HLWYM HEmails

From: Christopher Ryder
Sent: Wednesday, July 12, 2006 3:03 PM
To: Robert Johnson (NMSS); Rosemary Reeves; Albert Wong; Michael Waters
Cc: Marissa Bailey; Lawrence Kokajko
Subject: Re: Fwd: Dry Run for the ACNW presentation for Dry Cask Storage PRA
Attachments: Evaluating HVAC Performance.wpd

I was closely involved with the determination of the HVAC probability. The calculation was done by Peter Prassinos who started the work at NRC while on a rotational assignment form Los Alamos National Laboratory; I was the PM of that work. He modeled a the HVAC of a BWR containment. The BWR HVAC system is robust because is deigned to start when radioactive material is detected, but not to start do to false alarms from sensors that sporadically trip. Also, the system is designed to function such that the entire containment is not isolated at once. Peter used event trees and fault trees to model the HVAC. We have a simple example. The example and the PRA systems are not comparable; neither are the methods. I performed a similar analysis for an HVAC proposed by DOE years ago (see attached) to understand the DOE system (which is not being used anymore).

The probability of the canister breach from a 19 foot drop is due to the canister striking a non-yielding surface - the inside of the storage overpack as the canister is lowered from the transfer overpack on top. The design details and the drop height mean all the difference.

The crane work in the DCS PRA was done by myself and Lee Abramson.

We have only examples that should illustrate points. The examples are not full analyses. The examples should have some realism, but even if they numerically agree, the calculations themselves will not.

Chris

>>> Michael Waters 07/12/2006 2:16 PM >>>
Mahendra,

Thanks for sharing.

The debut of the dry cask storage PRA (for public comment?) is going to coincide with the timing of our PCSA ISG for public comment. The dry cask storage PRA calculates failure probabilities for crane, canister, and HVAC containment.

We are doing the exact same thing for those 3 systems as illustrative examples in the ISG! Although the accident scenarios (and perhaps design) are different, two of the three failure probability numbers between both documents may be significantly different. (The dry cask PRA calculates a 0.3 failure probability for a 19ft canister drop, and a 10-4 failure probability for HVAC)

The technical leads of our three ISG examples need to examine the dry cask PRA to make sure there are no glaring contradictions with what we are issuing. SFPO/RES may be interested as well on how we are calculating canister failure probabilities!!

Also, note that other portions of the dry cask PRA may be applicable to on-going preclosure issues such as HRA, source terms, and consequences.

Mike

>>> Mahendra Shah 07/12/2006 12:10 PM >>>
Attached please find an electronic file for the Storage Cask PRA, MAy 2006, prepared by RES and SFPO. Please note that the ACNW presentaion on the subjec is next Thursday, 7/20, in the afternoon. Thanks.

Mahendra

Dr. Mahendra J. Shah, P. E.
Senior Structural Engineer
Division of High-Level Waste Repository Safety US Nuclear Regulatory Commission
11545 Rockville Pike,
Rockville, MD 20852

Telephone: 301-415-8537
Fax: 301-415-5399
e-mail: mjs3@nrc.gov

Hearing Identifier: HLW_YuccaMountain_Hold_EX
Email Number: 65

Mail Envelope Properties (Christopher.Ryder@nrc.gov20060712150309)

Subject: Re: Fwd: Dry Run for the ACNW presentation for Dry Cask Storage PRA
Sent Date: 7/12/2006 3:03:09 PM
Received Date: 7/12/2006 3:03:09 PM
From: Christopher Ryder

Created By: Christopher.Ryder@nrc.gov

Recipients:
"Marissa Bailey" <Marissa.Bailey@nrc.gov>
Tracking Status: None
"Lawrence Kokajko" <Lawrence.Kokajko@nrc.gov>
Tracking Status: None
"Robert Johnson (NMSS)" <Robert.Johnson@nrc.gov>
Tracking Status: None
"Rosemary Reeves" <Rosemary.Reeves@nrc.gov>
Tracking Status: None
"Albert Wong" <Albert.Wong@nrc.gov>
Tracking Status: None
"Michael Waters" <Michael.Waters@nrc.gov>
Tracking Status: None

Post Office:

Files	**Size**	**Date & Time**
MESSAGE	3070	7/12/2006 3:03:09 PM
Evaluating HVAC Performance.wpd	1725412	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Appendix A

Performance of the HVAC System

A.1 Operation

DOE provided limited information on the design of the HVAC system. Based on the limited information and realistic assumptions, a preliminary analysis was performed to determine the response of the system to component failures and estimate the reliability of the system.

The dry transfer facility (DTF) is divided into four zones.

- Primary confinement zone (PCZ). Areas where radioactive material is present during normal operation.
- Secondary confinement zone. Areas where the potential for contamination is high.
- Tertiary confinement zone. Areas where the potential for contamination is low.
- Non-confinement zone. Areas with no potential for contamination.

Currently, only the HVAC of the PCZ is modeled.

The HVAC system of the primary confinement zone is illustrated in Figure A.1. The system consists of a supply side and an exhaust side. The exhaust side has two portions, a normal exhaust and a backup exhaust. The normal exhaust operates until there is a release of radioactive material in the PCZ at which point, the backup exhaust takes over. Normally, the throughput of the system is 85,000 cfm through the supply side and the normal exhaust. Given a release of radioactive material in the PCZ, both the supply side and the normal exhaust isolate, and backup exhaust system starts. The backup system is rated at 8,000 cfm. This changeover may be due to the lower volume backup system being better able to function

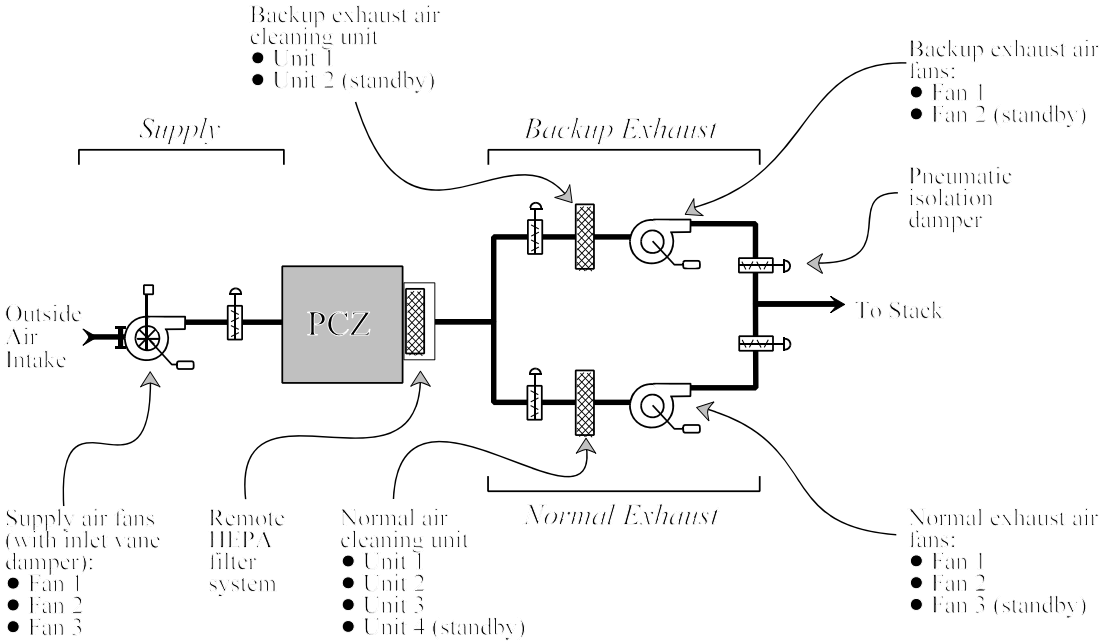


Figure A.1 HVAC system of the primary confinement zone.

with the supply side isolated; the higher volume normal exhaust may trip on low flow or high temperature with air from the supply. With the supply side isolated, a negative pressure develops in the PCZ; the volumetric flow is from leakage through cracks and past door seals. The DTF does not completely isolate when radioactive material is detected. More accurately, the normal HVAC system supply and exhaust isolate. At the same time, a backup system exhaust starts.

The HVAC system has two sets of HEPA filters, a remote set on the exhaust side of the PCZ and the other in the exhaust systems. The remote set prevents contamination from spreading in the exhaust ducts. The exhaust HEPA filters provide redundant filtering. Both filters are a glass fiber media with an efficiency of 99.97% removal of 0.3μ particles or larger.

The normal and backup exhaust systems vent through a common stack. By raising the release point, the radionuclides are disperse as they travel, thus, reducing the dose at the site boundary.

A.2 Aspects of the HVAC System That Have not Been Modeled

Several features of the HVAC system are not modeled because of a lack of information.

- Reliability of the electrical distribution system. The modeling treats electrical power as being available whenever needed. The electrical system has a backup diesel generator to power the facility when offsite power is lost. But electrical power may not always available. When electrical power is lost, reliance is placed on components to stop the operation in a fail-safe condition. For example, brakes on the crane may automatically engage to stop the motion of a fuel assembly or a cask. Another issue is what happens when power is restored. Also the shielded handling cell where fuel is transferred begins to heat up, giving rise to a potential for releases directly to the environment.

- Status of isolation valves upon a loss of power. When both normal power and backup power is lost, the fans will stop operating. The state (i.e., normally open, normally closed, previous state) of isolation valves when power is lost needs to be evaluated. This information is needed to assess the isolation state of the HVAC system.

- Capability of flow control values on the supply side of the PCZ, not shown in Figure A.1, to isolate the supply side. If the function of the valve is to throttle the supply side, the valves may not have a capacity to isolate the line. If the valves can isolate the line, then the valves provide additional assurance that the supply line can be isolated, making an unfiltered release to the environment highly unlikely.

- Resistance of the HEPA filters to low flow. The HEPA filters have resistance to flow. At low flow rates, such as from passive flow when the system is not functioning, the resistance may be enough to divert some flow through cracks and crevices through which the HVAC system normally draws air.

- Thermal loading rate in the PCZ when ventilation is lost. The modeling treats a release as occurring without regard to the time needed for the PCZ to heat up. The heating causes the air to expand and displace, carrying with it radionuclides. But the structures forming the PCZ have a heat capacity that will keep the temperature down. Many fuel assemblies in the PCZ, such as in the staging rack, can a significant heat load. An additional heat load occurs when the cladding oxidation rate increases with temperature.

- Radiation sensors and isolation logic. The current analysis is conditional on radioactive material

being detected given that it is released. But radiation detectors and associated logic have malfunctions; the sensors may be unable to detect radiation. Similarly, sensors give spurious signals. The sensor logic may be such that it guards against spurious signals placing the HVAC system in a emergency mode every time a sensor malfunctions. Yet it has to be sensitive enough to respond to radiation.

- Common cause failure during maintenance. Some failures may not be completely independent. A worker may, for example, incorrectly service all of the components in a redundant system. Procedures are needed to determine the extent to which redundant components are vulnerable.

- Reliability of the instrumentation monitoring the pressure differential across the HEPA filters. The modeling treats such instrumentation as being always available for the systems that are normally in use. The way in which the HEPA filters are monitored on the backup exhaust, which is normally not in use, has yet to be determined.

A.3 Assumptions

The following assumptions are made to make the analysis manageable.

1. A fan will trip from low flow or from over temperature when the isolation valves on either the inlet or the outlet are closed.

2. The fans on the supply side will trip on low flow or over temperature when the supply side is pushing air through the backup exhaust while the normal exhaust is isolated. The supply side delivers air at 85,000 cfm. The backup exhaust removes air at 8,000 cfm.

3. The fans on the normal exhaust will trip on low flow or over temperature when the supply side is isolated. The normal exhaust is rated at 80,000 cfm. This does not occur when the backup exhaust, rated at 8,000 cfm, draws on the isolated supply because this is a designed condition.

4. If one of multiple fans operating in parallel trips, the other fans will trip from excessive loads. Either a bank of components completely succeeds or completely fails

5. The HEPA filters are intact at the time that a cask or fuel assembly is dropped. Instrumentation measure the pressure differential across the filters. If a filter was on the PCZ or the normal exhaust was defective, the pressure differential would be reduced during normal operation, giving an indication, presumably in the control room. This assumption does not apply to the backup exhaust, which is normally inoperative; this is an open issue.

6. Though not indicated by the limited design information, the PCZ is normally at a slight negative pressure. This is typical of fuel handling facilities.

7. The HEPA filters have enough resistance to inhibit flow at low volumetric flow rates.

These assumptions allow the event tree to be simplified. Assumptions 1 and 2 eliminates branching at the fan events after the pneumatic isolation valves when these valves are closed. While the isolation valves are closed, the fan must trip. There is no need to represent the on/off state of the fan; the pass-through at this point implies that the fan is off. Notes on Figure A.2 explain the lack of branching at other points.

A.4 Model of the HVAC System

An event tree is used to delineate modes of HVAC failure that result from combinations of major component types on the supply and exhaust sides given a release of radioactive material into the PCZ. The event tree is shown in Figure A.2. The events at the top are the major components — fans, pneumatic isolation valves, and gravity dampers. The event tree does not model the progression of events, but the status of the major components. The upper branch is always the success path; the lower branch is always the failure path.

The event tree accounts for some types of common mode failures. Reference A.1 defines intrinsic dependencies, where the function state of a component is affected by the state of another component, and extrinsic dependencies, where the dependencies occur for reasons that are beyond the physical connections such as erroneous maintenance. Figure A.2 accounts for cascade failures — the failure of one component leads to the failure of another component. For example, a fan will not operate if the isolation valve is closed. Functional input (unavailability) and shared equipment dependencies are not modeled because of a paucity of information. For example, the reliability of the electrical system to power the HVAC system was not modeled. Extrinsic dependencies, such as erroneous maintenance on redundant components, are not taken into account because information about procedures is unavailable. The dependencies are taken into account by a lack of branching in Figure A.1. The lack of branching indicates that the subsequent component cannot have *either* a success or failure state, only one state that is taken to be a failure. Notes on page A.6 to Figure A.1 explain some such logic.

The event tree in Figure A.2 delineates twenty five states of the HVAC are delineated. Each path through the tree is a combination of component failures. These combinations are assessed in Section A.5. The assessments are summarized at the top right of Figure A.2 as the end states — the state of the system at the end of sequences. The end states are conditional on radioactive material being detected; normal operation is not an event sequence. The end states are defined as follows:

- In-leakage. A negative pressure exists in the PCZ, either because the system is oeraing as designed or because a particular combination of component failures leaves the system functioning with a similar result. Leakage into the cell is occurring from the surrounding zones.

- Reduced in-leakage. The system is drawing from the PCZ, but other system failures have degraded the function. In-leakage is occurring from surrounding zones.

- Partial out-leakage. The PCZ has a slight partial pressure, causing leakage out of, instead of into, the PCZ. The slight positive pressure may be due to passive flow from heating inside the PCZ.

- Out-leakage. The supply side is pushing air into the PCZ faster than it is removed, creating a positive pressure that forces out-leakage into surrounding areas

- Environmental release. A release occurs to the environment without passing through the HEPA filters.

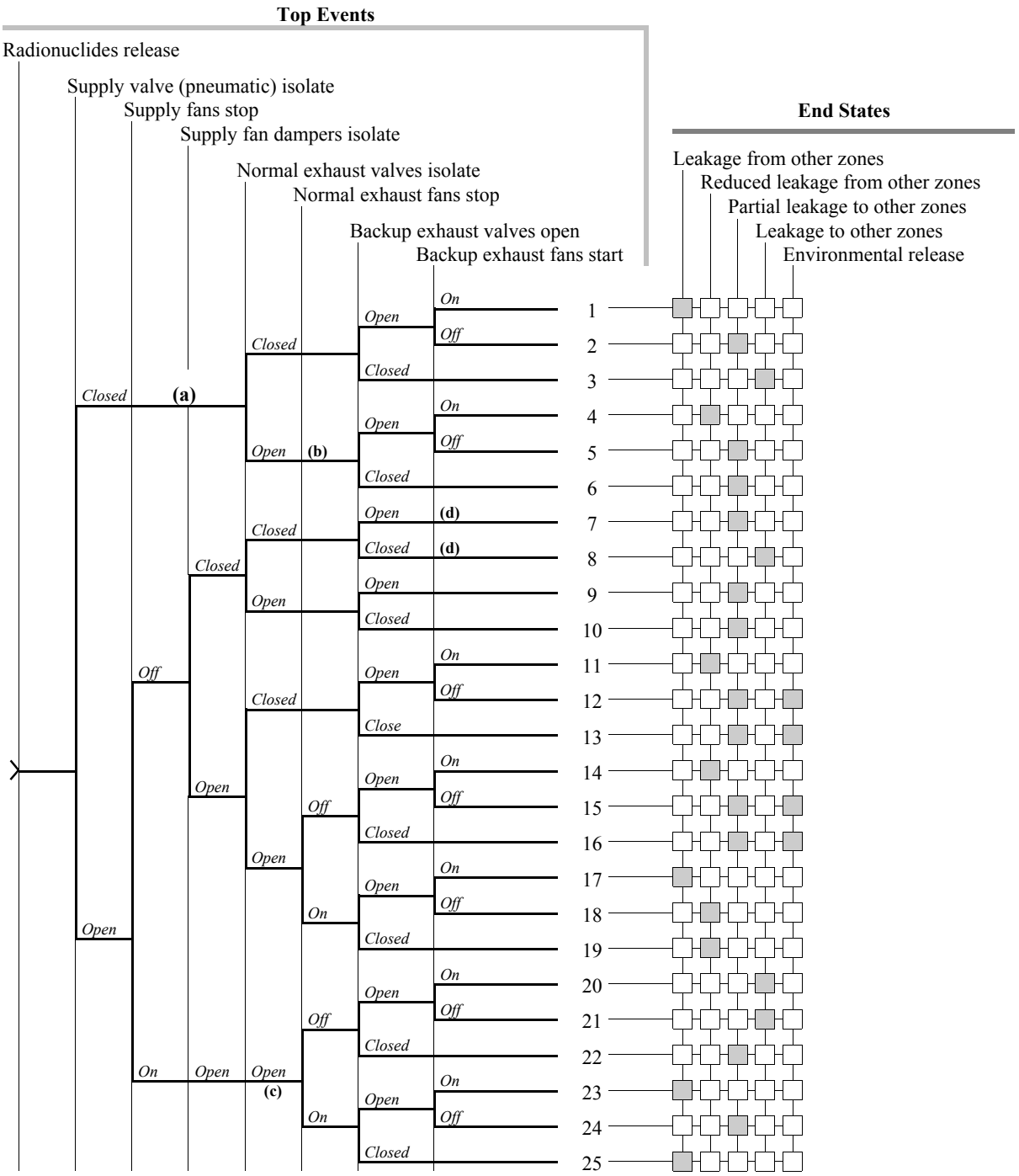


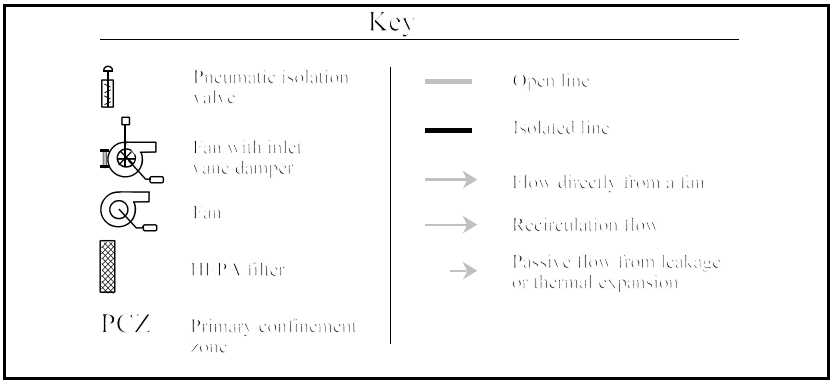
Figure A.2 Event tree delineating the failure modes of the HVAC system in the PCZ. LEGEND: Shaded box indicates that an end state is applicable to a sequence. White box indicates that an end state is inapplicable to a pathway. Letters in parentheses are notes on Page A.6.

Notes for Figure A.2

(a)	The pneumatic isolation valves are closed. Therefore, the fans must be tripped. The gravity dampers are no longer at issue because the supply side is isolated by the pneumatic valve.
(b)	The fan must be off for the gravity damper at (a) to be closed.
(c)	By Assumption 3, when the normal exhaust is isolated, the supply fans cannot be operating.
(d)	The fan cannot be operating because the gravity damper on the supply is closed.

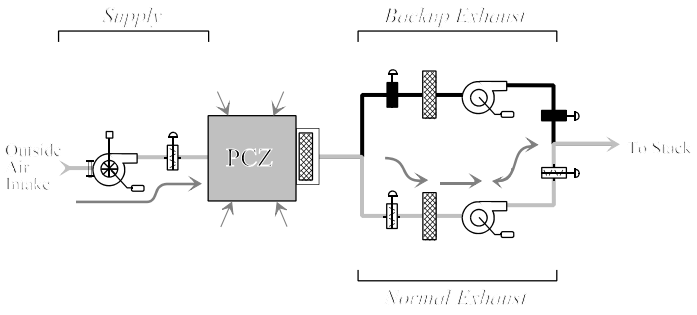
A summary of the end state determinations from Section A.5 is under the end state titles in Figure A.2. A shaded box indicates that a given end state was assessed as occurring; a white box indicates that the end state was assessed and not occurring. The ends state classes can be further grouped as necessary.

A.5 End State Determination

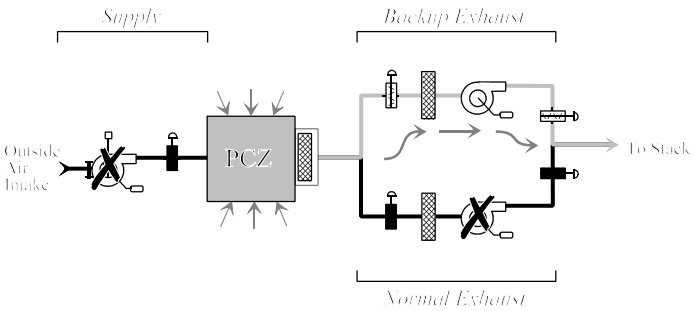


The end states of each sequence in Figure A.2 are characterized by assessing the effects of component failure combinations. For each pathway, the component failures are marked on a simplified diagram of the system. The effects of the failures are then qualitatively determined by reasoning the direction of air flow implied by the component failures. From the assessment, the result of the component failures given a release are characterized. The results of the determinations are summarized in Figure A.2 by the boxes after the ends of the paths.

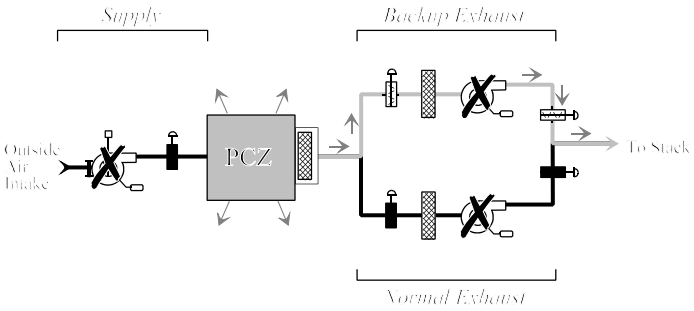
Normal operation. Supply side delivers 85,000 cfm. Normal exhaust removes 85,000 cfm. Backup exhaust is isolated. By Assumption 6 (page 3), the PCZ is maintained at a slight negative pressure.



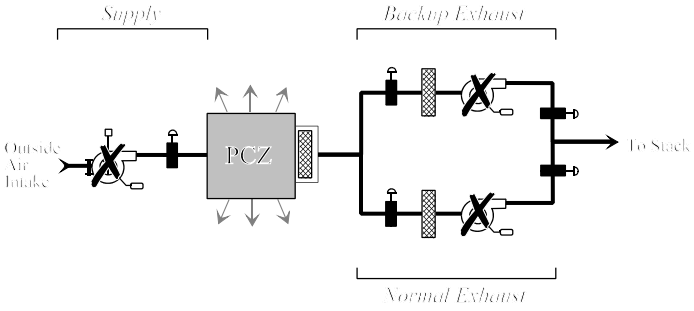
Sequence 1: Design isolation. Supply side and normal exhaust isolate. Backup exhaust opens and draws 8,000 cfm on the PCZ. Negative pressure in the PCZ draws leakage from 2° and 3° areas.



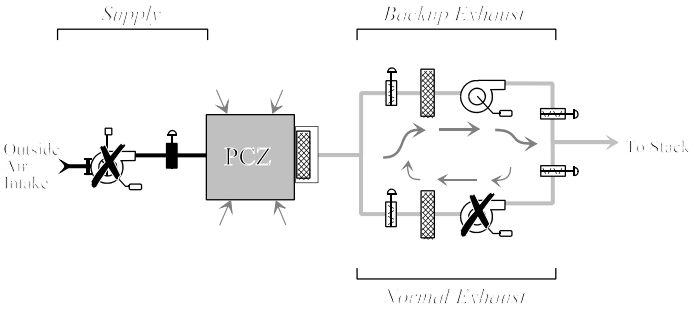
Sequence 2. Supply side and normal exhaust isolate. Backup exhaust opens, but fan fails to start. Passive flow through the backup exhaust, but some resistance of HEPA filter on the backup exhaust causes a slight positive pressure in the PCZ, resulting in some leakage from the PCZ into other zones.



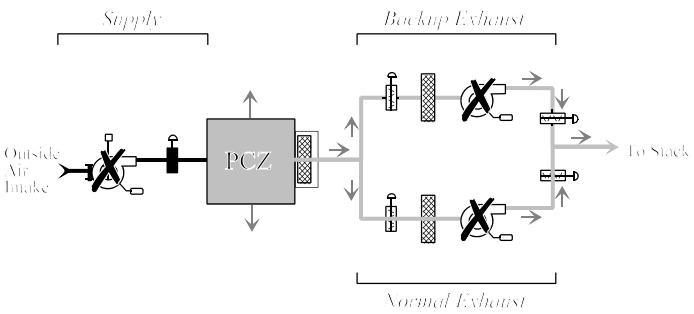
Sequence 3. Supply side and normal exhaust isolate. The backup exhaust fails to open. No passive flow through the supply and exhaust sides. Leakage from the PCZ into other zones.



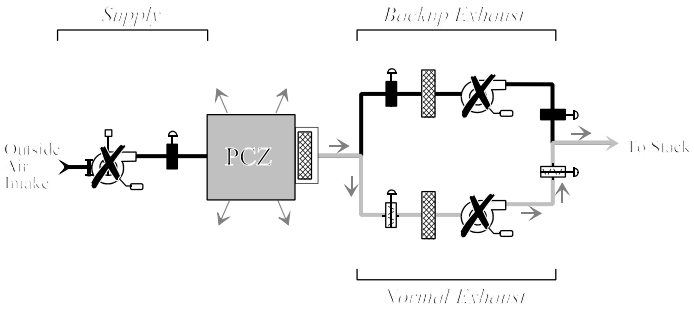
Sequence 4. Supply isolates. Normal exhaust fails to isolate, but the fan trips on low flow or high load without air from the supply. Backup exhaust opens and draws from PCZ. Some backup exhaust recirculates through normal exhaust, reducing suction on the PCZ. The reduced suction reduces the leakage from the other zones into the PCZ.



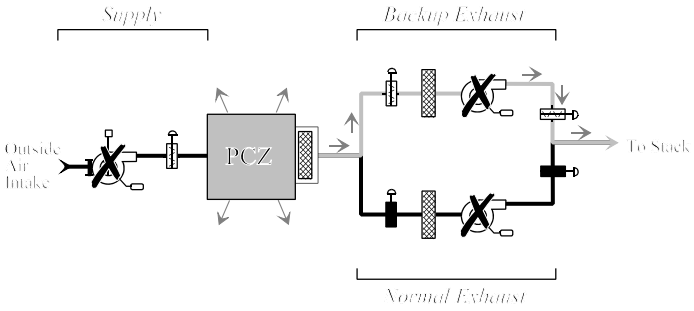
Sequence 5: Supply isolates. Normal exhaust fails to isolate, but the fan trips on low flow and high temperature without air from the supply. The backup exhaust opens, but the fans fail to start. Some passive flow though the normal and backup exhausts. Resistance of the HEPA filter causes some leakage from the PCZ into other zones.



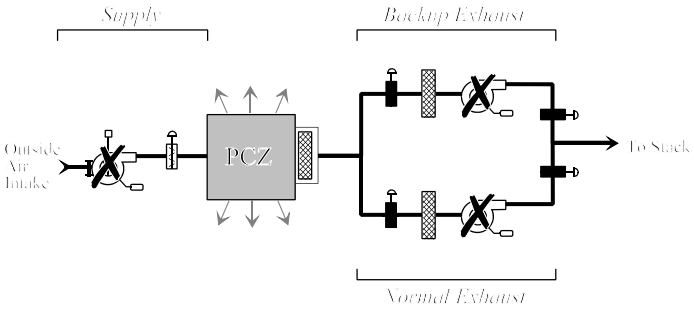
Sequence 6. Supply isolates. Normal exhaust fails to isolate, but the fan trips on low flow and high temperature without air from the supply. Backup exhaust does not open, hence, the fan cannot operate. Passive flow from heating in the PCZ occurs through the normal exhaust; resistance of the HEPA filters cause a slight positive pressure in the PCZ. Leakage to other zones occurs.



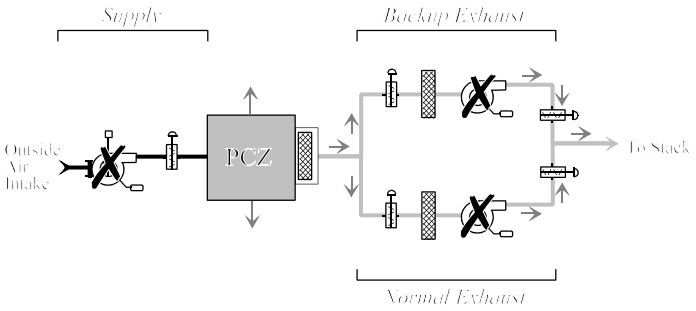
Sequence 7. Pneumatic valve fails to isolate on the supply side, but the fans stop. The normal exhaust isolates. The backup exhaust opens but the fan fails to start. Without flow through the supply side because there is no exhaust suction, the supply side dampers on the close, isolating the supply side. Passive flow through the backup exhaust is inhibited by the resistance of the HEPA filters. Slight positive pressure in the PCZ from heating causes leakage into the other zones.



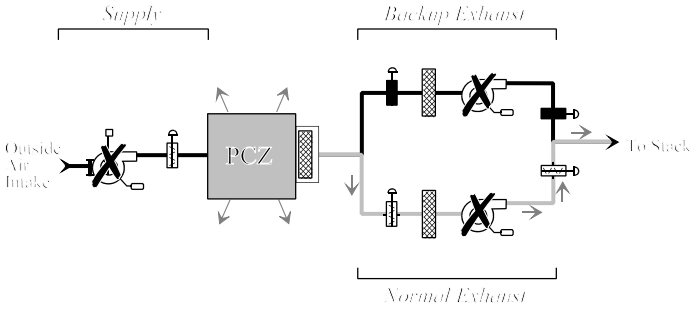
Sequence 8. Pneumatic valve fails to isolate on the supply side, but the fans stop. The normal exhaust isolates. The backup exhaust fails to open. Without flow through the supply side, either because the fans are stopped or there is no exhaust suction, the supply side dampers on the fan must be closed. Therefore, the supply side is isolated. Positive pressure in the PCZ from heating causes leakage into the other zones.



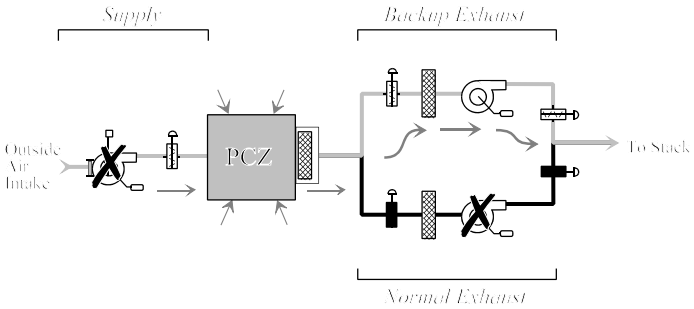
Sequence 9. Pneumatic valve fails to isolate on the supply side, but the fans stop. The normal exhaust fails to isolate, but the fans stop. The backup exhaust opens, but the fan fails to start. The closed supply side dampers means that there is no exhaust suction (e.g., fans are stopped). Therefore, the supply side is isolated. Passive flow from heating in the PCZ cause flow through both exhausts is inhibited by the resistance of the HEPA filters. Slight positive pressure in the PCZ causes leakage into other zones.



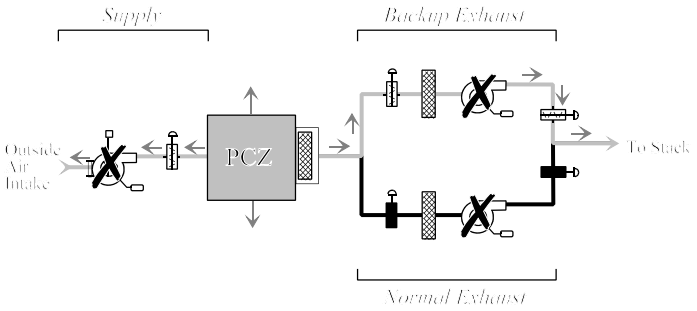
Sequence 10. Pneumatic valve fails to isolate on the supply side, but the fans stop. The normal exhaust fails to isolate, but the fans stop. The backup exhaust fails to open. Without suction because the fans are stopped, the supply side dampers are closed, isolating the supply side. Passive flow through the normal exhaust is inhibited by the resistance of the HEPA filters. Slight positive pressure in the PCZ causes leakage into the other zones.



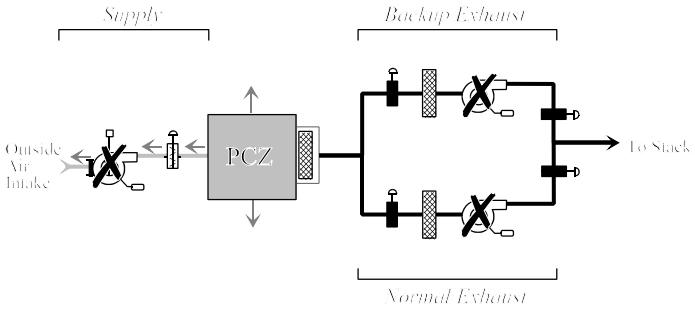
Sequence 11. Pneumatic valves on the supply fails to isolate, but fan trips. Normal exhaust isolates. Backup exhaust opens and draws from PCZ, keeping the dampers on the supply open. Reduced in-leakage into the PCZ because the open supply allows air into the PCZ, thus reducing the negative pressure that the backup exhaust can create.



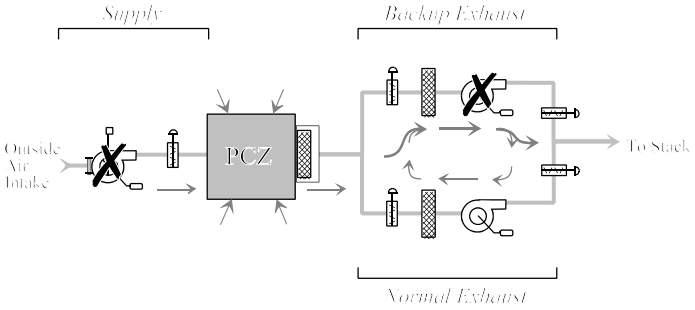
Sequence 12. Supply side fails to isolate, but the fan trips. Normal exhaust isolates. Backup exhaust opens, but fan fails to start. Without forced flow from the exhausts, the back draft gravity dampers on the supply side fail to close, leaving the supply open. Passive flow through the open backup exhaust is inhibited by the resistance of the HEPA filters. Slight positive pressure in the PCZ causes leakage occur into other zones; unfiltered passive flow through the open supply.



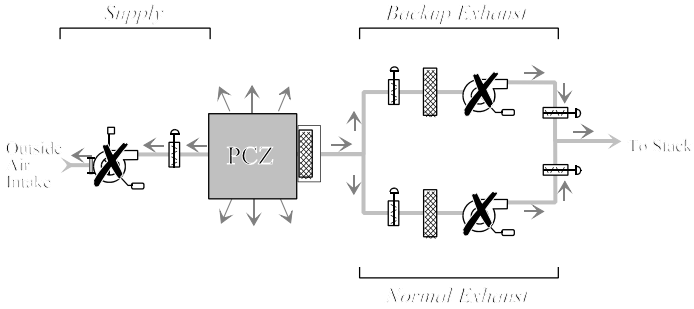
Sequence 13. Supply side pneumatic isolation valve fails to close, but the fan trips. Normal exhaust isolates. Backup exhaust fails to open. Without drawing from the PCZ, the gravity damper should close, but fails to do so. Slight positive pressure develops in the PCZ from heated air expanding. Leakage occurs into other zones; unfiltered passive flow occurs through the open supply.



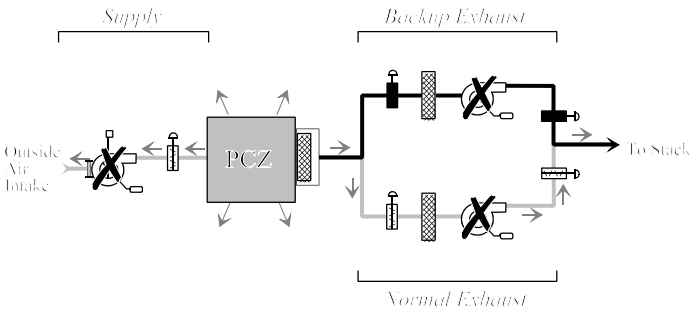
Sequence 14. Supply side and normal exhaust fail to isolate, but the fans stop. Backup exhaust opens and the fan energizes. The gravity damper on the supply side is remains open because of the suction from the backup exhaust. Some recirculation between the backup and normal exhausts, but resistance of the HEPA filter on the back up exhaust forces air to the stack. Suction of the backup exhaust draws a negative pressure on the PCZ that is reduced by the open supply. Reduced leakage into the PCZ from other zones.



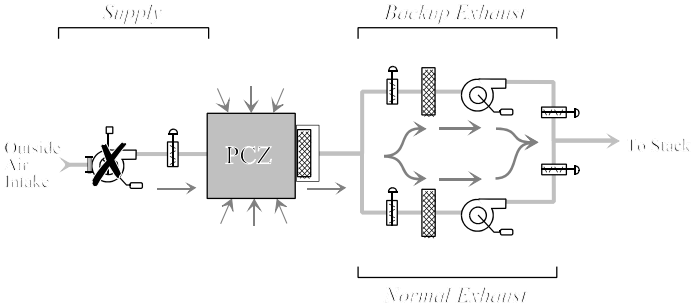
Sequence 15. Normal exhaust fails to isolate, but the fans stop. Backup exhaust opens, but the fans fail to start. Supply side pneumatic value fails to isolate, but the fan stops; even without forced flow, the gravity dampers on the supply fans fail to close. The HVAC system is open. From thermal expansion as the PCZ warms from decay heat, passive flow occurs through the exhausts, leakage occurs into the other zones, and an unfiltered release exists the supply side.



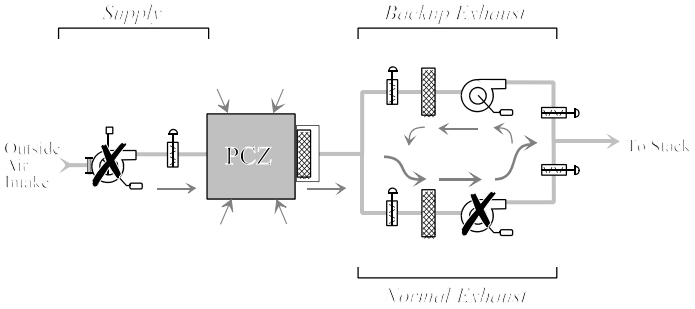
Sequence 16. Pneumatic isolation valve on the supply side fails to isolate, but the fan trips. Normal exhaust fails to isolate, but the fan trips. Backup exhaust fails to open. Without forced flow through the system, the gravity dampers on the supply side should isolate, but fail to do so. Heating in the PCZ causes passive flow through the normal exhaust, leakage into the other zones, and unfiltered release through the supply side.



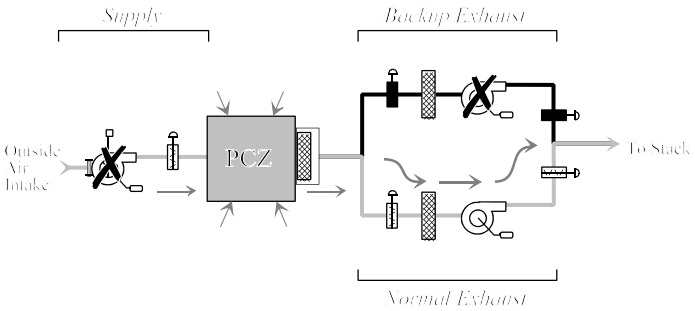
Sequence 17. Supply side fails to isolate, but the fan trips. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust opens and the fan energizes. Both exhaust systems draw air through the PCZ from the supply side, keeping the gravity dampers open. Normal exhaust draws air from the open supply to operate. Backup exhaust pulls additional air to draw a negative pressure equivalent to the normal response. Leakage from the other zones into the PCZ occurs.



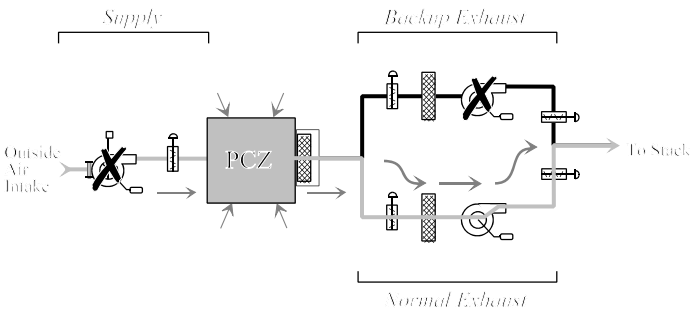
Sequence 18. Supply side fails to isolate, but the fan trips. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust opens, but the fan fails to start. The normal exhaust draws air through the supply side, keeping the gravity damper on the supply side open. Some recirculation through the backup exhaust reduces the suction on the PCZ. Leakage from the other zones into the PCZ occurs.



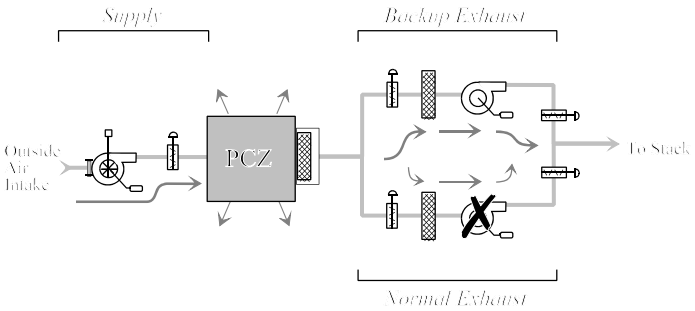
Sequence 19. Supply side fails to isolate, but the fan trips. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust fails to open. The open supply side allows the normal exhaust to function. The normal exhaust draws on PCZ and the supply side, keeping the gravity dampers on the supply side open. Because of slight negative pressure in the PCZ, some leakage from other zones occurs.



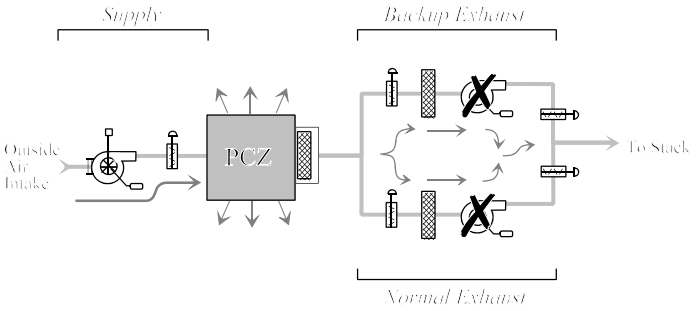
Sequence 19. The supply side fails to isolate, but the fans trip. The normal exhaust side fails to isolate and the fan fails to trip. The backup exhaust fails to open and the fans either fail to start or trip on low flow or high temperature. The normal exhaust draws air through the supply keeping the dampers open. The suction from the normal supply draws somewhat on the PCZ. The open supply allows the normal exhaust to function.



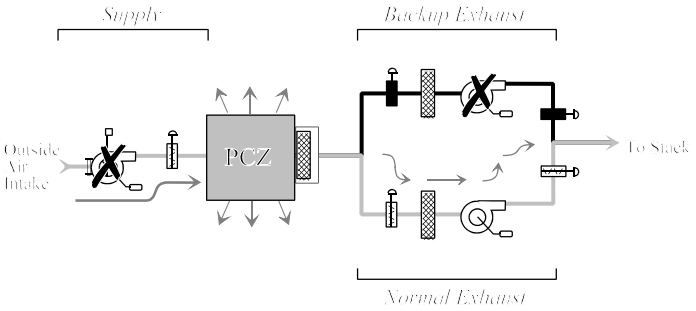
Sequence 20. The supply side fails to isolate and the fans fail to trip. The normal exhaust fails to isolate, but the fans trip. The backup exhaust opens and the fans start and operate. Because the supply is much greater than the backup exhaust, even with the backup exhaust drawing, some flow is through the normal exhaust. The PCZ has a somewhat positive pressure, causing leakage from the PCZ into the other zones.



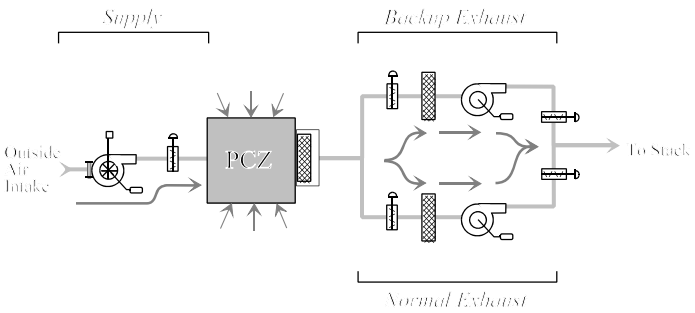
Sequence 21. Supply fails to isolate and the fan fails to trip. Normal exhaust fails to isolate, but the fan trips. Backup exhaust opens, but the fan fails to start. Supply pushes air through the normal exhaust, creating a positive pressure in the PCZ. Leakage occurs into other zones.



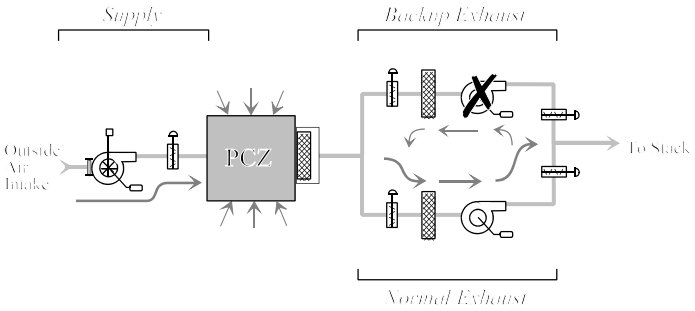
Sequence 22. Supply fails to isolate and fan fails to trip. Normal exhaust fails to isolate, but the fan trips. Backup exhaust remains isolated. Supply pushes air through the normal exhaust, creating a positive pressure in the PCZ. Leakage occurs into other zones.



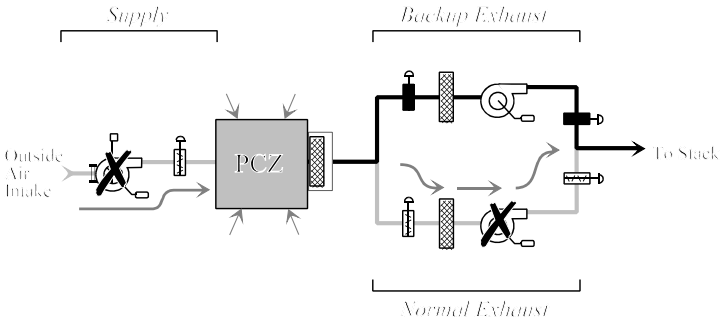
Sequence 23. Supply side fails to isolate and the fans fail to trip. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust opens and the fans energizes. Normal exhaust draws supply air volume. Backup draws additionally on PCZ causing in-leakage.



Sequence 24. Supply fails to isolate and the fan fails to trip. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust opens, but the fan fails to start. Some recirculation between the exhaust systems. Supply side pushes air into the PCZ; losses in the exhaust due to recirculation make pull by normal exhaust slightly less than the supply. Slightly positive pressure in the PCZ causes leakage into the other zones.



Sequence 25. Supply fails to isolate and the fan fails to trip. Normal exhaust fails to isolate and the fan fails to trip. Backup exhaust fails to open. The result is similar to the designed operation.



A.6 Fault trees

The top events of the event tree in Figure A.2 are developed with fault trees. Stylized illustrations of the fault trees are in Figures A.4 through A.9. For simplicity, the supply side and the exhaust side in the HVAC system are treated as being entirely on or entirely off. There are no gradations of operation, such as one fan out of 3 fans failing to stop. This greatly simplifies the analysis of air flow in the system as discussed in Section A.5.

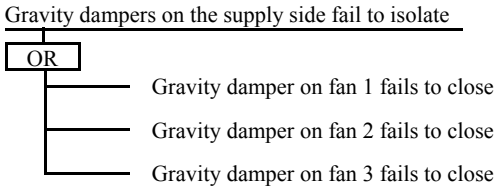


Figure A.4 Fault tree of supply fan dampers failing to close.

Figure A.4 illustrates the fault tree of the gravity dampers on the fans of the supply side. The supply fans operate in parallel. To isolate the line at this point, the damper on all three fans need to close. For the dampers collectively to fail, either one needs to fail; the logical relationship is an OR gate.

For a gravity damper to close, both the fan has to trip to remove the air flow keeping it open and the damper itself has to move to the closed position. But the dependency of the damper on the fan operation is taken into account in the event tree. Any forced flow through the system keeps the dampers will open.

Figure A.5 illustrates the fault tree of the supply side fans. Three fans deliver a total of 85,000 cfm. In Figure A.5, the fan, not the relay that operates the fan, is illustrated; in the fault tree model that was used for the calculations, the data of the relay was used. To isolate the line, all three fans must stop. To fail to isolate, any one fan must fail to stop by its relay failing to open. The logical relationship is Gate A, an OR gate. Gates B, C, and D account for combinations of two fans failing to trip. Gate E accounts for all three fans failing to trip.

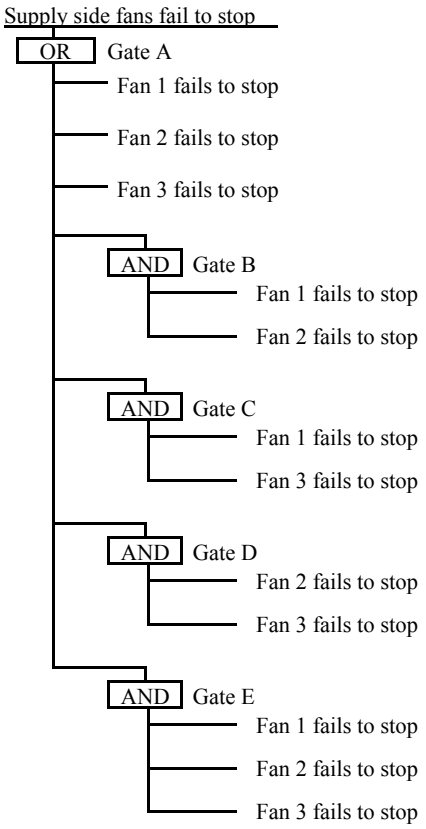


Figure A.5 Fault tree of the supply side fans ceasing to deliver.

Figure A.6 illustrates the fault tree of the normal exhaust valves failing to isolate. The pneumatic valves are in series. For the line to isolate, either value needs to close. For the line to fail to isolate, both valves must fail. Therefore, the logical relation is an AND gate.

Figure A.7 illustrates the fault tree of the normal exhaust fans. Three fans must stop as part of isolating the normal exhaust line. That is, Fan 1 and Fan 2 and Fan 3 must trip. A failure then is if any one or more of the fans does not trip. Thus Gate A is an OR

gate. The first three branches are for individual fan failures. Gates B, C and D account for combinations of two fails failing to stop. Gate E accounts for all three fans failing to stop.

When the probabilities are low, the combinations of failed components is insignificant and can be ignored. Thus, Gates B, C, D, and E are not in the model used for calculations.

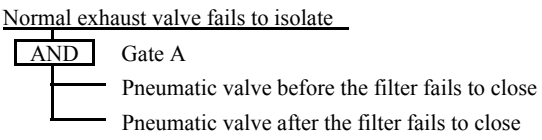


Figure A.6 Fault tree of the normal exhaust failing to isolate

Figure A.8 illustrates the fault tree of the backup exhaust fans failing to start. The system consists of Fan 1 and a standby fan. Each fan is modeled as starting by a relay de-energizing. For the system to operate, only one fan needs to operate. For the system to fail, both Fan 1 and the standby fan must fail to operate. This is relationship is Gate A, an AND gate. For Fan 1 to fail, the relay must fail to open, the fan must fail to start, and the fan must fail to continue to run. This logic is in Gate B, an AND gate. For the Standby Fan to fail, the transfer from Fan 1 must fail, the relay must fail to open, the fan must fail to start, and the fan must fail to continue to run. This logic is related by Gate C, an AND gate.

Figure A.9 illustrates the fault tree of the backup exhaust line to open. The line has two pneumatic valves in series. Both valves must open for the system to successfully operate. Either one of the valves can fail for the line to remain isolated. This logic is Gate A, an OR gate.

A.7 Data

The data used to for the reliability calculations are shown in Table A.1. The data were taken from References A.2 and A.3. Lacking a specific design and specification of components, the data are believed to be appropriate as a first approximation.

A.8 Insights

The failure of the HVAC system is more complex than a catastrophic failure where the HEPA filters are nor longer functioning.

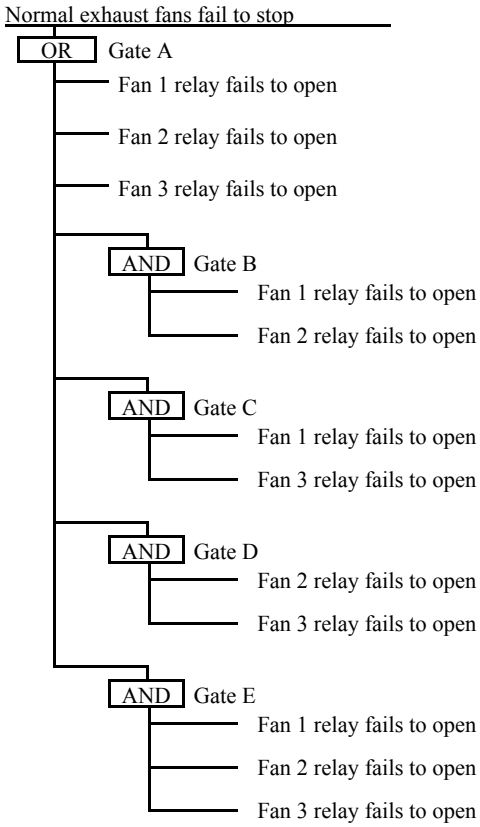


Figure A.7 Fault tree of the normal exhaust fans in the primary areas failing to stop.

The exhaust system is more important to maintain during an accident than supply to avoid pressurizing the PCZ. For added assurance, the normal exhaust has a standby fan to replace one of the normal fans, should one fail to run. Thus, there are four fans, of which, only three are needed for normal exhaust.

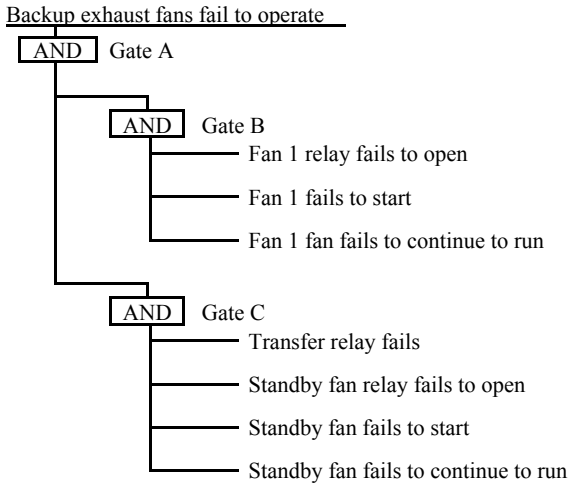


Figure A.8 Fault tree of the backup exhaust fans failing to remove air.

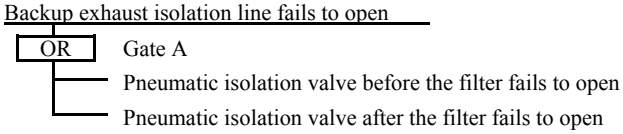


Figure A.9 Fault tree of the backup exhaust line in the HVAC system of the 1° zone failing to open.

Reference

A.1. A. Mosleh, et. al., "Guidelines on Modeling Common-cause Failures in Probabilistic Risk Assessment," NUREG/CR-5485, November 1998.

A.2. Combustion Engineering, Inc., "CESSAR Design Certification, System 80+ Standard Design FSAR, Appendix 19.5A — Data Calculations for Generic Component Data," Amendment M (March 15, 1993) and Amendment W (June 17, 1994).

A.3 General Electric Corporation, "ABWR Standard Safety Analysis Report - Chapter 19D, Probabilistic Evaluations," Amendment 31, July 1993.

Table A.1. Data used in the fault trees

Component	Mode	Probability
Transfer contact relay Tie breaker relay	Fails to close	$3x10^{-4}$ / d
	Fails to open	$3x10^{-4}$ / d
Gravity Damper (back-draft)	Fails to open	$7x10^{-4}$ / d
	Fails to close	$7x10^{-4}$ / d
Damper with operator	Fails to close	$3x10^{-3}$ / d
	Fails to open	$3x10^{-3}$ / d
Fan	Fails to start	$6x10^{-4}$ / d
	Fails to run	$1x10^{-5}$ / hr