Iterative Process for Development and Implementation of Safety Bases

Presented to:
NRC/DOE Technical Exchange and Management Meeting on Preclosure Safety Analysis and Supporting Information

Presented by:
Thomas Dunn
Preclosure Safety Analysis
Bechtel SAIC Company, LLC

Dave Tooker
Repository Design Engineering
Bechtel SAIC Company, LLC

May 16-17, 2006
Las Vegas, Nevada

Implementation Process for Safety Bases: Important to Safety (ITS) Active Systems

- **Approach**
  - **Nuclear safety design bases**
  - **Design detail necessary to demonstrate requirements are met**
  - **Assessment that requirements are achievable**
- **Examples of selected active systems**
  - **Standard equipment: Overhead cranes**
  - **Standard systems: HVAC / HEPA**
  - **Non-standard equipment: Trolley**

HVAC = heating, ventilation, and air conditioning
HEPA = high-efficiency particulate air (filter)

Example: Nuclear Safety Design Bases Reliability Requirement for Overhead Crane

- **Important to Safety**
  - **Minimize the probability of a load drop or collision**

- **Nuclear Safety Design Bases Requirement**
  - **The drop rate for cranes involved in handling waste forms shall be equal to or less than 10^{-5} drop / transfer**

Information Sufficient to Perform a Reliability Assessment on System

- **Basis of design (BOD) document**
- **Mechanical equipment envelope (MEE) drawings**
- **Piping and instrumentation diagram (P&IDs)**
- **Control logic functional diagrams**
- **System Description Document (SDD)**
- **Facility Description Document (FDD)**
- **Design / procurement specifications**
- **Mechanical handling calculations**

Demonstration of Safety for Overhead Crane in License Application

- **Basis of design document that defines the safety design requirements and safety functions**
- **NOG-1 Type 1 or Type 2 justification**
- **Mechanical equipment envelope drawing(s) for the crane**
- **Crane P&IDs that identify the principal controls on the crane**
- **Logic diagrams for the crane that present the controls and control logic for each of the crane safety functions**

Demonstration of Safety for Overhead Crane in License Application (cont.)

- System Description Document and Facility Description Document that provide description of crane controls, equipment, and operation
- Mechanical handling calculations that define the space envelope, load paths, load drops, and interactions with other systems, components, and structures
- Crane specification

Example: Demonstration that Overhead Cranes Meet Reliability Requirement

- **Reliability estimate based on operating experience at U.S. nuclear power plants**
  - **Data from NUREG-1774 (A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002) over the period 1980 to 2002**
  - **Data for an estimated 54,000 very heavy lifts (>30 tons) was used to estimate that overhead crane drop rate is about 9×10^{-6} drops per lift**

Example: Demonstration that Overhead Cranes Meet Reliability Requirement (cont.)

- **Calculated crane drop rate**
  - **Includes failures due to all modes (e.g., human error, control system failures, etc.)**
  - **Is conservative because operating experience covers both single failure-proof cranes and non-single failure proof cranes, while repository cranes will be designed to NOG-1**
- **Tracking of uncertainties and margins**
- **Stacking conservatisms**

Example: Nuclear Design Bases Reliability Requirement for HVAC / HEPA System

- **Important to Safety**
  - **HVAC / HEPA**

- **Nuclear Safety Design Bases Requirement**
  - **The probability that the HVAC system, including HEPA filtration in the primary confinement areas, becomes unavailable during a 4-hour mission time shall be 0.01 or less without credit for backup electrical power**

Information Sufficient to Perform a Reliability Assessment for HVAC / HEPA System

- Ventilation flow diagrams (VFDs)
- Ventilation and instrumentation diagrams (V&IDs)
- Process and instrumentation diagrams
- Electrical single lines
- Control logic diagrams
- Schematic / block diagrams
- Supporting calculations and analyses

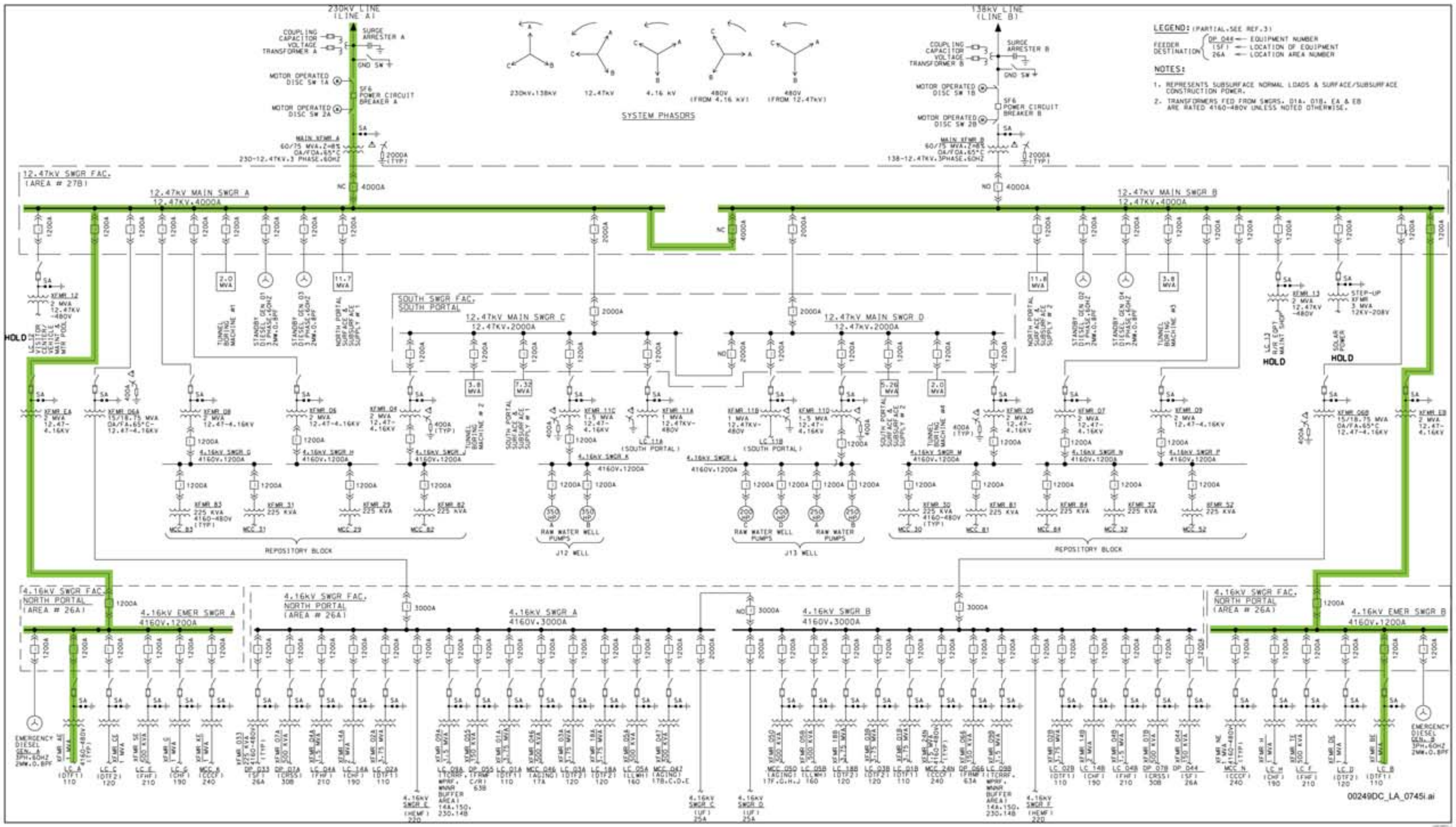
Demonstration of Safety for HVAC / HEPA System in License Application

- **Basis of design document that defines safety / design requirements and safety functions**
- **HVAC / HEPA System VFDs (and where appropriate V&IDs)**
- **P&IDs that identify flow rates, duct / damper arrangements, major equipment configuration, and controls for the HVAC system**
- **Functional logic diagrams for the HVAC / HEPA system that present the controls and control logic for each of the safety functions**

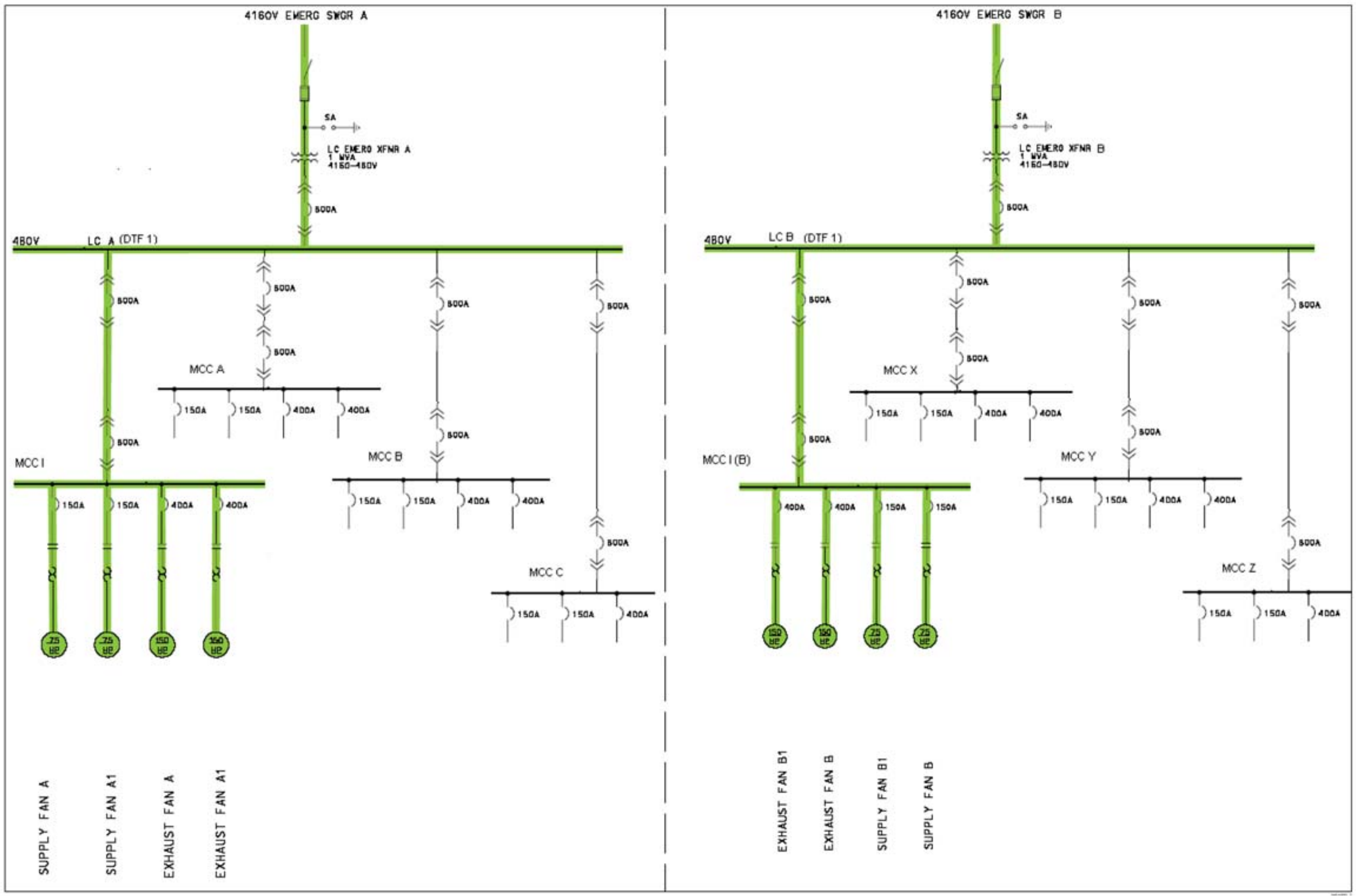
Demonstration of Safety for HVAC / HEPA System in License Application (cont.)

- **System Description Document and Facility Description Document that provide description of the HVAC / HEPA system controls, equipment, and operations**
- **Nuclear radiation and contamination zone drawings for the facility served by the HVAC / HEPA system**
- **Mechanical equipment sizing and heating / cooling calculations**

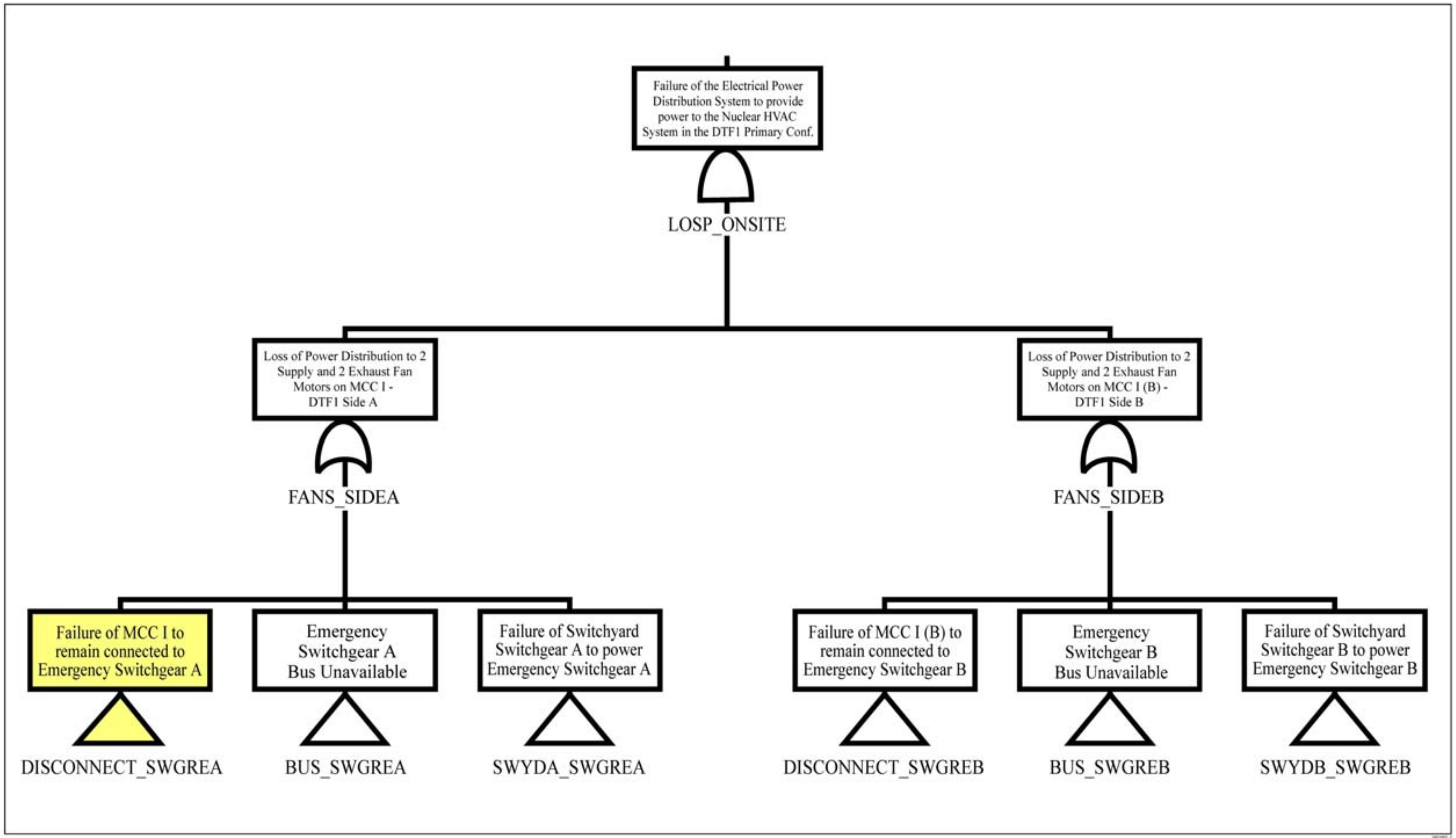
Example: Level of Detail for Electrical Single Line



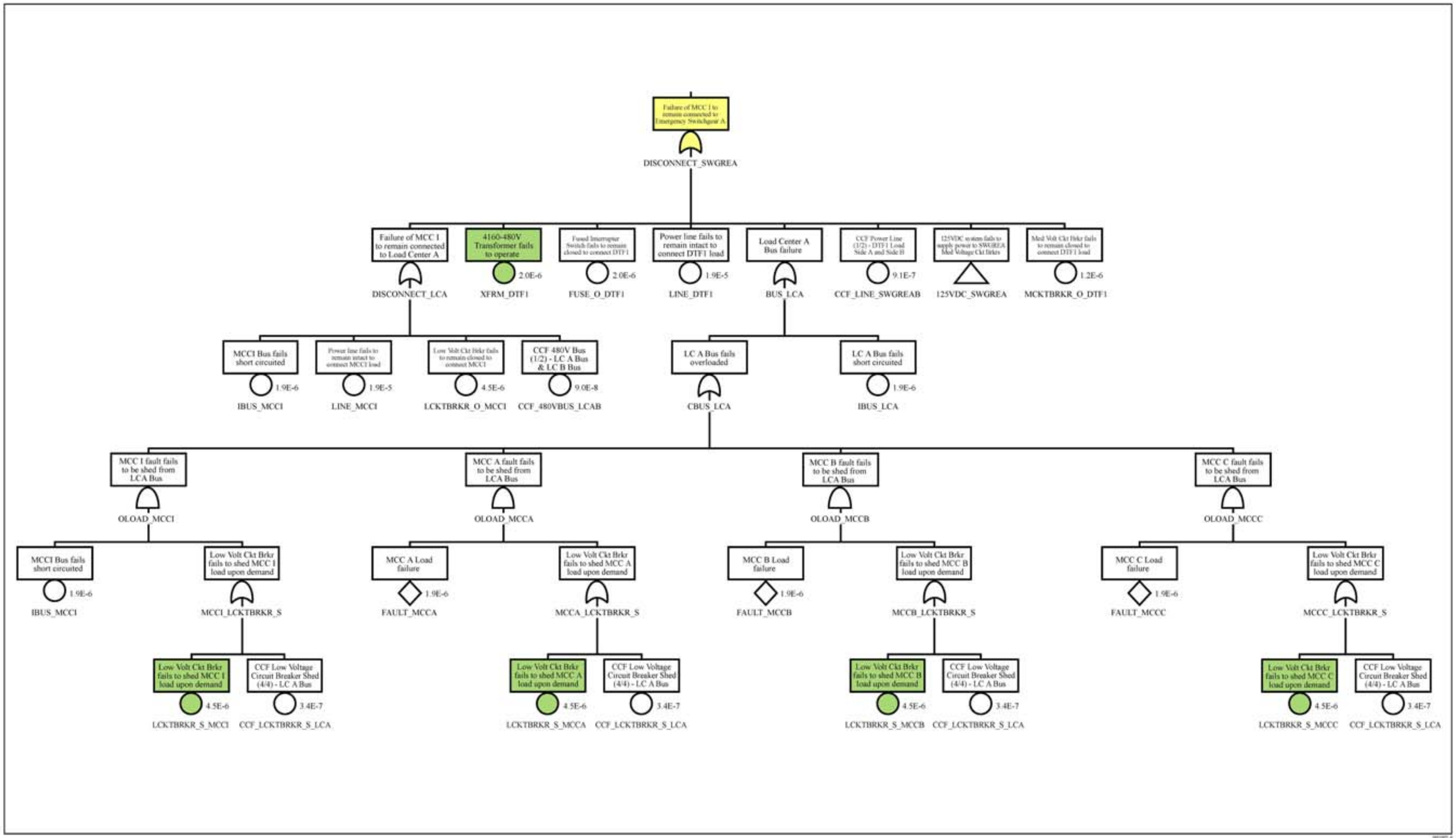
Example: Level of Detail for ITS Power from Load Center



Example: Electrical Power Distribution Fault Tree



Example: Subtree for Electrical Power Distribution MCC Failure

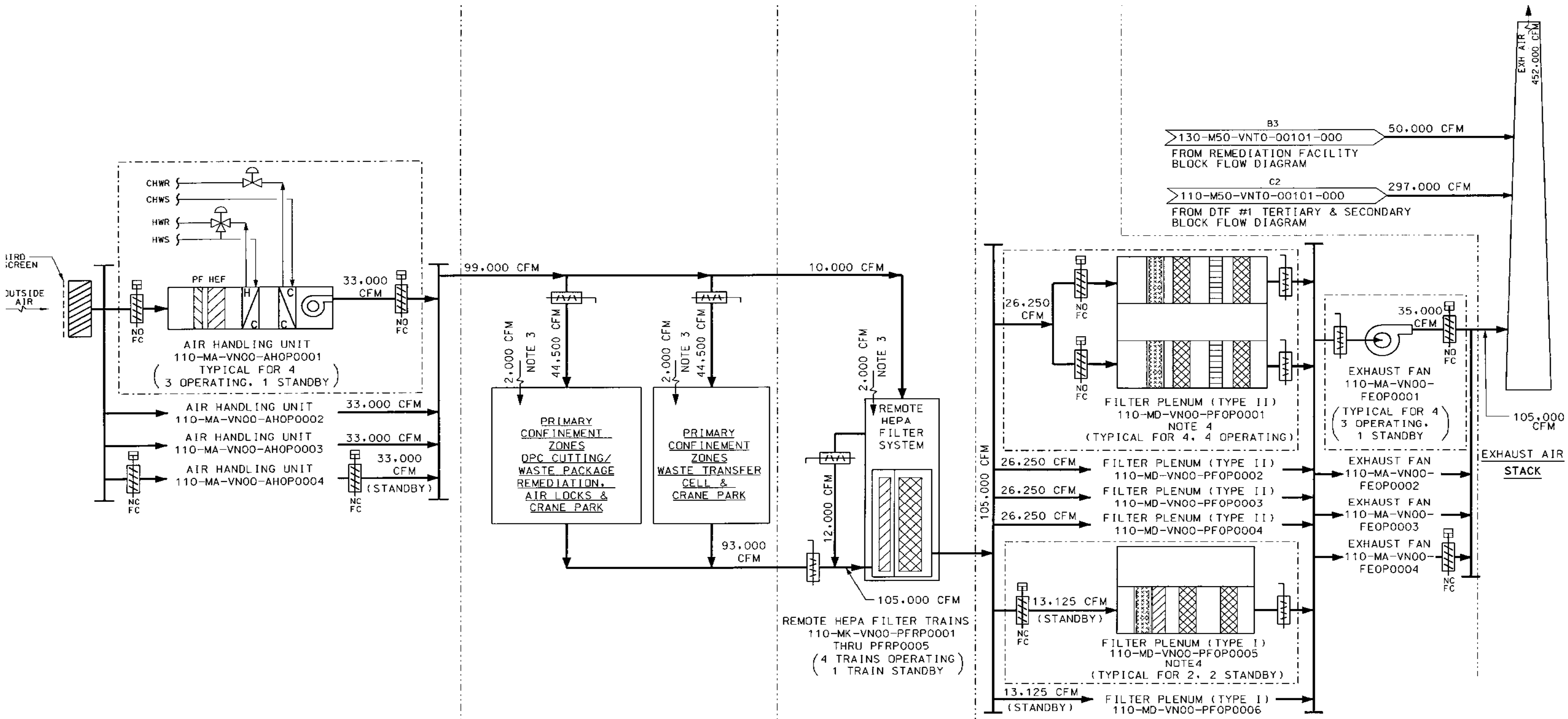


MCC = Motor Control Center

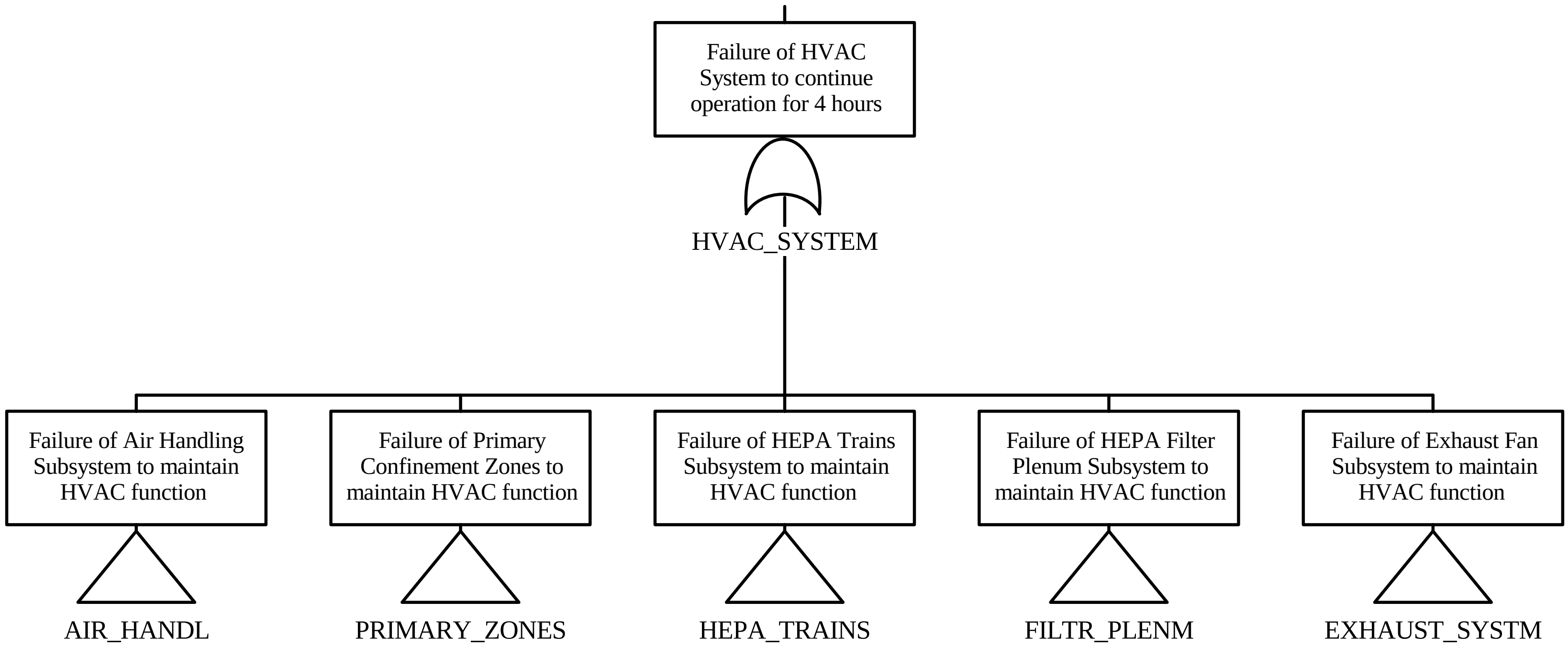
Industry Data Used to Assess Fault Tree

Component/ Subsystem Type	Failure Mode	Failure Rate	Unit	Data Source	Reference	Basis for Probability	Probability of Basic Event in FT Model	Comment
Substation Transformer Liquid Filled, 3 phase 146 -242kV	Fails to operate	2.23×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 392	λt	8.92×10^{-06}	Used for 230kV-12.47kV Main Transformer A
Substation Transformer Liquid Filled, 3 phase 73-145kV	Fails to operate	1.24×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 391	λt	4.96×10^{-06}	Used for 138kV-12.47kV Main Transformer B
Transmission Tie Transformer - Liquid Filled, 3 phase 2-30kV	Fails to operate	0.49×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 372	λt	1.96×10^{-06}	Used for 12.47kV - 4.16kV Transformer and 4.16kV - 480V Transformer
Power Cables	Fails to conduct power	4.84×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 747	λt	1.94×10^{-05}	Used for all Internal Power Lines
Bus Duct 480V, 3phase 100 -1600 Amps	Fails short circuited	0.48×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 797	λt	1.92×10^{-06}	Used for LCA, LCB, and all MCC Buses
Bare Buses, Outdoor Switchgear	Fails short circuited	0.26×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 804	λt	1.04×10^{-06}	Used for Main SWGR A and B, Emergency Switchgear A and B, and 125V DC Distribution Bus A and B
Metal Clad Drawout Circuit Breaker Above 600 Amps	Fails to close Fails to shed Fails to connect	0.30×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 146	λt	1.20×10^{-06}	Used for Medium Voltage Circuit Breakers
Molded Case Circuit Breaker	Fails to close Fails to shed Fails to connect	1.13×10^{-06}	h^{-1}	IEEE Std 500 - 1991	p. 124	λt	4.52×10^{-06}	Used for Low Voltage Circuit Breaker

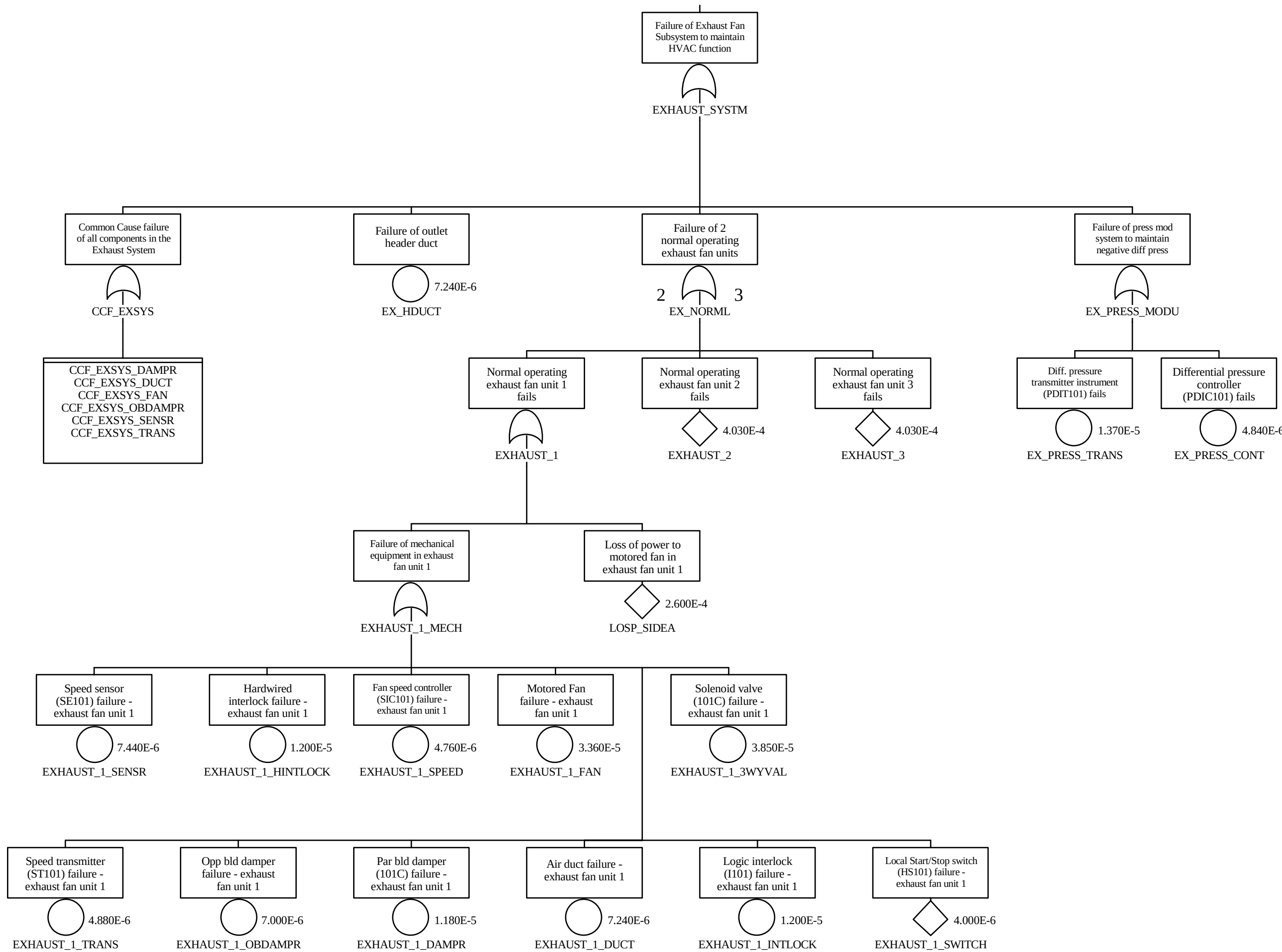
Example: Surface Nuclear HVAC System (Illustrative only)



Fault Tree Model of the Surface Nuclear HVAC System



Fault Tree Model - Subtree for the HVAC Exhaust Fan Subsystem



Industry Data Used to Assess Fault Tree

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^{-1}	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^{-1}	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^{-1}	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^{-1}	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^{-1}	Eide & Calley 1993, p. 1178	λt	1.20×10^{-06}	
Switch, general	Spurious operation	1.00×10^{-06}	h^{-1}	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^{-1}		q	1.00×10^{-05}	
Air Filter	Plugs	1.00×10^{-05}	h^{-1}	Eide & Calley 1993, p. 1178	λt	4.00×10^{-05}	Used for Clogged HEPA Filter
Heat Exchanger	Plugs	3.40×10^{-06}	h^{-1}	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^{-1}	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^{-1}	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^{-1}	IEEE Std 500-1984 (Reaffirmed 1991), p. 527	λt	6.92×10^{-06}	Used for smoke detector

Example: Nuclear Design Bases Reliability Requirements for Trolley

- **Important to Safety**
  - Waste package trolley
- **Nuclear Safety Design Bases Requirement**
  - Upon a loss of power, this trolley shall be designed to stop, retain its load, and enter a locked mode; upon a restoration of power, this trolley shall stay in the locked mode until operator action is taken
  - The trolley shall be designed with an inherent speed limit such that a collision at the trolley speed limit would not cause the trolley to drop its load

Information Sufficient to Perform a Reliability Assessment on Transfer Trolley

- **Basis of design document that defines the safety design requirements and safety functions**
- **Mechanical equipment envelope drawings**
- **P&IDs that identify the principal controls on the trolley**
- **Functional control logic diagrams for the trolley that present the controls and control logic for each of the trolley safety functions**

Information Sufficient to Perform a Reliability Assessment on Transfer Trolley (cont.)

- **System Description Document and Facility Description Document**
- **Specification for the trolley**
- **Mechanical handling design reports**
- **Mechanical handling calculations that define the space envelope, load paths, load drops, and interactions with other systems, components, and structures**

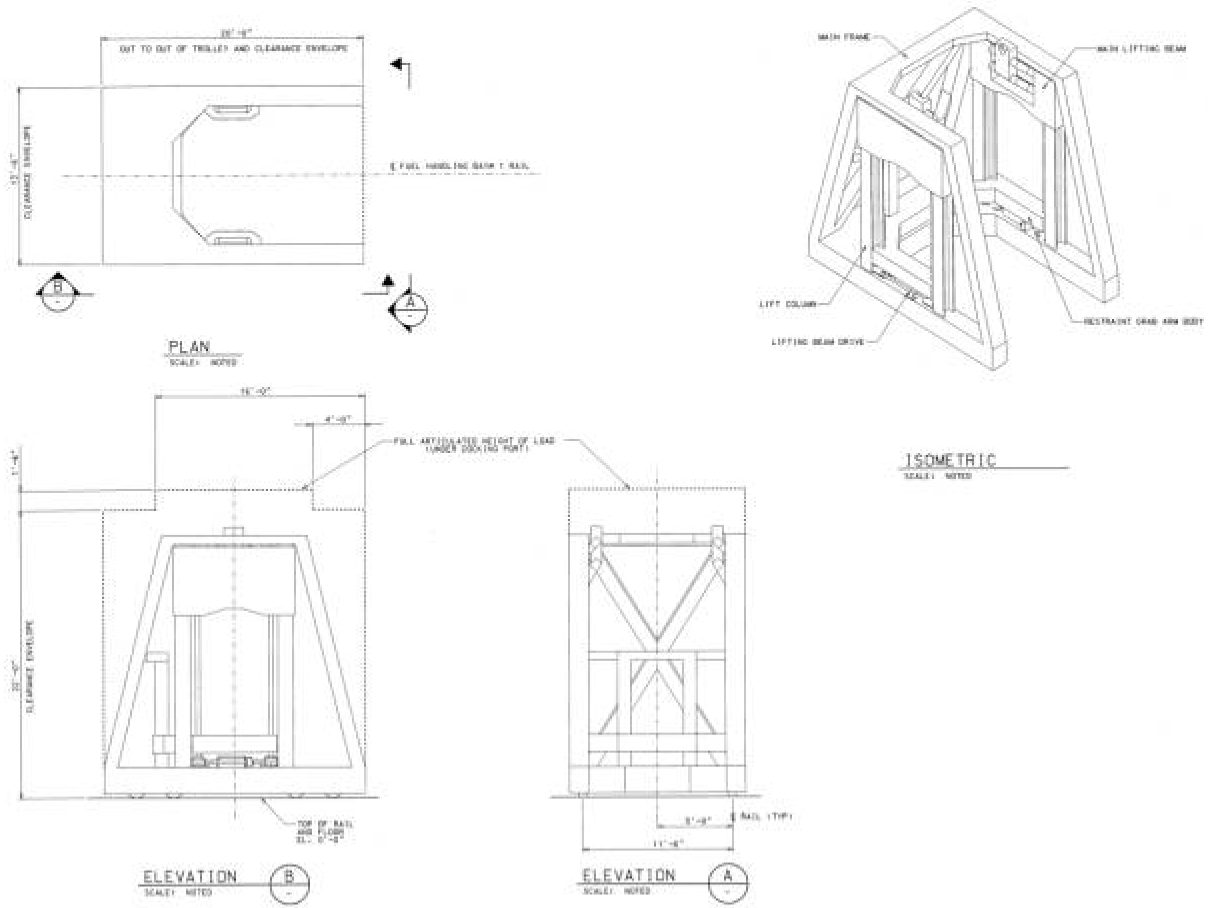
Transfer Trolley Design Information in License Application

- **Basis of design document that defines the safety design requirements and safety functions**
- **Mechanical handling design reports**
- **Mechanical equipment envelope drawings**
- **P&IDs that identify the principal controls on the trolley**
- **Functional logic diagrams for the trolley that present the controls and control logic**

Transfer Trolley Design Information in License Application (cont.)

- **System Description Document and Facility Description Document**
- **Mechanical handling calculations that define the space envelope, load paths, load drops, and interactions with other systems, components, and structures**
- **Trolley specification**

Transfer Trolley for Waste Package (Illustrative example only)



Fault Tree Analysis of Transfer Trolley

- Electrical and mechanical design details will be analyzed similar to the level of detail performed for the HVAC / HEPA system to assess the probability of system failure
- Industry reliability data will be used for subsystems and components
- Fault tree evaluation will be compared to nuclear safety basis reliability requirements
- Uncertainties considered
- Reliability evaluation based on design detail demonstrates compliance with the safety requirements

Summary

- **The examples presented demonstrate how safety requirements are implemented in the design**
- **A sufficient level of design detail will be developed to support assessment that systems and components can achieve required reliability requirements**
- **The Preclosure Safety Analysis (PCSA) process, following an iterative approach and development of appropriate design detail, ensures compliance with safety requirements**