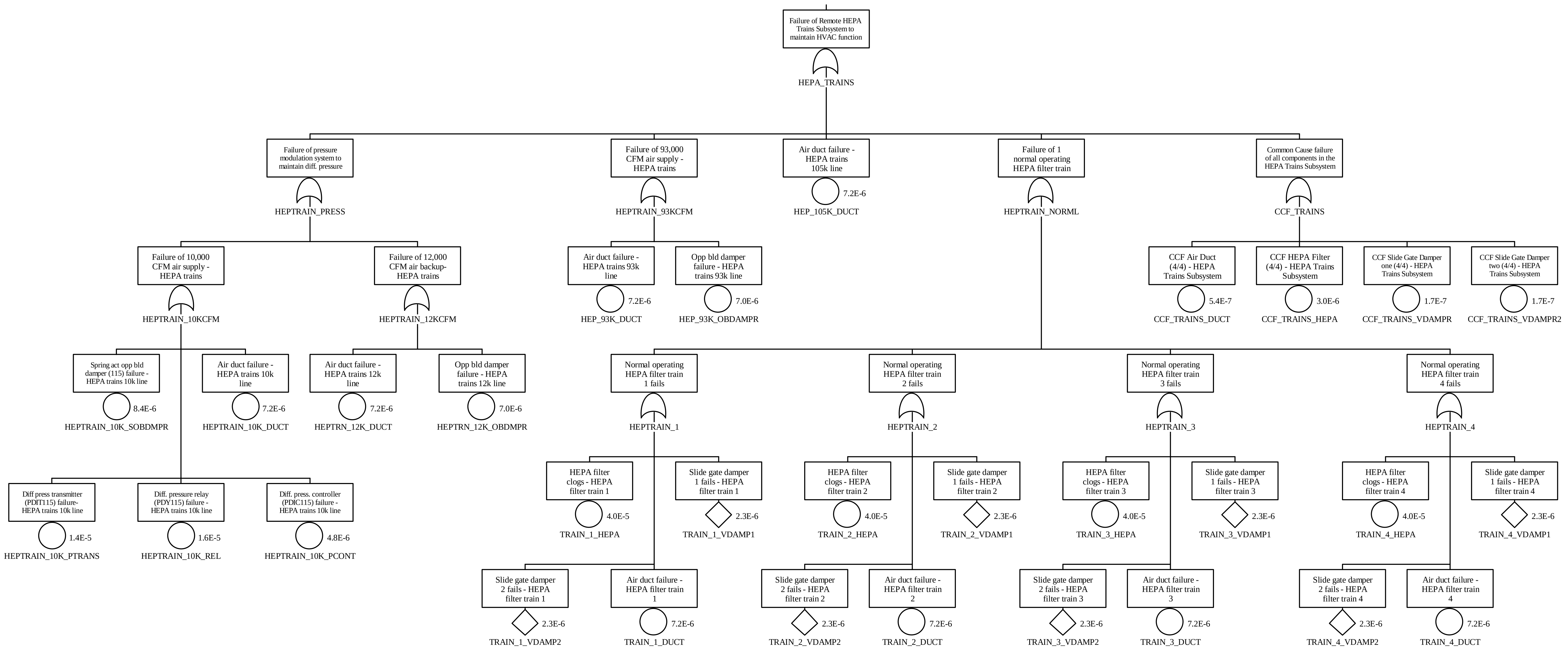

Failure of Remote HEPA Trains Subsystem to maintain HVAC function
HEPA_TRAINS
Failure of pressure modulation system to maintain diff. pressure
HEPTRAIN_PRESS
Failure of 93,000 CFM air supply - HEPA trains
HEPTRAIN_93KCFM
Air duct failure - HEPA trains 105k line
7.2E-6
HEP_105K_DUCT
Failure of 1 normal operating HEPA filter train
HEPTRAIN_NORML
Common Cause failure of all components in the HEPA Trains Subsystem
CCF_TRAINS
Failure of 10,000 CFM air supply - HEPA trains
HEPTRAIN_10KCFM
Failure of 12,000 CFM air backup- HEPA trains
HEPTRAIN_12KCFM
Air duct failure - HEPA trains 93k line
7.2E-6
HEP_93K_DUCT
Opp bld damper failure - HEPA trains 93k line
7.0E-6
HEP_93K_OBDAMPR
CCF Air Duct (4/4) - HEPA Trains Subsystem
5.4E-7
CCF_TRAINS_DUCT
CCF HEPA Filter (4/4) - HEPA Trains Subsystem
3.0E-6
CCF_TRAINS_HEPA
CCF Slide Gate Damper one (4/4) - HEPA Trains Subsystem
1.7E-7
CCF_TRAINS_VDAMPR
CCF Slide Gate Damper two (4/4) - HEPA Trains Subsystem
1.7E-7
CCF_TRAINS_VDAMPR2
Spring act opp bld damper (115) failure - HEPA trains 10k line
8.4E-6
HEPTRAIN_10K_SOBDMPR
Air duct failure - HEPA trains 10k line
7.2E-6
HEPTRAIN_10K_DUCT
Air duct failure - HEPA trains 12k line
7.2E-6
HEPTRN_12K_DUCT
Opp bld damper failure - HEPA trains 12k line
7.0E-6
HEPTRN_12K_OBDMPR
Normal operating HEPA filter train 1 fails
HEPTRAIN_1
Normal operating HEPA filter train 2 fails
HEPTRAIN_2
Normal operating HEPA filter train 3 fails
HEPTRAIN_3
Normal operating HEPA filter train 4 fails
HEPTRAIN_4
HEPA filter clogs - HEPA filter train 1
4.0E-5
TRAIN_1_HEPA
Slide gate damper 1 fails - HEPA filter train 1
2.3E-6
TRAIN_1_VDAMP1
HEPA filter clogs - HEPA filter train 2
4.0E-5
TRAIN_2_HEPA
Slide gate damper 1 fails - HEPA filter train 2
2.3E-6
TRAIN_2_VDAMP1
HEPA filter clogs - HEPA filter train 3
4.0E-5
TRAIN_3_HEPA
Slide gate damper 1 fails - HEPA filter train 3
2.3E-6
TRAIN_3_VDAMP1
HEPA filter clogs - HEPA filter train 4
4.0E-5
TRAIN_4_HEPA
Slide gate damper 1 fails - HEPA filter train 4
2.3E-6
TRAIN_4_VDAMP1
Diff press transmitter (PDIT115) failure- HEPA trains 10k line
1.4E-5
HEPTRAIN_10K_PTRANS
Diff. pressure relay (PDY115) failure - HEPA trains 10k line
1.6E-5
HEPTRAIN_10K_REL
Diff. press. controller (PDIC115) failure - HEPA trains 10k line
4.8E-6
HEPTRAIN_10K_PCONT
Slide gate damper 2 fails - HEPA filter train 1
2.3E-6
TRAIN_1_VDAMP2
Air duct failure - HEPA filter train 1
7.2E-6
TRAIN_1_DUCT
Slide gate damper 2 fails - HEPA filter train 2
2.3E-6
TRAIN_2_VDAMP2
Air duct failure - HEPA filter train 2
7.2E-6
TRAIN_2_DUCT
Slide gate damper 2 fails - HEPA filter train 3
2.3E-6
TRAIN_3_VDAMP2
Air duct failure - HEPA filter train 3
7.2E-6
TRAIN_3_DUCT
Slide gate damper 2 fails - HEPA filter train 4
2.3E-6
TRAIN_4_VDAMP2
Air duct failure - HEPA filter train 4
7.2E-6
TRAIN_4_DUCT

Figure C-4. Subtree HEPA_TRAINS

INTENTIONALLY LEFT BLANK

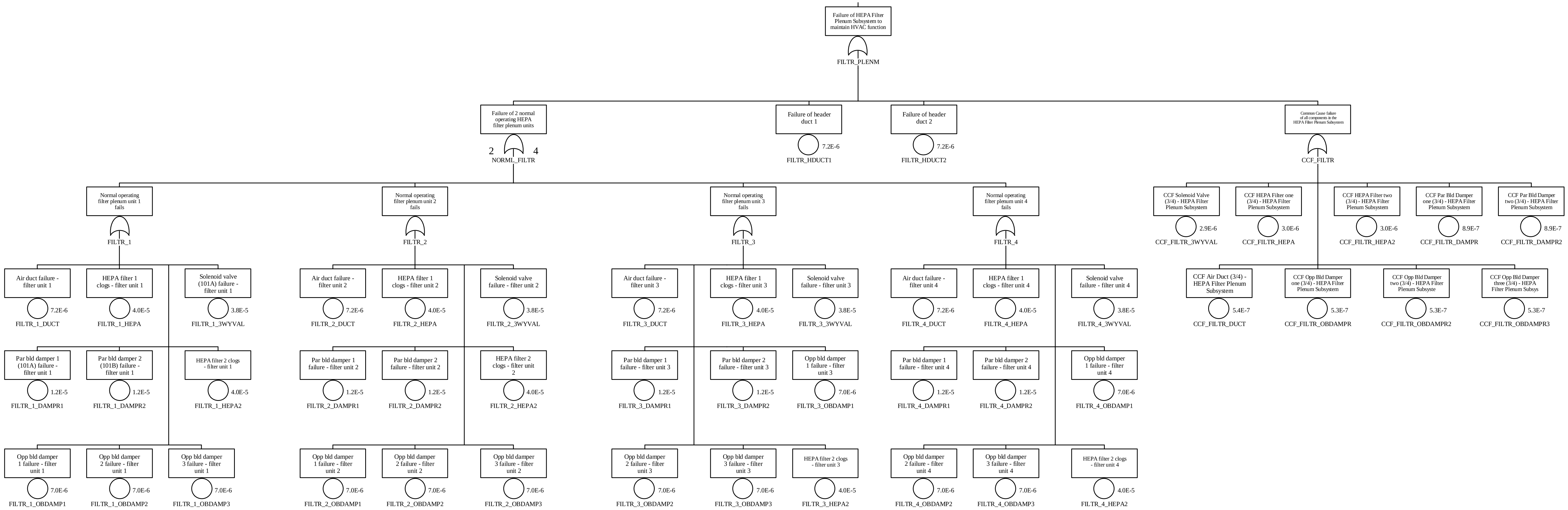

Failure of HEPA Filter Plenum Subsystem to maintain HVAC function
FILTR_PLENM
Failure of 2 normal operating HEPA filter plenum units
2
4
NORML_FILTR
Failure of header duct 1
7.2E-6
FILTR_HDUCT1
Failure of header duct 2
7.2E-6
FILTR_HDUCT2
Common Cause failure of all components in the HEPA Filter Plenum Subsystem
CCF_FILTR
Normal operating filter plenum unit 1 fails
FILTR_1
Normal operating filter plenum unit 2 fails
FILTR_2
Normal operating filter plenum unit 3 fails
FILTR_3
Normal operating filter plenum unit 4 fails
FILTR_4
CCF Solenoid Valve (3/4) - HEPA Filter Plenum Subsystem
2.9E-6
CCF_FILTR_3WYVAL
CCF HEPA Filter one (3/4) - HEPA Filter Plenum Subsystem
3.0E-6
CCF_FILTR_HEPA
CCF HEPA Filter two (3/4) - HEPA Filter Plenum Subsystem
3.0E-6
CCF_FILTR_HEPA2
CCF Par Bld Damper one (3/4) - HEPA Filter Plenum Subsystem
8.9E-7
CCF_FILTR_DAMPR
CCF Par Bld Damper two (3/4) - HEPA Filter Plenum Subsystem
8.9E-7
CCF_FILTR_DAMPR2
CCF Air Duct (3/4) - HEPA Filter Plenum Subsystem
5.4E-7
CCF_FILTR_DUCT
CCF Opp Bld Damper one (3/4) - HEPA Filter Plenum Subsystem
5.3E-7
CCF_FILTR_OBDAMPR
CCF Opp Bld Damper two (3/4) - HEPA Filter Plenum Subsyste
5.3E-7
CCF_FILTR_OBDAMPR2
CCF Opp Bld Damper three (3/4) - HEPA Filter Plenum Subsys
5.3E-7
CCF_FILTR_OBDAMPR3
Air duct failure - filter unit 1
7.2E-6
FILTR_1_DUCT
HEPA filter 1 clogs - filter unit 1
4.0E-5
FILTR_1_HEPA
Solenoid valve (101A) failure - filter unit 1
3.8E-5
FILTR_1_3WYVAL
Par bld damper 1 (101A) failure - filter unit 1
1.2E-5
FILTR_1_DAMPR1
Par bld damper 2 (101B) failure - filter unit 1
1.2E-5
FILTR_1_DAMPR2
HEPA filter 2 clogs - filter unit 1
4.0E-5
FILTR_1_HEPA2
Opp bld damper 1 failure - filter unit 1
7.0E-6
FILTR_1_OBDAMP1
Opp bld damper 2 failure - filter unit 1
7.0E-6
FILTR_1_OBDAMP2
Opp bld damper 3 failure - filter unit 1
7.0E-6
FILTR_1_OBDAMP3
Air duct failure - filter unit 2
7.2E-6
FILTR_2_DUCT
HEPA filter 1 clogs - filter unit 2
4.0E-5
FILTR_2_HEPA
Solenoid valve failure - filter unit 2
3.8E-5
FILTR_2_3WYVAL
Par bld damper 1 failure - filter unit 2
1.2E-5
FILTR_2_DAMPR1
Par bld damper 2 failure - filter unit 2
1.2E-5
FILTR_2_DAMPR2
HEPA filter 2 clogs - filter unit 2
4.0E-5
FILTR_2_HEPA2
Opp bld damper 1 failure - filter unit 2
7.0E-6
FILTR_2_OBDAMP1
Opp bld damper 2 failure - filter unit 2
7.0E-6
FILTR_2_OBDAMP2
Opp bld damper 3 failure - filter unit 2
7.0E-6
FILTR_2_OBDAMP3
Air duct failure - filter unit 3
7.2E-6
FILTR_3_DUCT
HEPA filter 1 clogs - filter unit 3
4.0E-5
FILTR_3_HEPA
Solenoid valve failure - filter unit 3
3.8E-5
FILTR_3_3WYVAL
Par bld damper 1 failure - filter unit 3
1.2E-5
FILTR_3_DAMPR1
Par bld damper 2 failure - filter unit 3
1.2E-5
FILTR_3_DAMPR2
Opp bld damper 1 failure - filter unit 3
7.0E-6
FILTR_3_OBDAMP1
Opp bld damper 2 failure - filter unit 3
7.0E-6
FILTR_3_OBDAMP2
Opp bld damper 3 failure - filter unit 3
7.0E-6
FILTR_3_OBDAMP3
HEPA filter 2 clogs - filter unit 3
4.0E-5
FILTR_3_HEPA2
Air duct failure - filter unit 4
7.2E-6
FILTR_4_DUCT
HEPA filter 1 clogs - filter unit 4
4.0E-5
FILTR_4_HEPA
Solenoid valve failure - filter unit 4
3.8E-5
FILTR_4_3WYVAL
Par bld damper 1 failure - filter unit 4
1.2E-5
FILTR_4_DAMPR1
Par bld damper 2 failure - filter unit 4
1.2E-5
FILTR_4_DAMPR2
Opp bld damper 1 failure - filter unit 4
7.0E-6
FILTR_4_OBDAMP1
Opp bld damper 2 failure - filter unit 4
7.0E-6
FILTR_4_OBDAMP2
Opp bld damper 3 failure - filter unit 4
7.0E-6
FILTR_4_OBDAMP3
HEPA filter 2 clogs - filter unit 4
4.0E-5
FILTR_4_HEPA2

Figure C-5. Subtree FILTR_PLENM

INTENTIONALLY LEFT BLANK

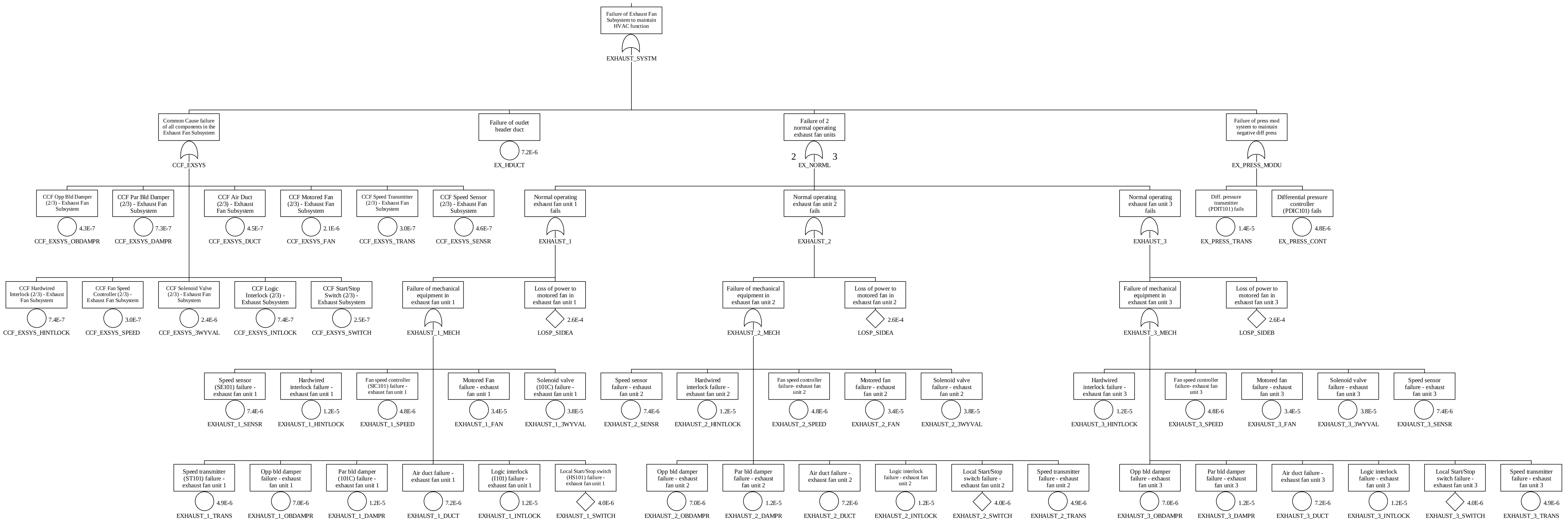

Failure of Exhaust Fan Subsystem to maintain HVAC function
EXHAUST_SYSTM
Common Cause failure of all components in the Exhaust Fan Subsystem
CCF_EXSYS
Failure of outlet header duct
7.2E-6
EX_HDUCT
Failure of 2 normal operating exhaust fan units
2
3
EX_NORML
Failure of press mod system to maintain negative diff press
EX_PRESS_MODU
CCF Opp Bld Damper (2/3) - Exhaust Fan Subsystem
4.3E-7
CCF_EXSYS_OBDAMPR
CCF Par Bld Damper (2/3) - Exhaust Fan Subsystem
7.3E-7
CCF_EXSYS_DAMPR
CCF Air Duct (2/3) - Exhaust Fan Subsystem
4.5E-7
CCF_EXSYS_DUCT
CCF Motored Fan (2/3) - Exhaust Fan Subsystem
2.1E-6
CCF_EXSYS_FAN
CCF Speed Transmitter (2/3) - Exhaust Fan Subsystem
3.0E-7
CCF_EXSYS_TRANS
CCF Speed Sensor (2/3) - Exhaust Fan Subsystem
4.6E-7
CCF_EXSYS_SENSR
CCF Hardwired Interlock (2/3) - Exhaust Fan Subsystem
7.4E-7
CCF_EXSYS_HINTLOCK
CCF Fan Speed Controller (2/3) - Exhaust Fan Subsystem
3.0E-7
CCF_EXSYS_SPEED
CCF Solenoid Valve (2/3) - Exhaust Fan Subsystem
2.4E-6
CCF_EXSYS_3WYVAL
CCF Logic Interlock (2/3) - Exhaust Subsystem
7.4E-7
CCF_EXSYS_INTLOCK
CCF Start/Stop Switch (2/3) - Exhaust Subsystem
2.5E-7
CCF_EXSYS_SWITCH
Normal operating exhaust fan unit 1 fails
EXHAUST_1
Normal operating exhaust fan unit 2 fails
EXHAUST_2
Normal operating exhaust fan unit 3 fails
EXHAUST_3
Diff. pressure transmitter (PDIT101) fails
1.4E-5
EX_PRESS_TRANS
Differential pressure controller (PDIC101) fails
4.8E-6
EX_PRESS_CONT
Failure of mechanical equipment in exhaust fan unit 1
EXHAUST_1_MECH
Loss of power to motored fan in exhaust fan unit 1
2.6E-4
LOSP_SIDEA
Failure of mechanical equipment in exhaust fan unit 2
EXHAUST_2_MECH
Loss of power to motored fan in exhaust fan unit 2
2.6E-4
LOSP_SIDEA
Failure of mechanical equipment in exhaust fan unit 3
EXHAUST_3_MECH
Loss of power to motored fan in exhaust fan unit 3
2.6E-4
LOSP_SIDEB
Speed sensor (SE101) failure - exhaust fan unit 1
7.4E-6
EXHAUST_1_SENSR
Hardwired interlock failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_HINTLOCK
Fan speed controller (SIC101) failure - exhaust fan unit 1
4.8E-6
EXHAUST_1_SPEED
Motored Fan failure - exhaust fan unit 1
3.4E-5
EXHAUST_1_FAN
Solenoid valve (101C) failure - exhaust fan unit 1
3.8E-5
EXHAUST_1_3WYVAL
Speed sensor failure - exhaust fan unit 2
7.4E-6
EXHAUST_2_SENSR
Hardwired interlock failure - exhaust fan unit 2
1.2E-5
EXHAUST_2_HINTLOCK
Fan speed controller failure- exhaust fan unit 2
4.8E-6
EXHAUST_2_SPEED
Motored fan failure - exhaust fan unit 2
3.4E-5
EXHAUST_2_FAN
Solenoid valve failure - exhaust fan unit 2
3.8E-5
EXHAUST_2_3WYVAL
Hardwired interlock failure - exhaust fan unit 3
1.2E-5
EXHAUST_3_HINTLOCK
Fan speed controller failure- exhaust fan unit 3
4.8E-6
EXHAUST_3_SPEED
Motored fan failure - exhaust fan unit 3
3.4E-5
EXHAUST_3_FAN
Solenoid valve failure - exhaust fan unit 3
3.8E-5
EXHAUST_3_3WYVAL
Speed sensor failure - exhaust fan unit 3
7.4E-6
EXHAUST_3_SENSR
Speed transmitter (ST101) failure - exhaust fan unit 1
4.9E-6
EXHAUST_1_TRANS
Opp bld damper failure - exhaust fan unit 1
7.0E-6
EXHAUST_1_OBDAMPR
Par bld damper (101C) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_DAMPR
Air duct failure - exhaust fan unit 1
7.2E-6
EXHAUST_1_DUCT
Logic interlock (I101) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_INTLOCK
Local Start/Stop switch (HS101) failure - exhaust fan unit 1
4.0E-6
EXHAUST_1_SWITCH
Opp bld damper failure - exhaust fan unit 2
7.0E-6
EXHAUST_2_OBDAMPR
Par bld damper failure - exhaust fan unit 2
1.2E-5
EXHAUST_2_DAMPR
Air duct failure - exhaust fan unit 2
7.2E-6
EXHAUST_2_DUCT
Logic interlock failure - exhaust fan unit 2
1.2E-5
EXHAUST_2_INTLOCK
Local Start/Stop switch failure - exhaust fan unit 2
4.0E-6
EXHAUST_2_SWITCH
Speed transmitter failure - exhaust fan unit 2
4.9E-6
EXHAUST_2_TRANS
Opp bld damper failure - exhaust fan unit 3
7.0E-6
EXHAUST_3_OBDAMPR
Par bld damper failure - exhaust fan unit 3
1.2E-5
EXHAUST_3_DAMPR
Air duct failure - exhaust fan unit 3
7.2E-6
EXHAUST_3_DUCT
Logic interlock failure - exhaust fan unit 3
1.2E-5
EXHAUST_3_INTLOCK
Local Start/Stop switch failure - exhaust fan unit 3
4.0E-6
EXHAUST_3_SWITCH
Speed transmitter failure - exhaust fan unit 3
4.9E-6
EXHAUST_3_TRANS

Figure C-6. Subtree EXHAUST_SYSTM

INTENTIONALLY LEFT BLANK

ATTACHMENT D

FAULT TREE MODEL FOR THE FHF PRIMARY CONFINEMENT NUCLEAR HVAC SYSTEM

INTENTIONALLY LEFT BLANK

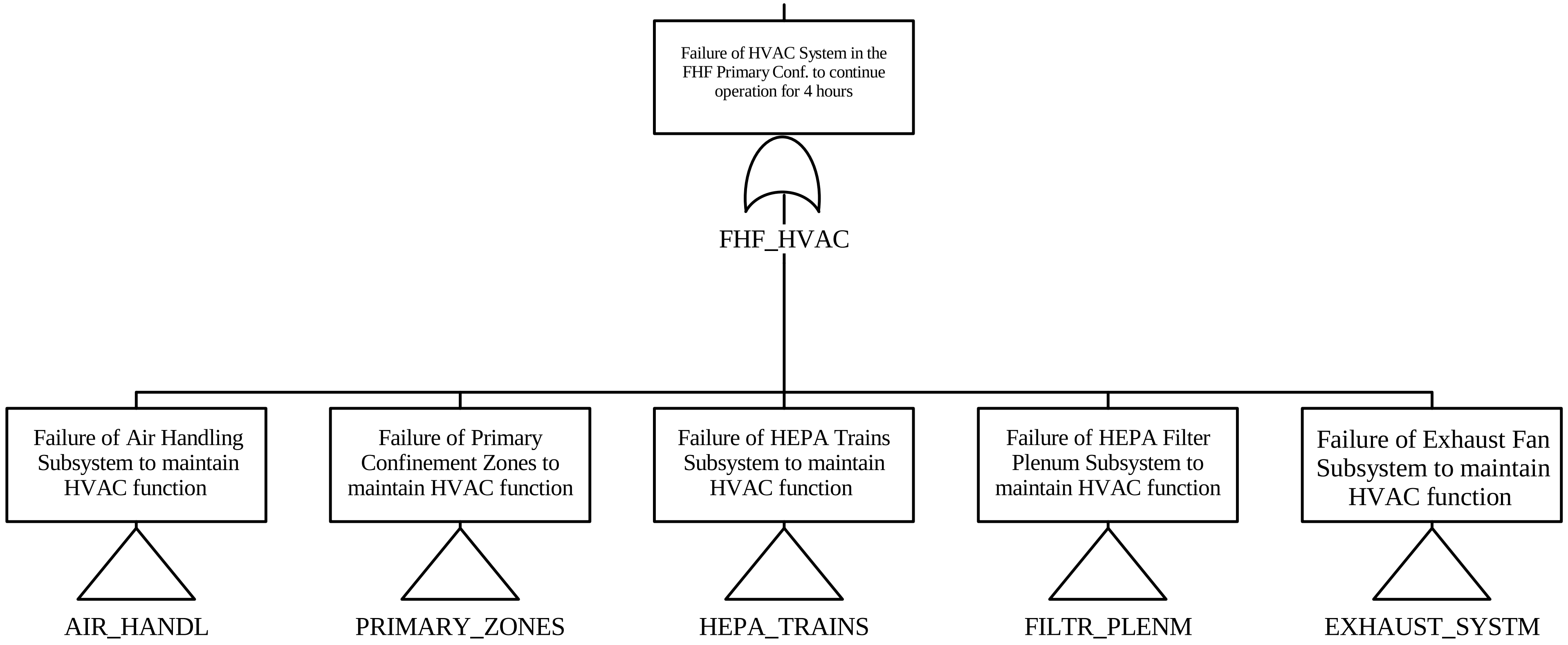

Failure of HVAC System in the FHF Primary Conf. to continue operation for 4 hours
FHF_HVAC
Failure of Air Handling Subsystem to maintain HVAC function
AIR_HANDL
Failure of Primary Confinement Zones to maintain HVAC function
PRIMARY_ZONES
Failure of HEPA Trains Subsystem to maintain HVAC function
HEPA_TRAINS
Failure of HEPA Filter Plenum Subsystem to maintain HVAC function
FILTR_PLENM
Failure of Exhaust Fan Subsystem to maintain HVAC function
EXHAUST_SYSTM

Figure D-1. FT Model for the FHF Primary Confinement HVAC System

INTENTIONALLY LEFT BLANK

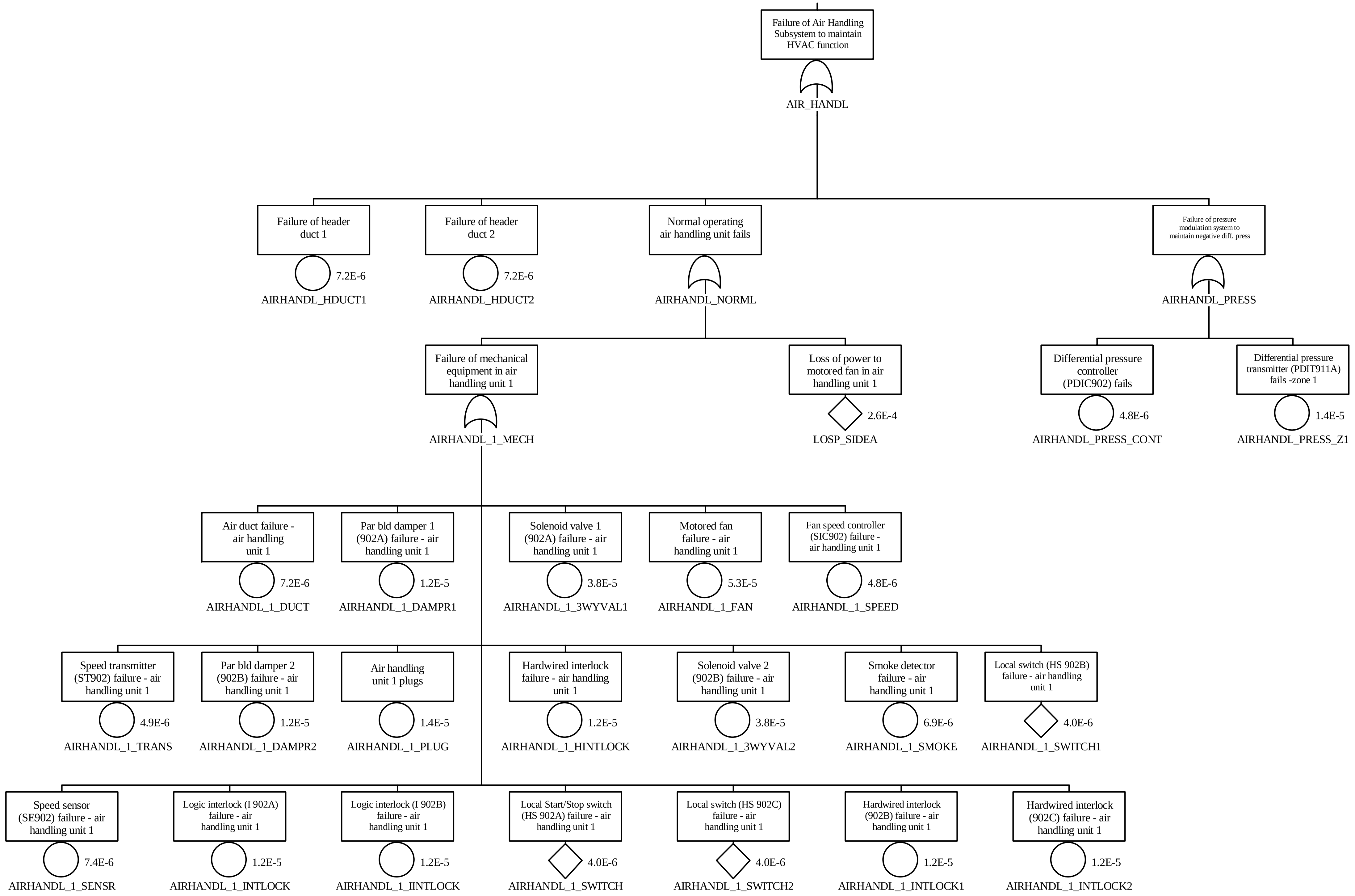

Failure of Air Handling Subsystem to maintain HVAC function
AIR_HANDL
Failure of header duct 1
7.2E-6
AIRHANDL_HDUCT1
Failure of header duct 2
7.2E-6
AIRHANDL_HDUCT2
Normal operating air handling unit fails
AIRHANDL_NORML
Failure of pressure modulation system to maintain negative diff. press
AIRHANDL_PRESS
Failure of mechanical equipment in air handling unit 1
AIRHANDL_1_MECH
Loss of power to motored fan in air handling unit 1
2.6E-4
LOSP_SIDEA
Differential pressure controller (PDIC902) fails
4.8E-6
AIRHANDL_PRESS_CONT
Differential pressure transmitter (PDIT911A) fails -zone 1
1.4E-5
AIRHANDL_PRESS_Z1
Air duct failure - air handling unit 1
7.2E-6
AIRHANDL_1_DUCT
Par bld damper 1 (902A) failure - air handling unit 1
1.2E-5
AIRHANDL_1_DAMPR1
Solenoid valve 1 (902A) failure - air handling unit 1
3.8E-5
AIRHANDL_1_3WYVAL1
Motored fan failure - air handling unit 1
5.3E-5
AIRHANDL_1_FAN
Fan speed controller (SIC902) failure - air handling unit 1
4.8E-6
AIRHANDL_1_SPEED
Speed transmitter (ST902) failure - air handling unit 1
4.9E-6
AIRHANDL_1_TRANS
Par bld damper 2 (902B) failure - air handling unit 1
1.2E-5
AIRHANDL_1_DAMPR2
Air handling unit 1 plugs
1.4E-5
AIRHANDL_1_PLUG
Hardwired interlock failure - air handling unit 1
1.2E-5
AIRHANDL_1_HINTLOCK
Solenoid valve 2 (902B) failure - air handling unit 1
3.8E-5
AIRHANDL_1_3WYVAL2
Smoke detector failure - air handling unit 1
6.9E-6
AIRHANDL_1_SMOKE
Local switch (HS 902B) failure - air handling unit 1
4.0E-6
AIRHANDL_1_SWITCH1
Speed sensor (SE902) failure - air handling unit 1
7.4E-6
AIRHANDL_1_SENSR
Logic interlock (I 902A) failure - air handling unit 1
1.2E-5
AIRHANDL_1_INTLOCK
Logic interlock (I 902B) failure - air handling unit 1
1.2E-5
AIRHANDL_1_IINTLOCK
Local Start/Stop switch (HS 902A) failure - air handling unit 1
4.0E-6
AIRHANDL_1_SWITCH
Local switch (HS 902C) failure - air handling unit 1
4.0E-6
AIRHANDL_1_SWITCH2
Hardwired interlock (902B) failure - air handling unit 1
1.2E-5
AIRHANDL_1_INTLOCK1
Hardwired interlock (902C) failure - air handling unit 1
1.2E-5
AIRHANDL_1_INTLOCK2

Figure D-2. Subtree AIR_HANDL

INTENTIONALLY LEFT BLANK

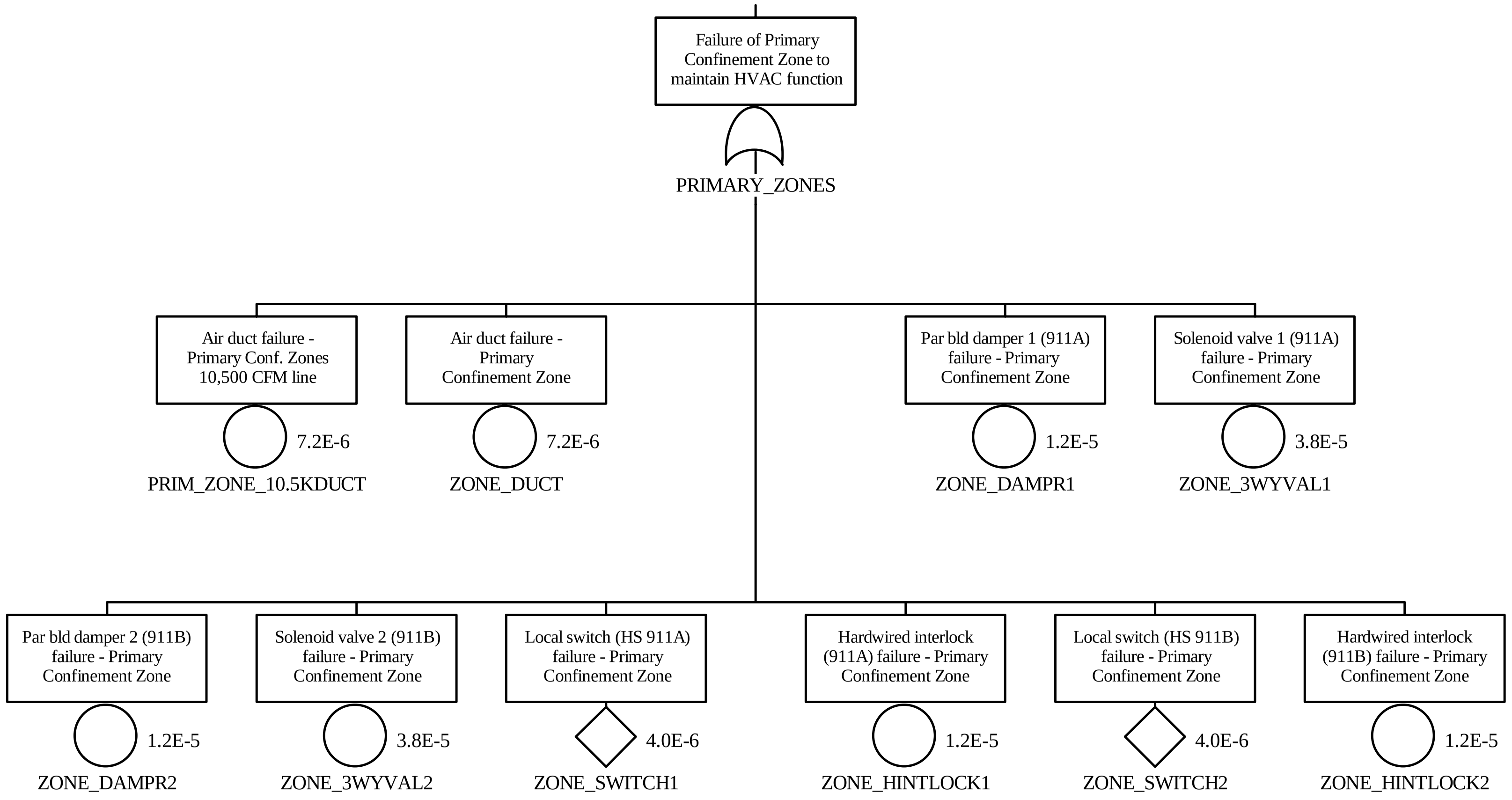

Failure of Primary Confinement Zone to maintain HVAC function
PRIMARY_ZONES
Air duct failure - Primary Conf. Zones 10,500 CFM line
7.2E-6
PRIM_ZONE_10.5KDUCT
Air duct failure - Primary Confinement Zone
7.2E-6
ZONE_DUCT
Par bld damper 1 (911A) failure - Primary Confinement Zone
1.2E-5
ZONE_DAMPR1
Solenoid valve 1 (911A) failure - Primary Confinement Zone
3.8E-5
ZONE_3WYVAL1
Par bld damper 2 (911B) failure - Primary Confinement Zone
1.2E-5
ZONE_DAMPR2
Solenoid valve 2 (911B) failure - Primary Confinement Zone
3.8E-5
ZONE_3WYVAL2
Local switch (HS 911A) failure - Primary Confinement Zone
4.0E-6
ZONE_SWITCH1
Hardwired interlock (911A) failure - Primary Confinement Zone
1.2E-5
ZONE_HINTLOCK1
Local switch (HS 911B) failure - Primary Confinement Zone
4.0E-6
ZONE_SWITCH2
Hardwired interlock (911B) failure - Primary Confinement Zone
1.2E-5
ZONE_HINTLOCK2

Figure D-3. Subtree PRIMARY_ZONES

INTENTIONALLY LEFT BLANK

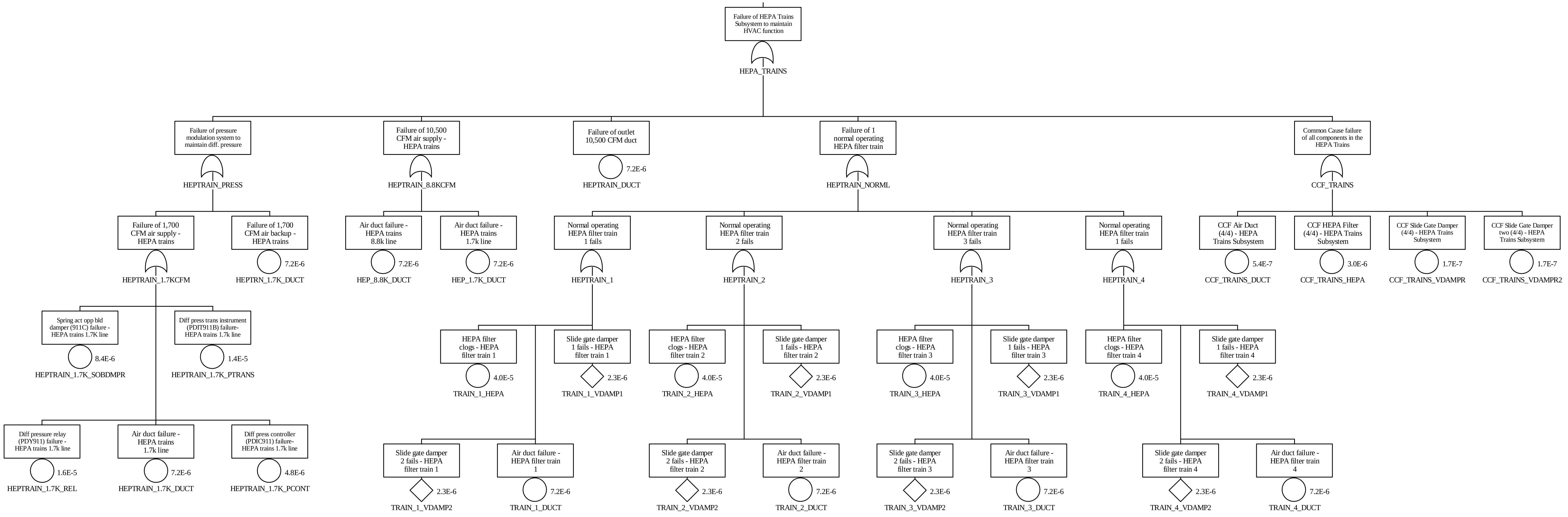

Failure of HEPA Trains Subsystem to maintain HVAC function
HEPA_TRAINS
Failure of pressure modulation system to maintain diff. pressure
HEPTRAIN_PRESS
Failure of 1,700 CFM air supply - HEPA trains
HEPTRAIN_1.7KCFM
Spring act opp bld damper (911C) failure - HEPA trains 1.7K line
8.4E-6
HEPTRAIN_1.7K_SOBDMPR
Diff press trans instrument (PDIT911B) failure- HEPA trains 1.7k line
1.4E-5
HEPTRAIN_1.7K_PTRANS
Diff pressure relay (PDY911) failure - HEPA trains 1.7k line
1.6E-5
HEPTRAIN_1.7K_REL
Air duct failure - HEPA trains 1.7k line
7.2E-6
HEPTRAIN_1.7K_DUCT
Diff press controller (PDIC911) failure- HEPA trains 1.7k line
4.8E-6
HEPTRAIN_1.7K_PCONT
Failure of 1,700 CFM air backup - HEPA trains
7.2E-6
HEPTRN_1.7K_DUCT
Failure of 10,500 CFM air supply - HEPA trains
HEPTRAIN_8.8KCFM
Air duct failure - HEPA trains 8.8k line
7.2E-6
HEP_8.8K_DUCT
Air duct failure - HEPA trains 1.7k line
7.2E-6
HEP_1.7K_DUCT
Failure of outlet 10,500 CFM duct
7.2E-6
HEPTRAIN_DUCT
Failure of 1 normal operating HEPA filter train
HEPTRAIN_NORML
Normal operating HEPA filter train 1 fails
HEPTRAIN_1
HEPA filter clogs - HEPA filter train 1
4.0E-5
TRAIN_1_HEPA
Slide gate damper 1 fails - HEPA filter train 1
2.3E-6
TRAIN_1_VDAMP1
Slide gate damper 2 fails - HEPA filter train 1
2.3E-6
TRAIN_1_VDAMP2
Air duct failure - HEPA filter train 1
7.2E-6
TRAIN_1_DUCT
Normal operating HEPA filter train 2 fails
HEPTRAIN_2
HEPA filter clogs - HEPA filter train 2
4.0E-5
TRAIN_2_HEPA
Slide gate damper 1 fails - HEPA filter train 2
2.3E-6
TRAIN_2_VDAMP1
Slide gate damper 2 fails - HEPA filter train 2
2.3E-6
TRAIN_2_VDAMP2
Air duct failure - HEPA filter train 2
7.2E-6
TRAIN_2_DUCT
Normal operating HEPA filter train 3 fails
HEPTRAIN_3
HEPA filter clogs - HEPA filter train 3
4.0E-5
TRAIN_3_HEPA
Slide gate damper 1 fails - HEPA filter train 3
2.3E-6
TRAIN_3_VDAMP1
Slide gate damper 2 fails - HEPA filter train 3
2.3E-6
TRAIN_3_VDAMP2
Air duct failure - HEPA filter train 3
7.2E-6
TRAIN_3_DUCT
Normal operating HEPA filter train 1 fails
HEPTRAIN_4
HEPA filter clogs - HEPA filter train 4
4.0E-5
TRAIN_4_HEPA
Slide gate damper 1 fails - HEPA filter train 4
2.3E-6
TRAIN_4_VDAMP1
Slide gate damper 2 fails - HEPA filter train 4
2.3E-6
TRAIN_4_VDAMP2
Air duct failure - HEPA filter train 4
7.2E-6
TRAIN_4_DUCT
Common Cause failure of all components in the HEPA Trains
CCF_TRAINS
CCF Air Duct (4/4) - HEPA Trains Subsystem
5.4E-7
CCF_TRAINS_DUCT
CCF HEPA Filter (4/4) - HEPA Trains Subsystem
3.0E-6
CCF_TRAINS_HEPA
CCF Slide Gate Damper (4/4) - HEPA Trains Subsystem
1.7E-7
CCF_TRAINS_VDAMPR
CCF Slide Gate Damper two (4/4) - HEPA Trains Subsystem
1.7E-7
CCF_TRAINS_VDAMPR2

Figure D-4. Subtree HEPA_TRAINS

INTENTIONALLY LEFT BLANK

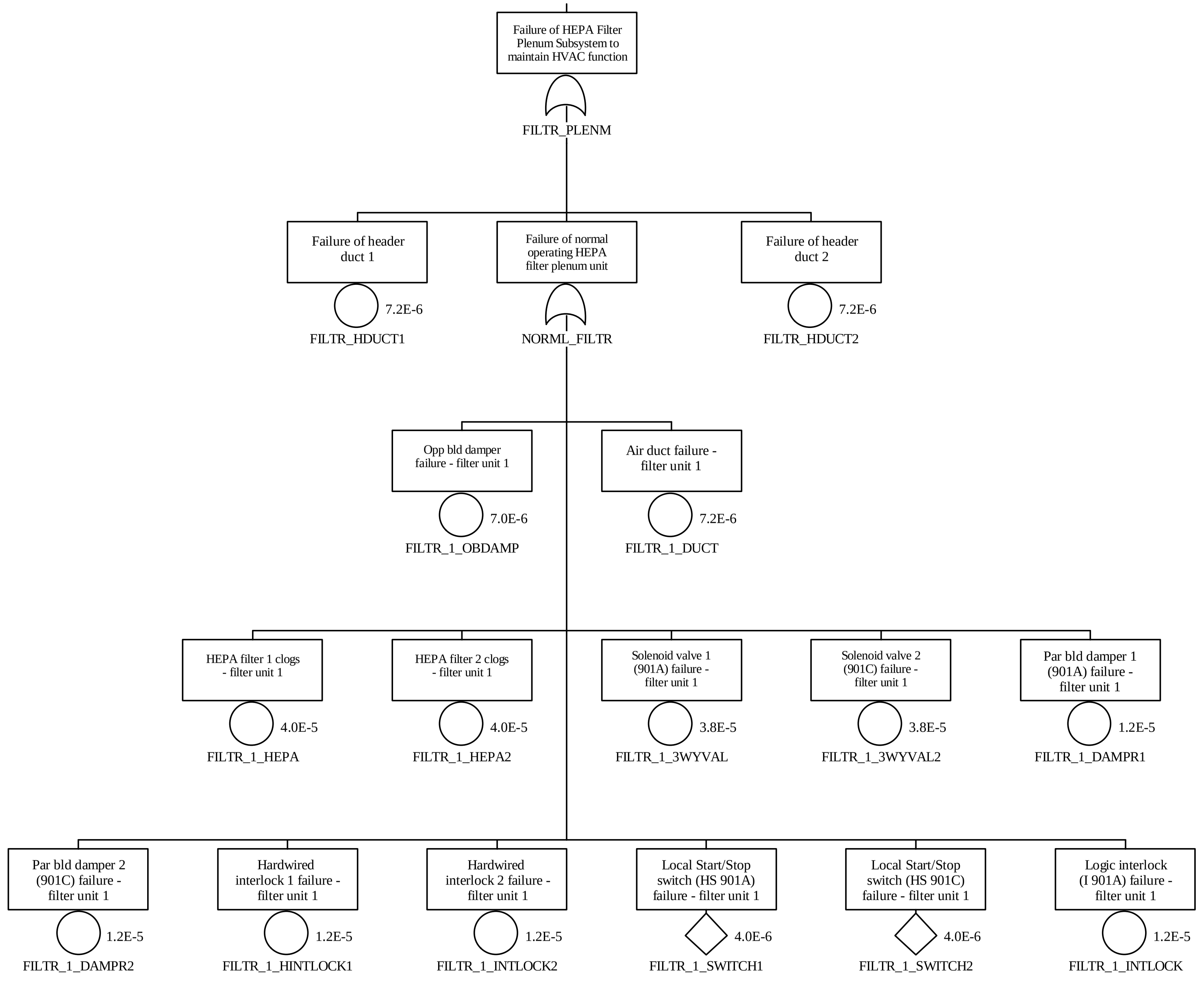

Failure of HEPA Filter Plenum Subsystem to maintain HVAC function
FILTR_PLENM
Failure of header duct 1
7.2E-6
FILTR_HDUCT1
Failure of normal operating HEPA filter plenum unit
NORML_FILTR
Failure of header duct 2
7.2E-6
FILTR_HDUCT2
Opp bld damper failure - filter unit 1
7.0E-6
FILTR_1_OBDAMP
Air duct failure - filter unit 1
7.2E-6
FILTR_1_DUCT
HEPA filter 1 clogs - filter unit 1
4.0E-5
FILTR_1_HEPA
HEPA filter 2 clogs - filter unit 1
4.0E-5
FILTR_1_HEPA2
Solenoid valve 1 (901A) failure - filter unit 1
3.8E-5
FILTR_1_3WYVAL
Solenoid valve 2 (901C) failure - filter unit 1
3.8E-5
FILTR_1_3WYVAL2
Par bld damper 1 (901A) failure - filter unit 1
1.2E-5
FILTR_1_DAMPR1
Par bld damper 2 (901C) failure - filter unit 1
1.2E-5
FILTR_1_DAMPR2
Hardwired interlock 1 failure - filter unit 1
1.2E-5
FILTR_1_HINTLOCK1
Hardwired interlock 2 failure - filter unit 1
1.2E-5
FILTR_1_INTLOCK2
Local Start/Stop switch (HS 901A) failure - filter unit 1
4.0E-6
FILTR_1_SWITCH1
Local Start/Stop switch (HS 901C) failure - filter unit 1
4.0E-6
FILTR_1_SWITCH2
Logic interlock (I 901A) failure - filter unit 1
1.2E-5
FILTR_1_INTLOCK

Figure D-5. Subtree FILTR_PLENM

INTENTIONALLY LEFT BLANK

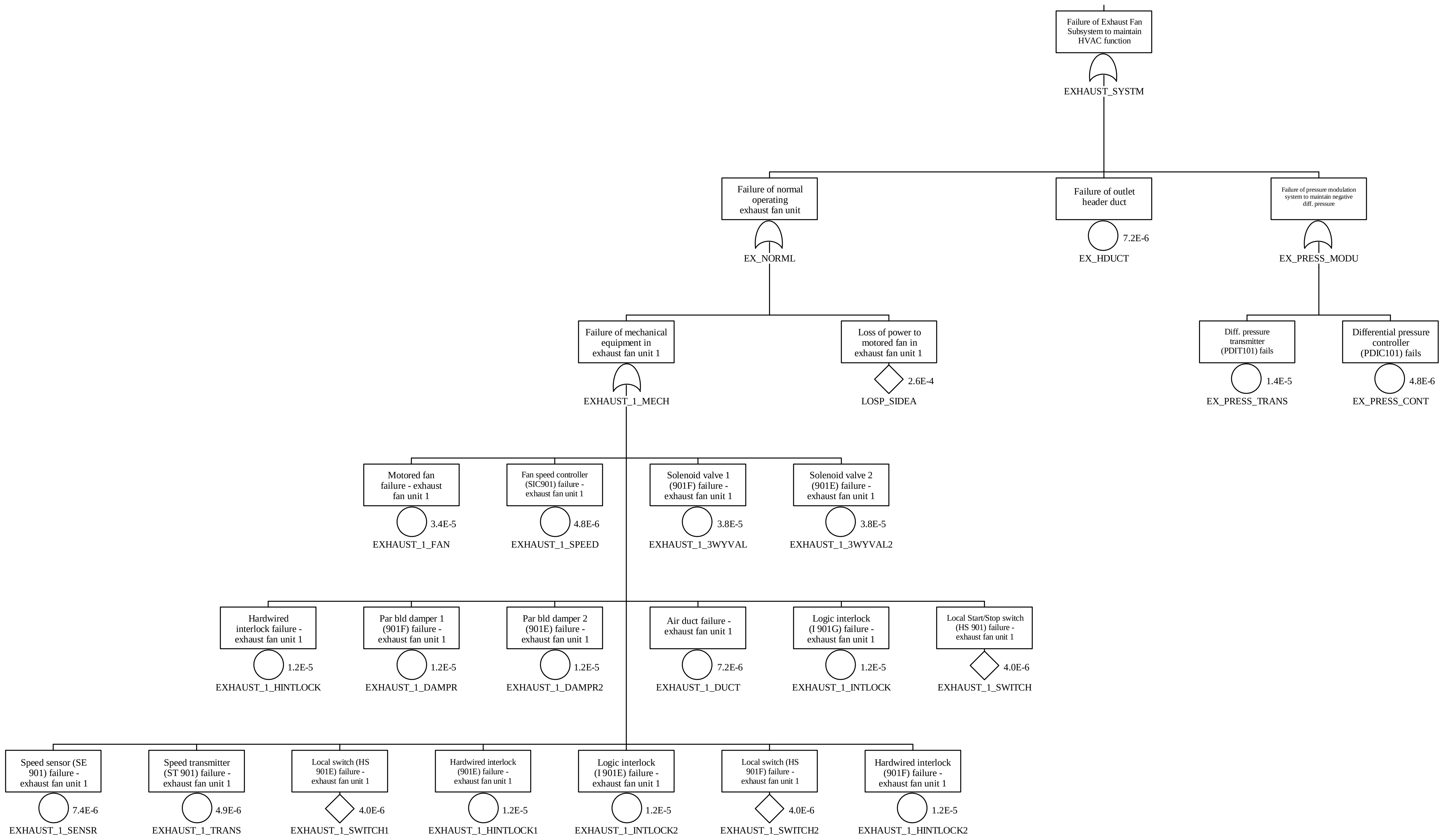

Failure of Exhaust Fan Subsystem to maintain HVAC function
EXHAUST_SYSTM
Failure of normal operating exhaust fan unit
EX_NORML
Failure of outlet header duct
7.2E-6
EX_HDUCT
Failure of pressure modulation system to maintain negative diff. pressure
EX_PRESS_MODU
Failure of mechanical equipment in exhaust fan unit 1
EXHAUST_1_MECH
Loss of power to motored fan in exhaust fan unit 1
2.6E-4
LOSP_SIDEA
Diff. pressure transmitter (PDIT101) fails
1.4E-5
EX_PRESS_TRANS
Differential pressure controller (PDIC101) fails
4.8E-6
EX_PRESS_CONT
Motored fan failure - exhaust fan unit 1
3.4E-5
EXHAUST_1_FAN
Fan speed controller (SIC901) failure - exhaust fan unit 1
4.8E-6
EXHAUST_1_SPEED
Solenoid valve 1 (901F) failure - exhaust fan unit 1
3.8E-5
EXHAUST_1_3WYVAL
Solenoid valve 2 (901E) failure - exhaust fan unit 1
3.8E-5
EXHAUST_1_3WYVAL2
Hardwired interlock failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_HINTLOCK
Par bld damper 1 (901F) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_DAMPR
Par bld damper 2 (901E) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_DAMPR2
Air duct failure - exhaust fan unit 1
7.2E-6
EXHAUST_1_DUCT
Logic interlock (I 901G) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_INTLOCK
Local Start/Stop switch (HS 901) failure - exhaust fan unit 1
4.0E-6
EXHAUST_1_SWITCH
Speed sensor (SE 901) failure - exhaust fan unit 1
7.4E-6
EXHAUST_1_SENSR
Speed transmitter (ST 901) failure - exhaust fan unit 1
4.9E-6
EXHAUST_1_TRANS
Local switch (HS 901E) failure - exhaust fan unit 1
4.0E-6
EXHAUST_1_SWITCH1
Hardwired interlock (901E) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_HINTLOCK1
Logic interlock (I 901E) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_INTLOCK2
Local switch (HS 901F) failure - exhaust fan unit 1
4.0E-6
EXHAUST_1_SWITCH2
Hardwired interlock (901F) failure - exhaust fan unit 1
1.2E-5
EXHAUST_1_HINTLOCK2

Figure D-6. Subtree EXHAUST_SYSTM

INTENTIONALLY LEFT BLANK

ATTACHMENT E

GLOSSARY

These terms have specific meaning in this reliability analysis. Note that the analysis determines the reliability of the system and does not distinguish between components that are designated as important to safety and those not so designated.

Redundant: Components that are the same type and perform the same function. Note that several components may be required to meet 100 percent system functionality and that these redundant components may not necessarily meet the typical nuclear industry criteria for redundant safety-related components or systems.

Independent and Dependent (events): Two basic events, A and B, are statistically independent if and only if the probability of A and B occurring together is equal to the probability of A times the probability of B. Otherwise the two events are statistically dependent. Events having common cause failures are examples of dependent events.

Common-Cause Failure (CCF): Failure of two or more identical and redundant structures, systems or components due to a single specific event or cause. Examples include a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon such as an earthquake, a man-induced event including ineffective maintenance, or some kind of a system interaction or domino effect that occurs when failure of one component leads to failure of one or more other components through some coupling mechanism. The potential CCFs and their coupling mechanisms that can be specifically identified, evaluated, or prevented through design or operational controls are termed “explicit” CCFs. Despite such controls, experience with highly reliable systems has demonstrated that there remains a finite probability of CCFs between components. Such failures are termed “implicit” CCFs. The analysis of implicit CCFs is especially important when analyzing systems comprised of identical and redundant components. The quantification of the probabilities of implicit CCFs is termed “parametric” methods.

INTENTIONALLY LEFT BLANK