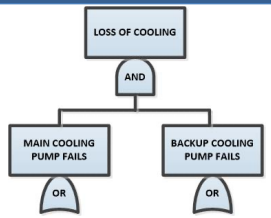
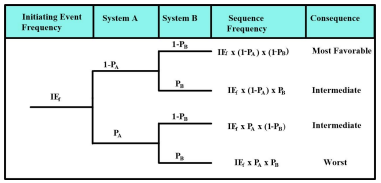


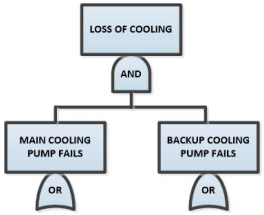
Fault Tree Analysis Session 2 of 4



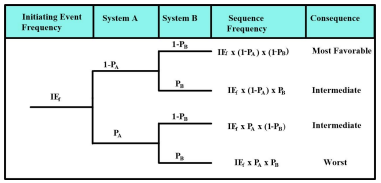
Present fault tree analysis basics with examples and case studies

Howard Lambert
FTA Associates

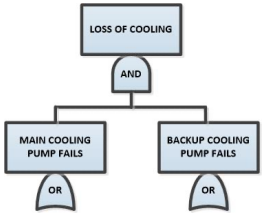
2022



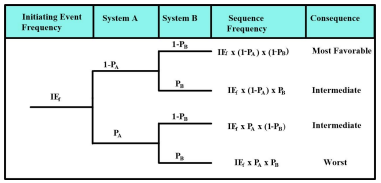
Possible Steps in Fault Tree Analysis



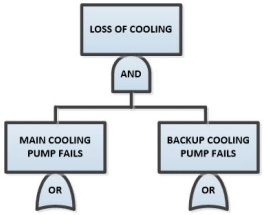
1. Define the Undesired Event/Top Event
2. Acquire an Understanding of the System
3. Establish Scope and Bounds of the Analysis
4. List Assumptions
5. Construct the Fault Tree
6. Perform Qualitative Evaluation
    1. Find Single point failures
    2. Find Min cut sets
    3. Find Common cause failures



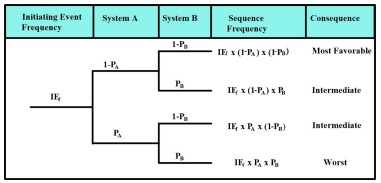
Possible Steps in Fault Tree Analysis Continued



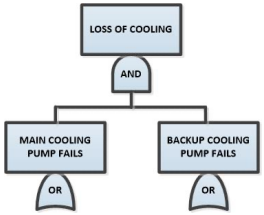
7. Perform Quantitative (Probabilistic Analysis)
   1. Compute Probability/Frequency of the top event
   2. Compute Importance of basic events/min cut sets as an example of sensitivity analysis
8. Conduct Tradeoff Studies
9. Make Decisions and Recommendations
10. Document Results
11. Conduct Uncertainty Analysis
12. Perform Peer Review



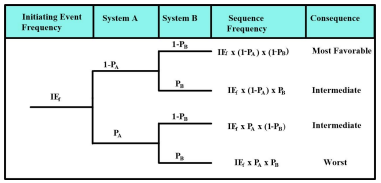
Fault Tree Analysis Topics



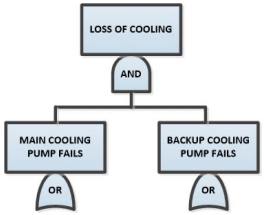
- Engineering Design Tool
- Logic Rules
- Historical Concepts
- Levels of Fault Tree Development
- Logic Gates OR, AND, Combination -- other logic gates
- Fault Tree Construction Rules
  - Type 1 fault events
  - Type 2 fault events
- Redundancy
  - System level
  - Component level



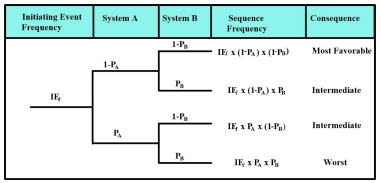
Fault Tree Analysis Topics Continued



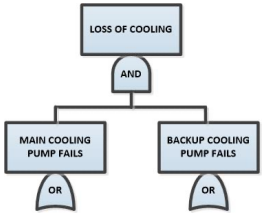
- Min Cut sets
- Common Cause Failure Analysis
- Human Reliability Assessment
- Initiating and enabling events
- Success Criteria



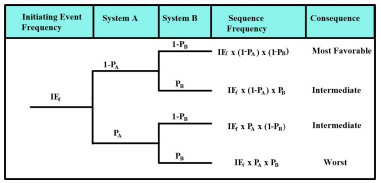
Evolution of Fault Tree Analysis in the beginning …



- Minuteman Launch Control System (1962)
  - Fault Tree Analysis Evolved (Bell Labs, improved by Boeing)
  - Precursor Events
    - Missile explosions on launch pad
    - Lightning Strike
  - Undesired Events
    - Failure to Launch Upon demand (type 1 fault event)
    - Inadvertent Missile Launch (type 2 fault event)
    - Missile Blows up on launch pad (type 2 fault event)
  - System attributes
    - Complex
    - Many modes of failures
    - Malfunction of system can cause substantial injury or harm
    - Little operational experience

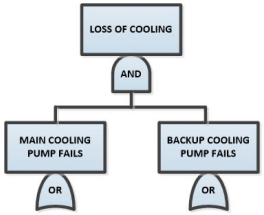


Failure Modes and Effects versus Fault Tree Analysis

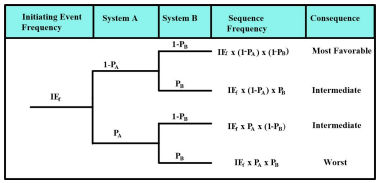


- Minuteman Launch Control System (1962) disadvantage to FMEA (no. of failure combinations)

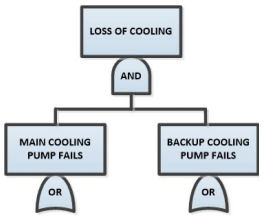
Number of components	doubles	triples	quadruples
100	5,000	162,000	3,900,000
500	125,000	20,000,000	2.6 E+9
1000	500,000	170,000,000	4.1 E+10



Minuteman Launch Control FTA



- What is the credible worst case scenario?
- Reliability Goal Inadvertent Launch
  —1.0 E-9 per year



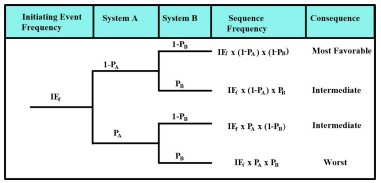
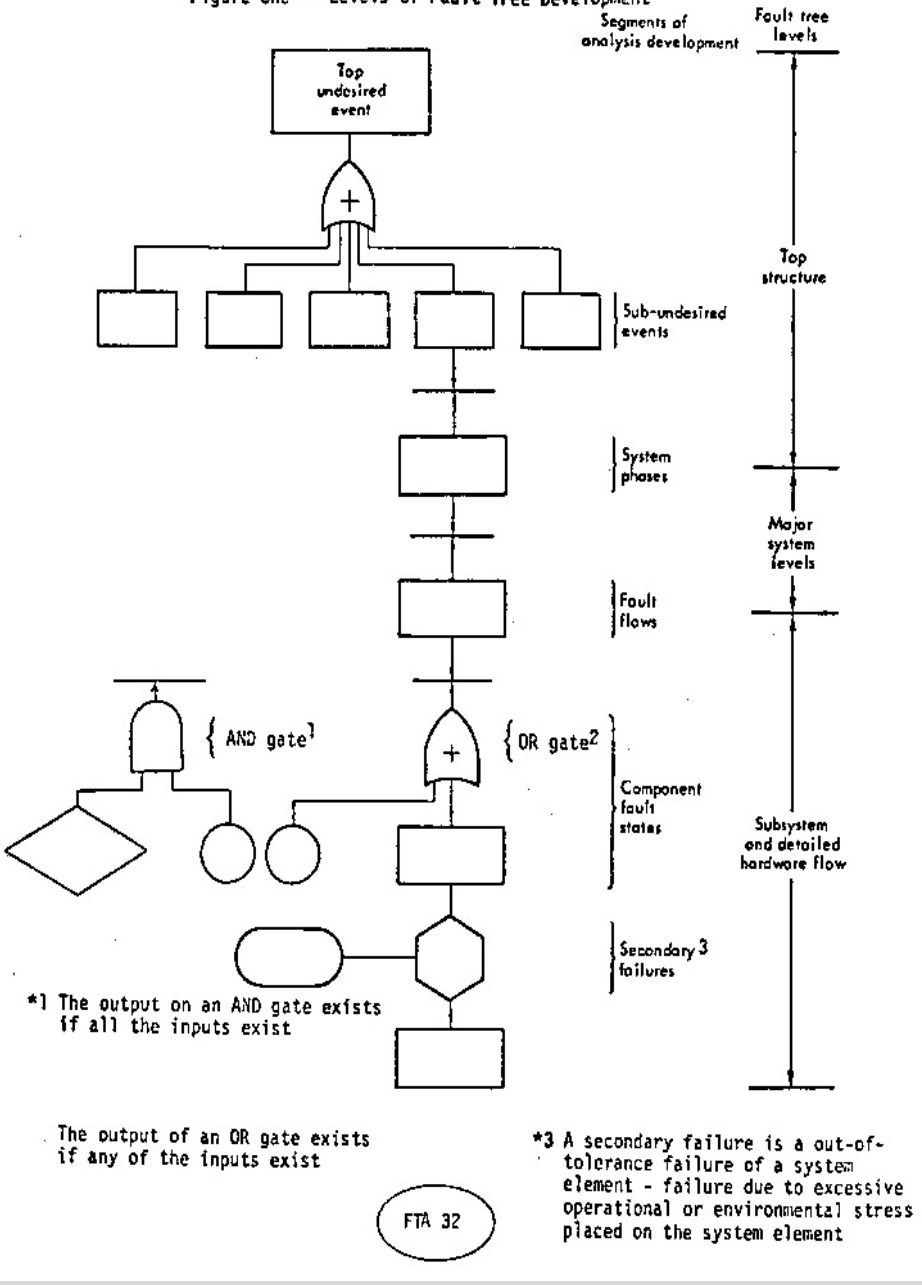
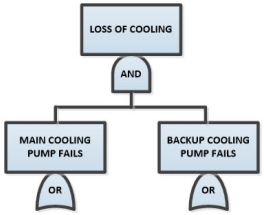


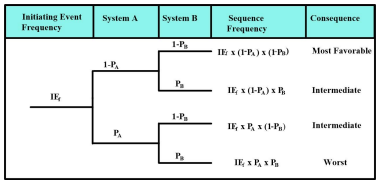
Figure One -- Levels of Fault Tree Development



FTA – Levels of Development



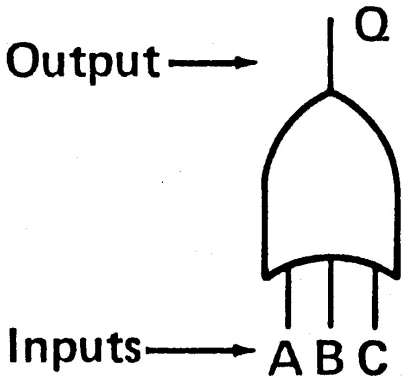
FTA -- Event Representation



A. Introduction
   1. Algebraic relationships
   2. Algebraic symbols for events; A, B,… etc.
   3. A means event A occurs,

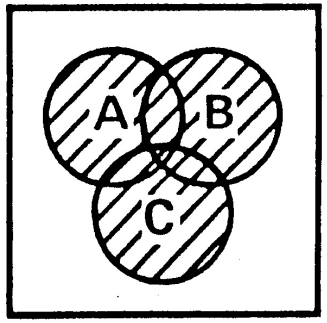
$\bar{A}$ Means that event A has not occurred

B. OR gate representation



The event Q occurs if either events A, B or C exist

OR

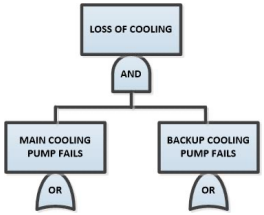


Mutually inclusive OR gate

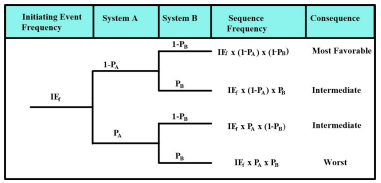
Q = A + B + C

+ denotes logical union

Venn diagram

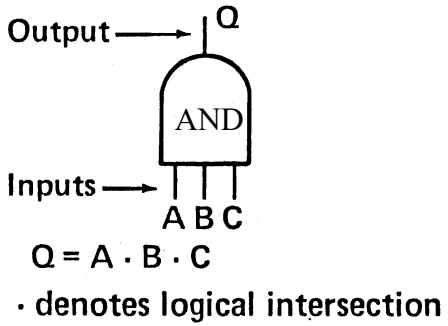


FTA – Fault Tree Events

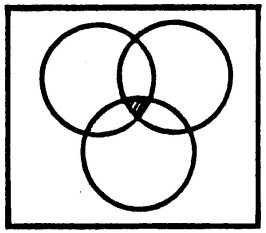


Event Representation (cont.)

C. AND gate representation

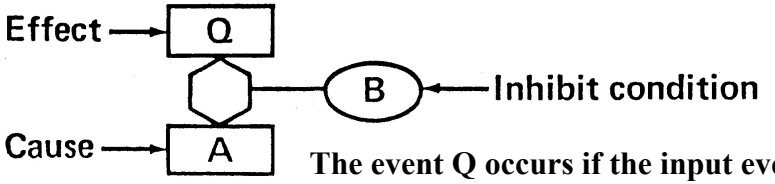


The event Q occurs if either events A, B or C exits

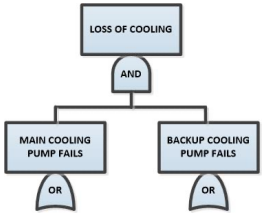


Venn diagram

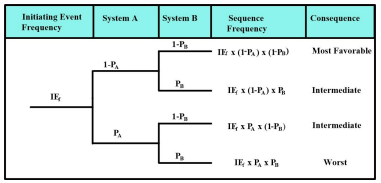
D. Inhibit gates



The event Q occurs if the input event A and the the conditional event B occur

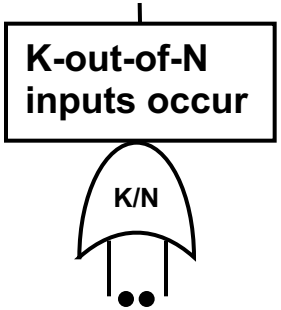


K-out-of N logic Gates

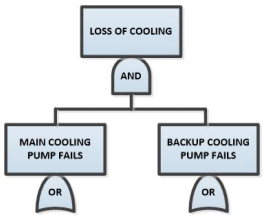


K-out-of-N

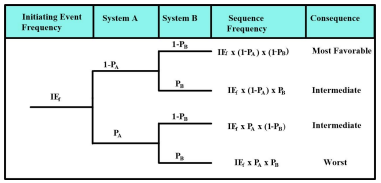
Combination



N possible inputs

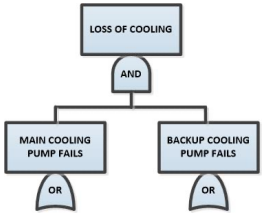


FTA -- Fault Tree Event Representation (cont.)

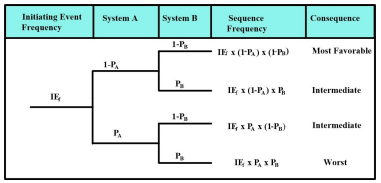


E. Event symbols

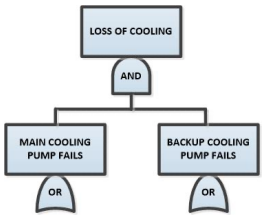
Symbol	Event description
Rectangle	Gate event
Circle	Primary failure (basic event)
Diamond	An event not further developed (basic event)
Oval	Conditional event
House	Normal event



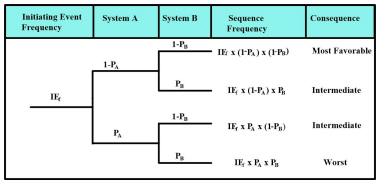
FTA -- Logic Gates From Event Viewpoint



- Simple rule to determine the logic gate to use: “If the event considered by itself can cause the next higher event to occur, use an OR gate.”
- In the case of the AND gate, input events are necessary and sufficient events to cause the output event to occur.



Example of AND gate and Inhibit gate conditions for fire aboard a plane



FIRE CAUSED BY ATOMIZED HYDRAULIC FLUID LEAK WITH IGNITION SOURCE PRESENT

AND

FUEL SOURCES:
JET FUEL
ENGINE OIL
HYDRAULIC FLUID

OXYGEN CONCENTRATION ABOVE MOC

TRUE

HIGH PRESSURE LEAK OF HYDRAULIC FLUID CREATES A COMBUSTIBLE MIXTURE

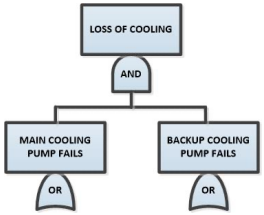
HYDRAULIC FLUID UNDER HIGH PRESSURE CAUSES FLUID TO ATOMIZE

PRESSURE FITTINGS BETWEEN PUMP AND SOLENOID LEAK [1000 -1500 PSI]

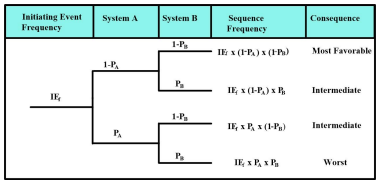
IGNITION SOURCES CAUSES THE ATOMIZED HYDRAULIC FLUID TO BURN

POTENTIAL IGNITION SOURCES (ELECRTICAL SPARK OR HEAT SOURCE)

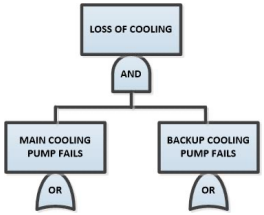
TRANSFER FROM SHEET 2



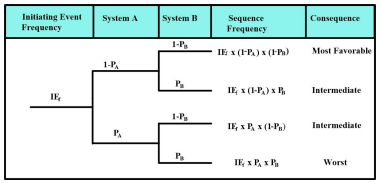
Fault Tree Construction



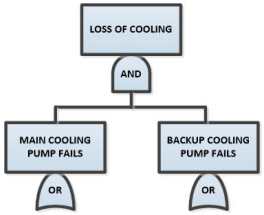
- Immediate Cause Principle --One step process (Used to develop fault events) traditional FTA
  - —Examples
    - Light bulb
    - Fire and Explosion
      - –B341 (Hydrogen Deflagration 1976)
      - –FAA Flammability rule (TWA 800)
      - –Heated wire example (published 1965)
    - Apollo 13



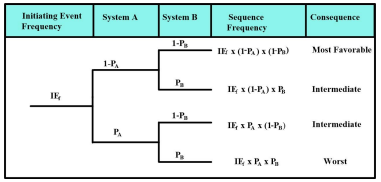
Fault Tree Construction Continued



- Directed Graphs (Two step process) Used for FTA of control systems
  - —DuPont Chlorine Vaporizer Example
  - —Precipitate Hydrolysis Savanah River Site
  - —Safeguards Analysis



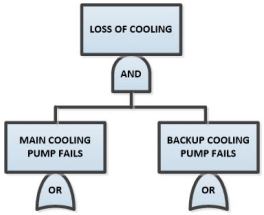
FTA -- Construction Rules Immediate Cause Principle



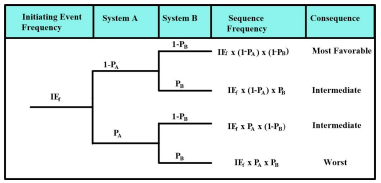
1. Write the **what** and **when** portion of the fault statement.

2. Determine if the event is a **state-of-component fault event** or **state of system fault event**.

   If the fault event can consist of a simple failure of the component, then the event is a **state-of-component fault event**. Otherwise, the fault event is **state-of-system fault event**.

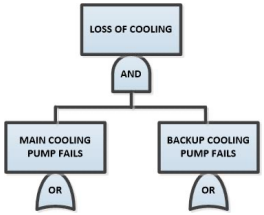


FTA -- Construction Rules (cont.) Immediate Cause Principle

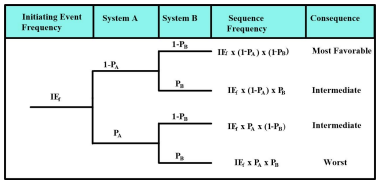


3. If the fault event is a state-of-component fault event, then an OR gate is used at an immediately lower level to combine the inputs that consist of three causes, (1) a **primary failure** (2) a **secondary failure** or (3) a **command fault**.

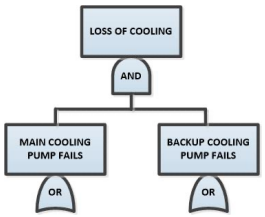
   If the fault event is a **state-of-system fault**, the fault event is preceded at a lower level by an AND gate, an OR gate, an inhibit gate, or no gate at all. To determine which gate to use, we must specify the minimum necessary and sufficient fault input events for the output event to occur.



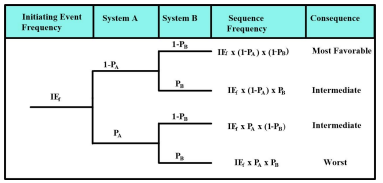
FTA -- Failure Causes of a "State-of-Component" Fault

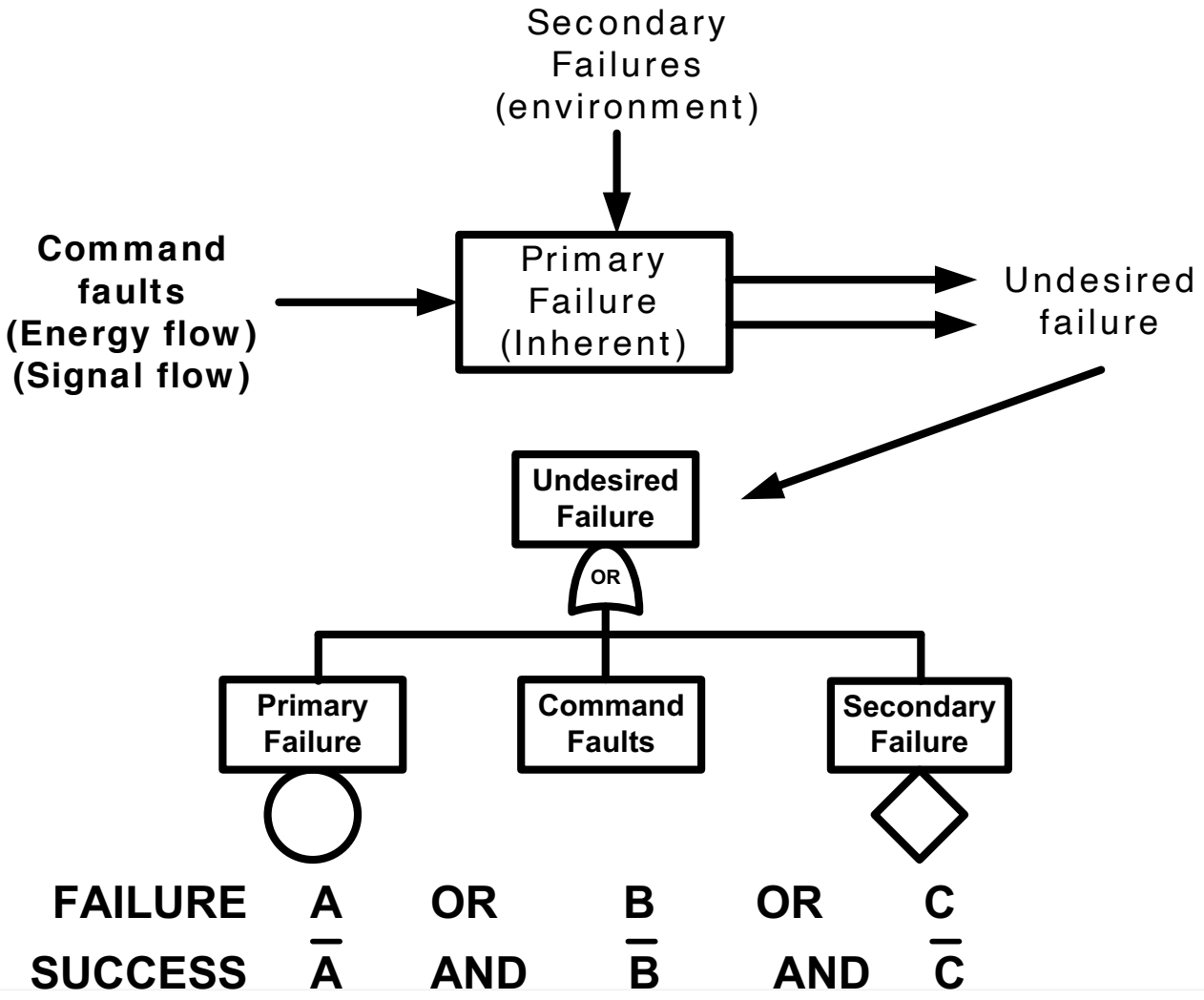


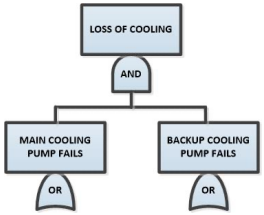
- A primary failure is a failure of a component within the design envelope, i.e., failure due to the inherent characteristics of the system element under consideration in the fault event – a random failure in reliability
- A secondary failure is a failure of a component outside the design envelope, i.e., failure due to excessive environmental or operational stresses placed on the component.
- A command fault is inadvertent operation or non-operation of a component due to failure of external inputs such as energy and/or signal flow necessary for the component to function



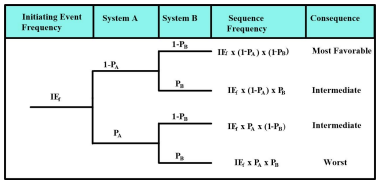
FTA -- Failure causes of a "State-of-Component" Fault Primary, and Secondary Failures Command Faults



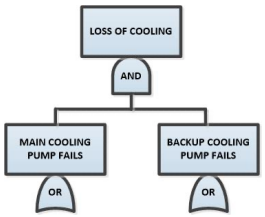




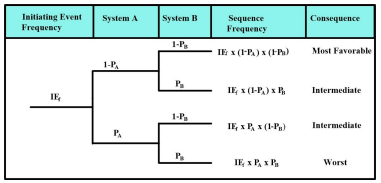
Fault Tree Construction Continued



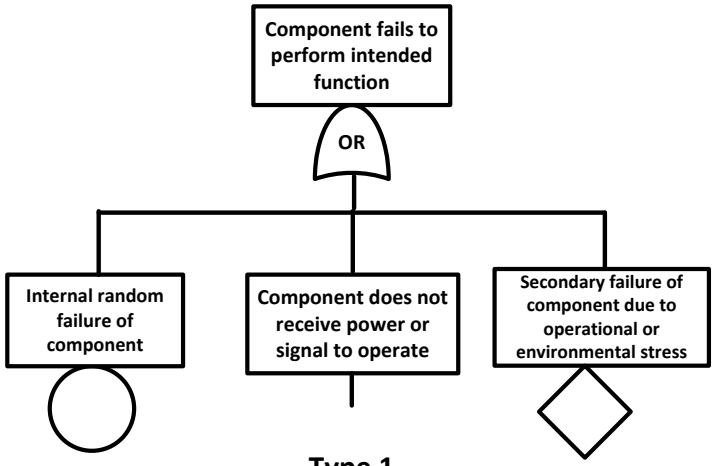
- Fault Tree Operators for two types of fault events
  - Type 1 fault event component does not perform its intended function
  - Type 2 fault event for component works inadvertently (normal operation at the wrong time)



State of Component Operator for Two Types of Fault Events

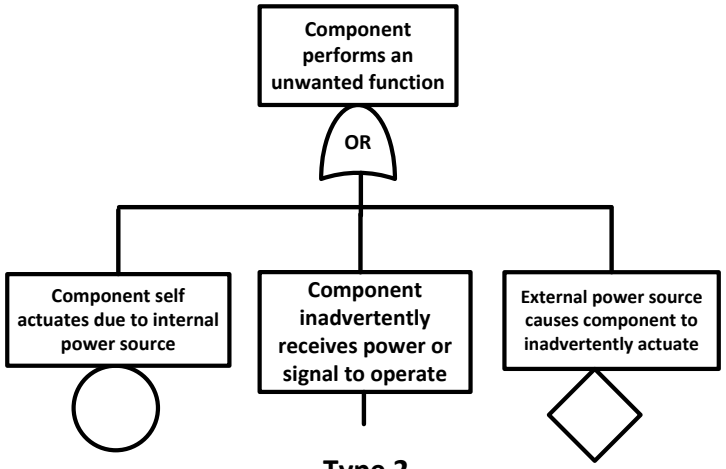


STATE OF COMPONENT OPERATOR FOR TYPE 1 COMPONENT FAILURES



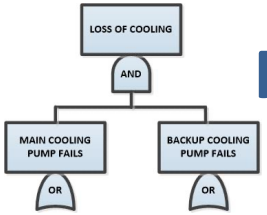
Type 1 command fault

STATE OF COMPONENT OPERATOR FOR TYPE 2 COMPONENT FAULTS

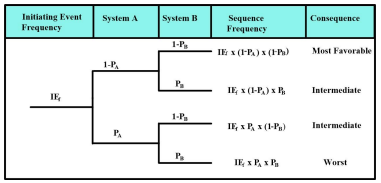


For example include components that contain springs, power supplies gas or gas bottles otherwise excluded from consideration

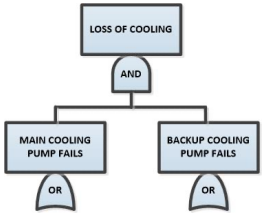
Type 2 command fault



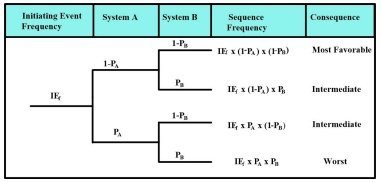
FTA -- Example of Structuring Process -- Immediate Cause Principle

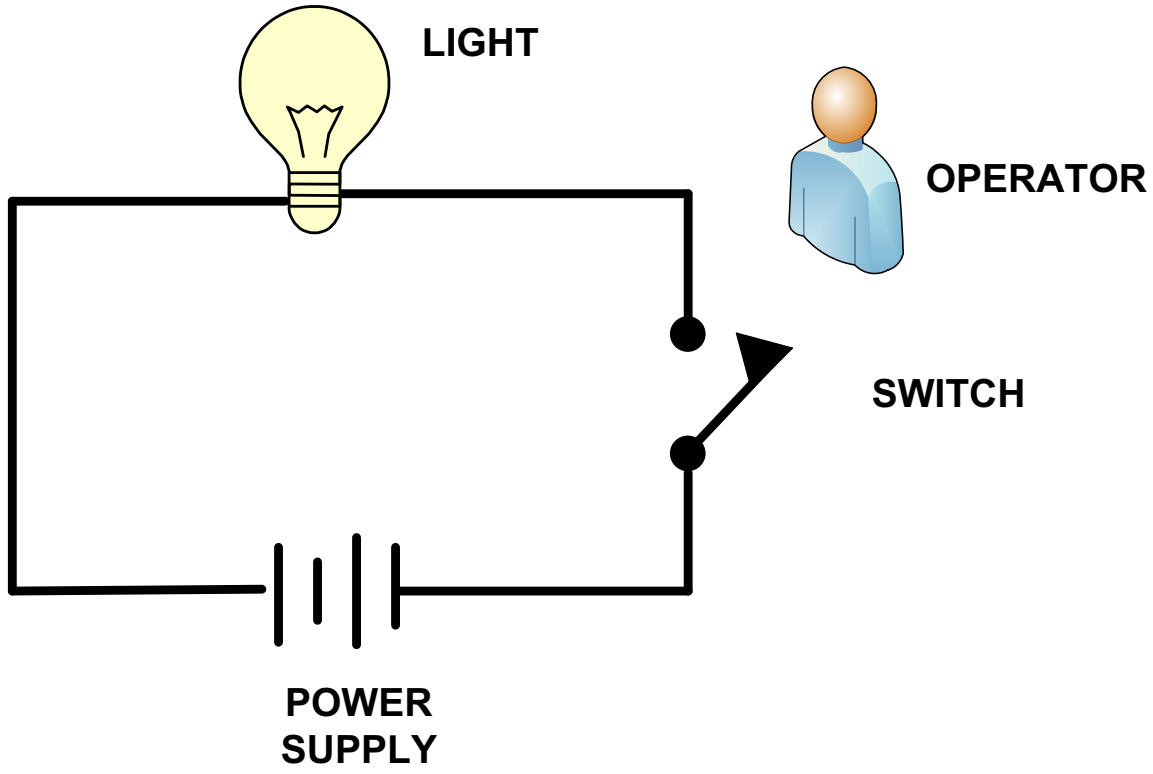


- At the beginning of each working day, the operator is instructed to close a switch while starting up the reactor to signify the reactor is ON. At the end of the working day during shutdown, the operator opens the switch. The switch provides current to a warning light located at the entrances to the room where the reactor is located.
- Circuit is shown on the next slide

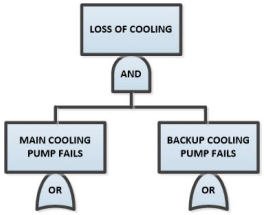


LIGHT BULB SYSTEM

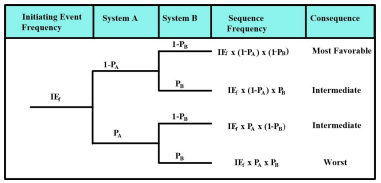




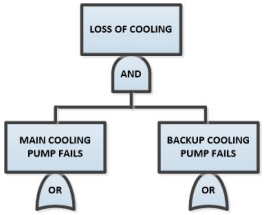
SYSTEM A – SIMPLE SYSTEM



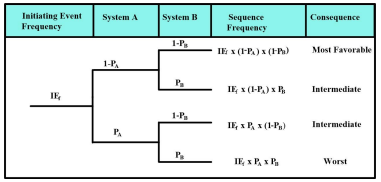
FTA – Event Types



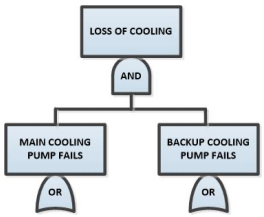
- Consider the following fault events. Assume wires do not contribute to system failure. Determine the event type (i.e., state of component or state of system) –
  1. Switch closed after reactor shutdown
  2. Switch open when reactor is operating
  3. Light on when reactor is shutdown
  4. Light off when reactor is operating

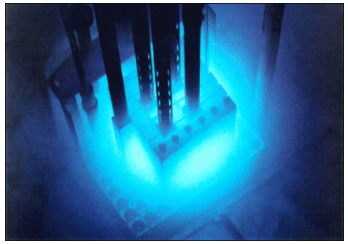


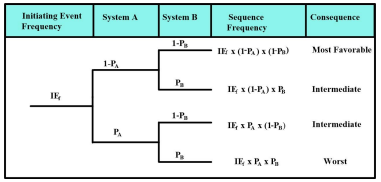
Fault tree example

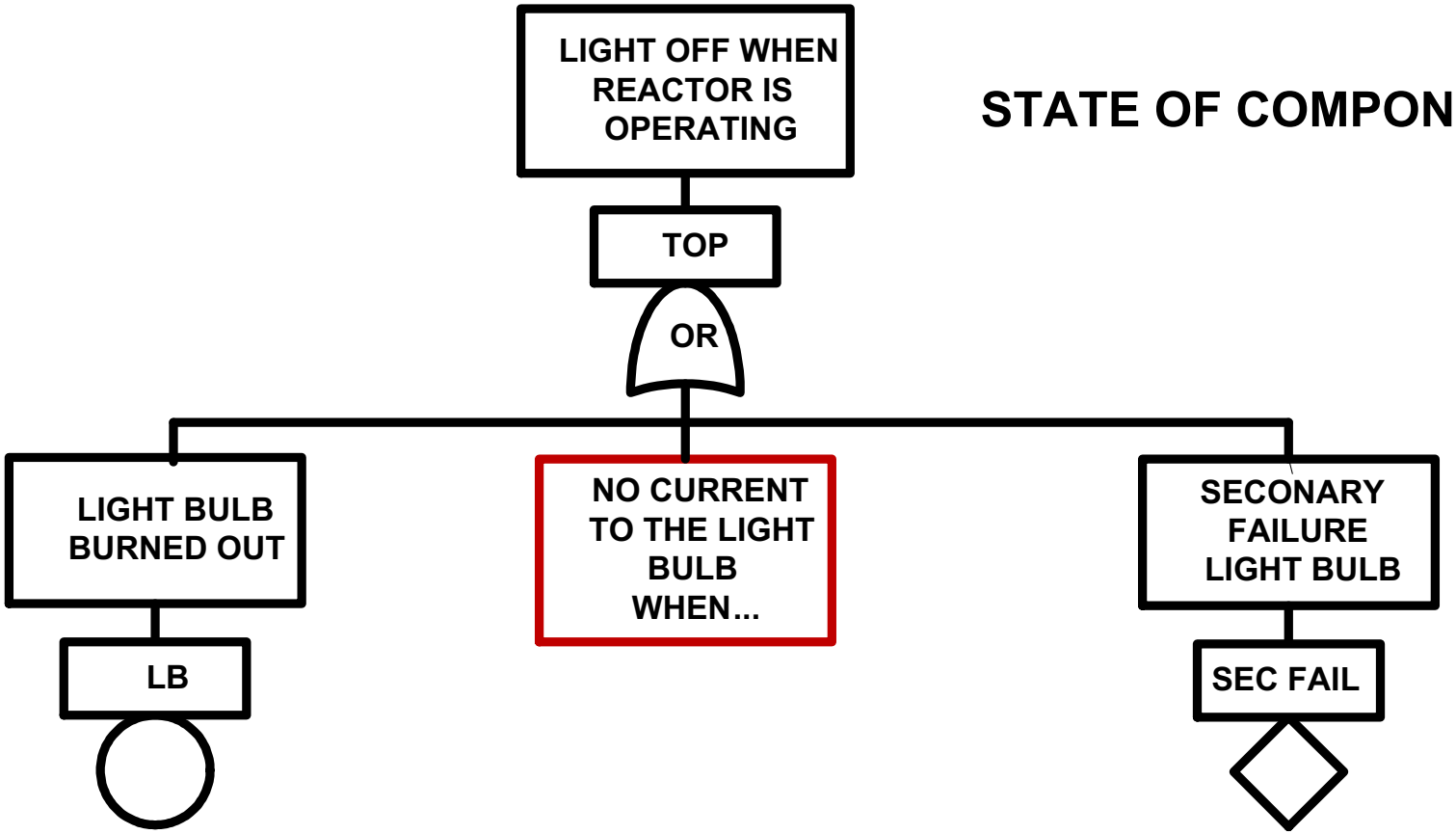


- TOP EVENT -- LIGHT OFF WHEN REACTOR IS OPERATING
- Scope – internal events only
- Assumptions – connector reliability unity
- Failure modes (Active components only)
  - Light
    - light bulb burned out
  - Switch
    - Fails to close
    - Fails to open
  - Operator
    - Fails to close switch (or inadvertently opens the switch)
    - Fails to open switch (or inadvertently closes the switch)
  - Power Supply
    - Fails off

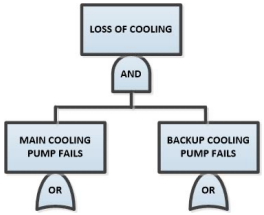


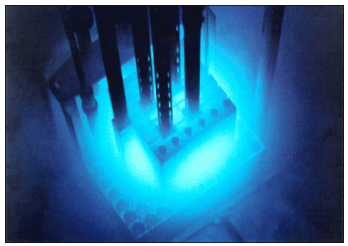


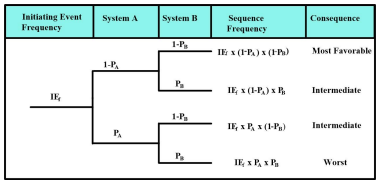


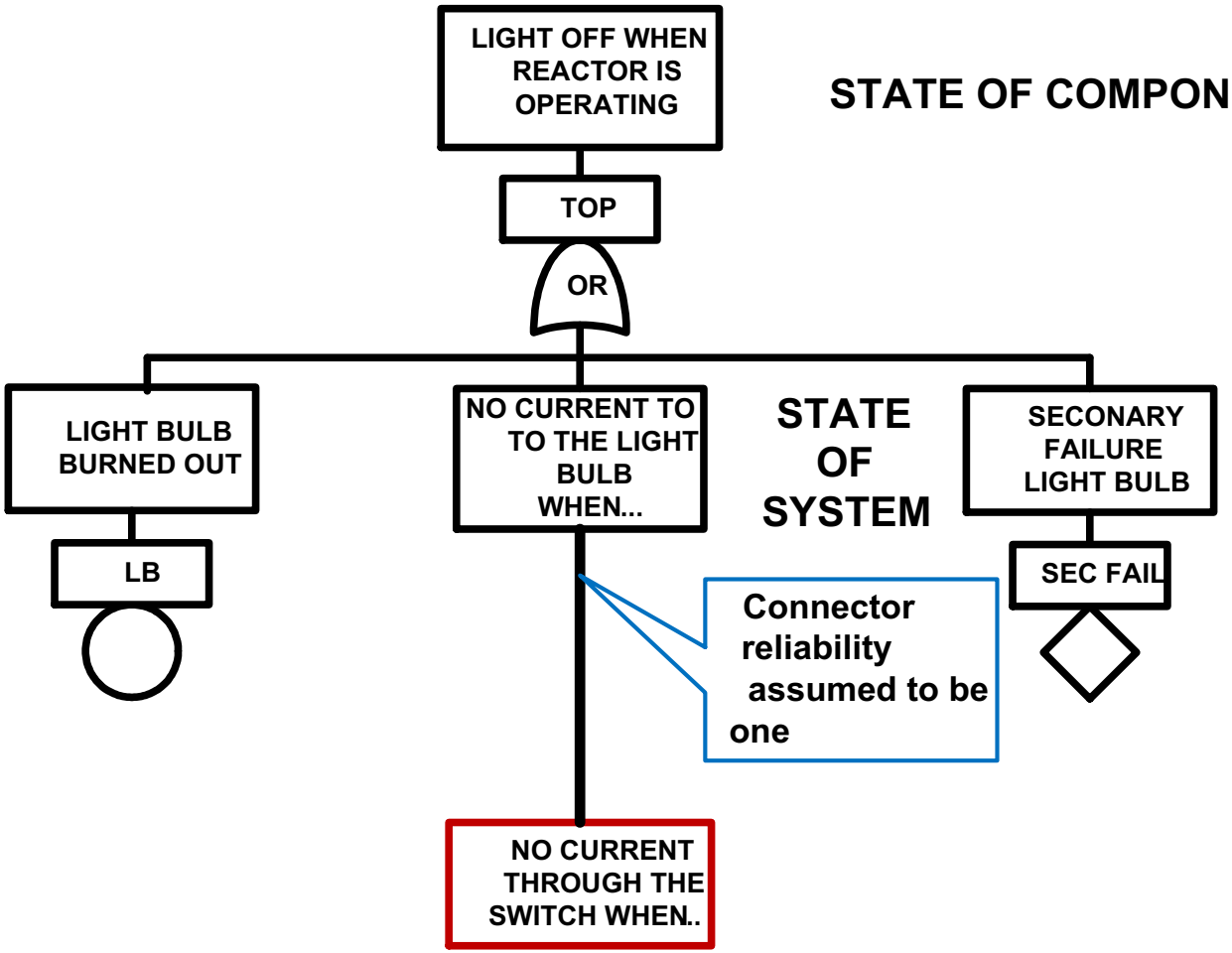


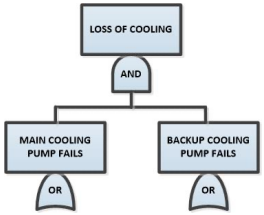
STATE OF COMPONENT

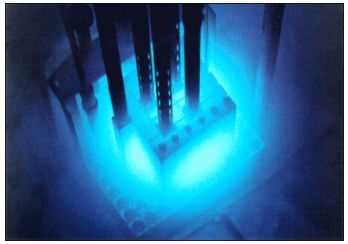

LOSS OF COOLING
AND
MAIN COOLING PUMP FAILS
BACKUP COOLING PUMP FAILS
OR
OR

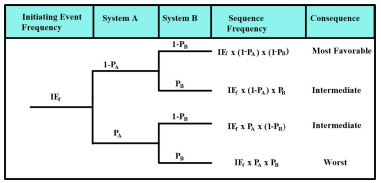



Initiating Event Frequency
System A
System B
Sequence Frequency
Consequence
1-P_B
IE_I x (1-P_A) x (1-P_B)
Most Favorable
1-P_A
P_B
IE_I x (1-P_A) x P_B
Intermediate
IE_I
1-P_B
P_A
IE_I x P_A x (1-P_B)
Intermediate
P_B
IE_I x P_A x P_B
Worst


LIGHT OFF WHEN REACTOR IS OPERATING
TOP
OR
LIGHT BULB BURNED OUT
LB
NO CURRENT TO TO THE LIGHT BULB WHEN...
STATE OF SYSTEM
SECONARY FAILURE LIGHT BULB
SEC FAIL
Connector reliability assumed to be one
NO CURRENT THROUGH THE SWITCH WHEN..
STATE OF COMPONENT







SUCCESS CRITERIA FOR THE SWITCH TO CARRY CURRENT

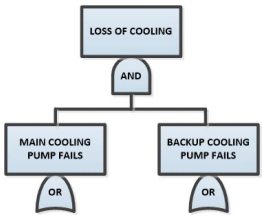
1. SWITCH CONTACTS ARE CLOSED
AND
2. CURRENT TO THE SWITCH

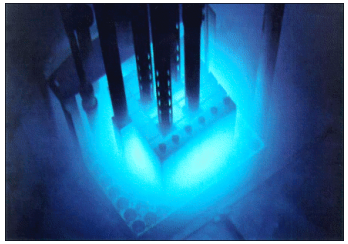
FAILURE

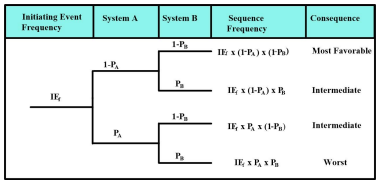
1. SWITCH CONTACTS ARE OPEN
OR
2. NO CURRENT TO SWITCH

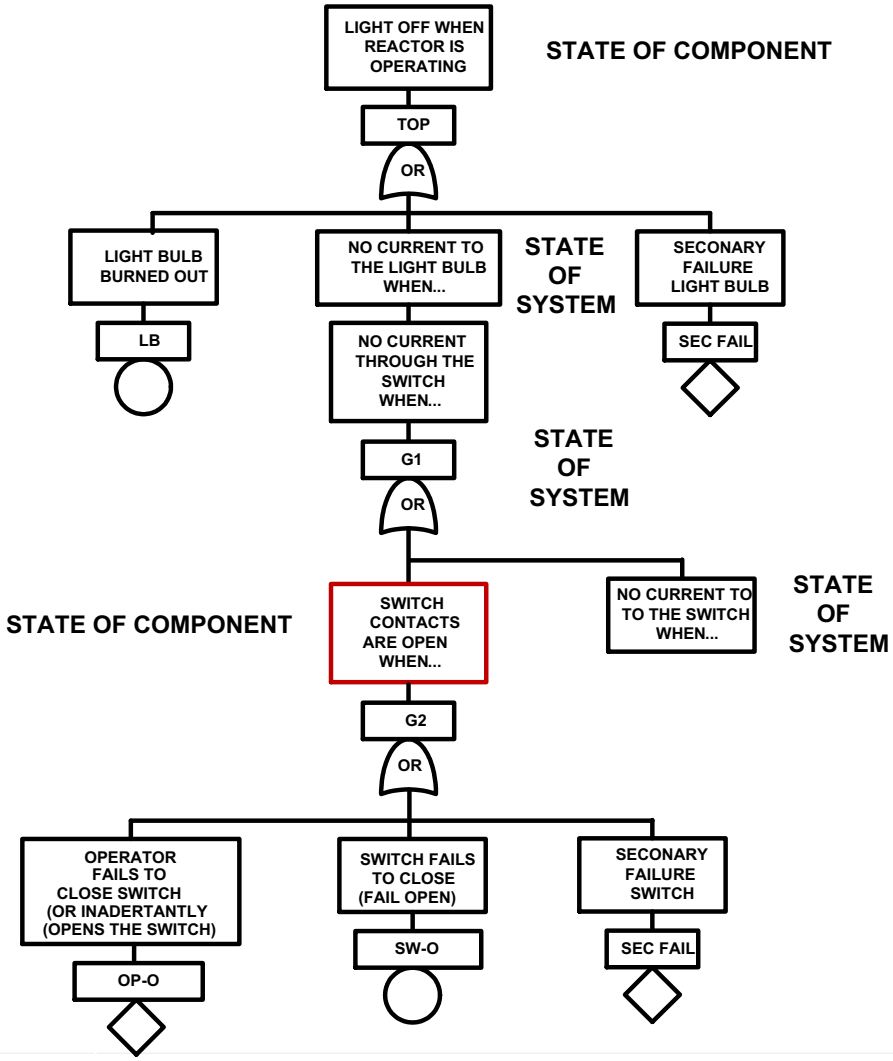
SWITCH CONTACTS ARE OPEN

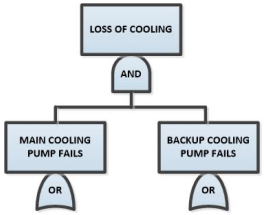
1. SWITCH CONTACTS FAIL TO CLOSE
OR
2. OPERATOR FAILS TO CLOSE SWITCH (OR INADVERTANTLY OPENS THE SWITCH)

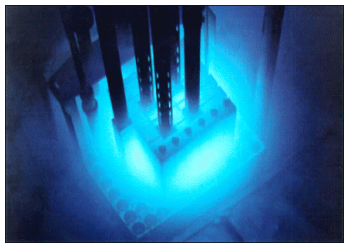

LOSS OF COOLING
AND
MAIN COOLING PUMP FAILS
BACKUP COOLING PUMP FAILS
OR
OR

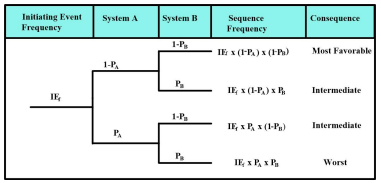


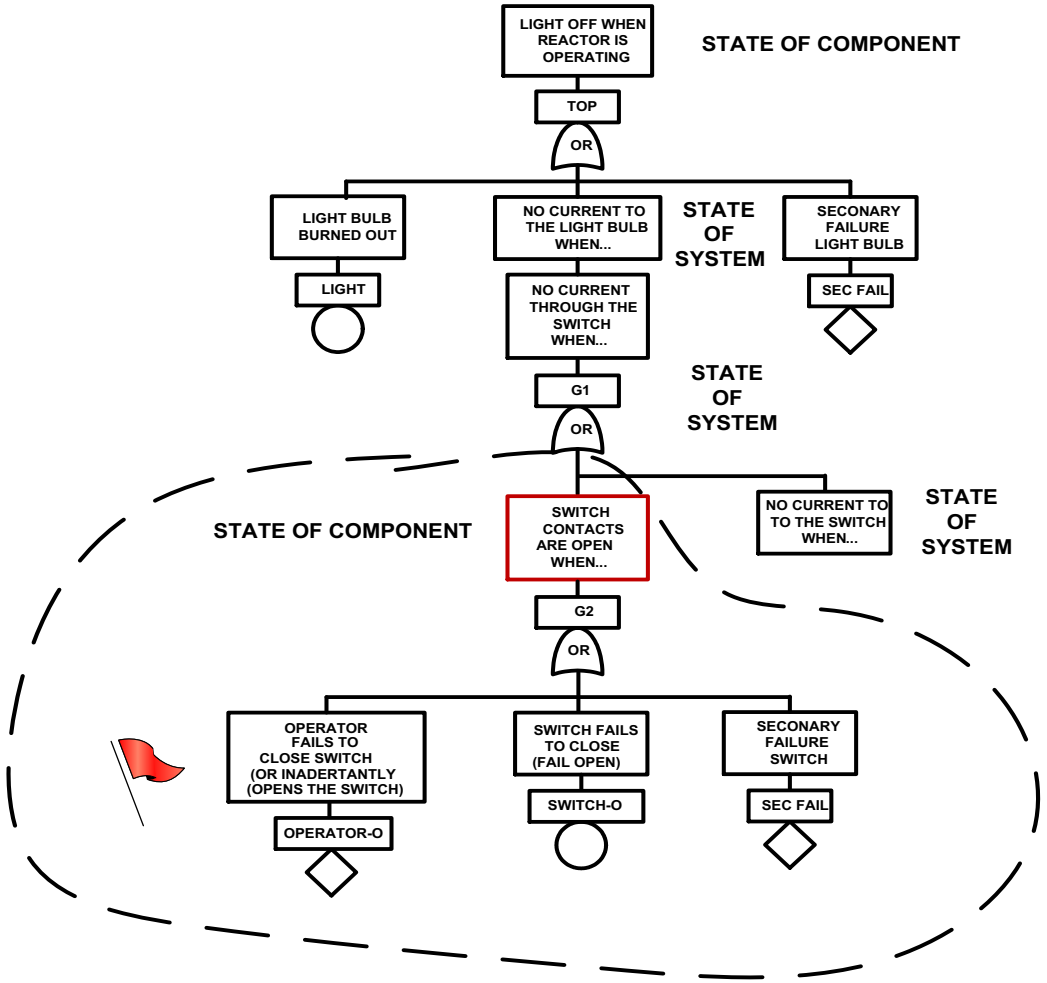

Initiating Event Frequency
System A
System B
Sequence Frequency
Consequence
1-P_B
IE_F x (1-P_A) x (1-P_B)
Most Favorable
1-P_A
P_B
IE_F x (1-P_A) x P_B
Intermediate
IE_F
1-P_B
P_A
IE_F x P_A x (1-P_B)
Intermediate
P_B
IE_F x P_A x P_B
Worst

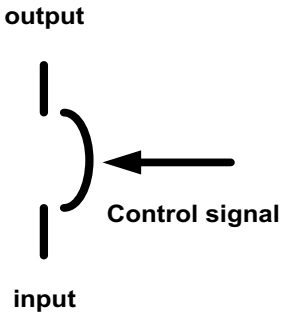

LIGHT OFF WHEN REACTOR IS OPERATING
STATE OF COMPONENT
TOP
OR
LIGHT BULB BURNED OUT
NO CURRENT TO THE LIGHT BULB WHEN...
STATE OF SYSTEM
SECONARY FAILURE LIGHT BULB
LB
NO CURRENT THROUGH THE SWITCH WHEN...
SEC FAIL
G1
STATE OF SYSTEM
OR
STATE OF COMPONENT
SWITCH CONTACTS ARE OPEN WHEN...
NO CURRENT TO TO THE SWITCH WHEN...
STATE OF SYSTEM
G2
OR
OPERATOR FAILS TO CLOSE SWITCH (OR INADERTANTLY (OPENS THE SWITCH)
SWITCH FAILS TO CLOSE (FAIL OPEN)
SECONARY FAILURE SWITCH
OP-O
SW-O
SEC FAIL

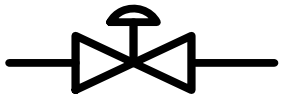






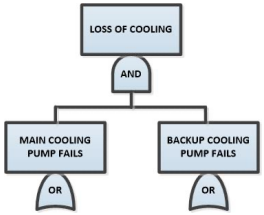




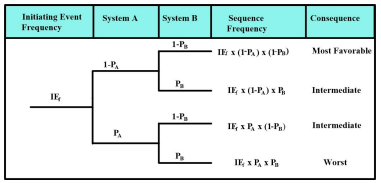


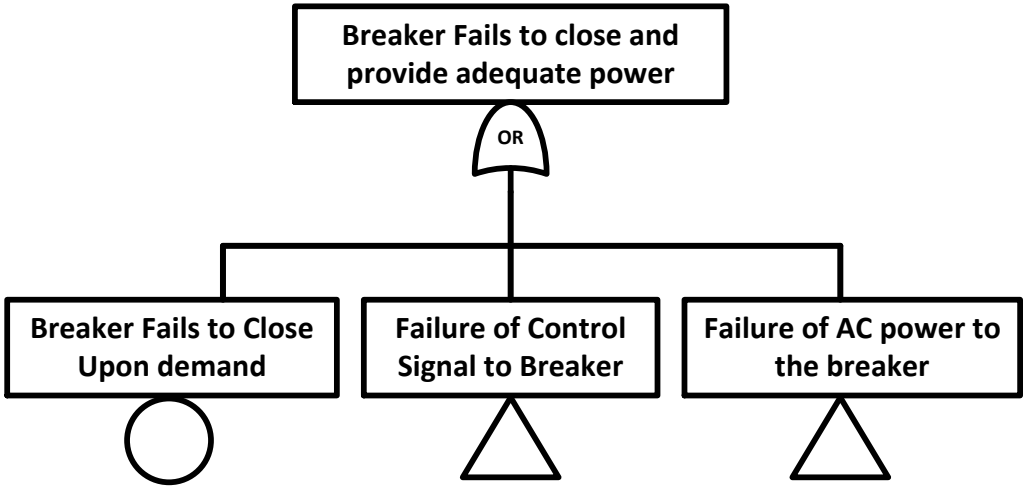
MANUAL VALVE

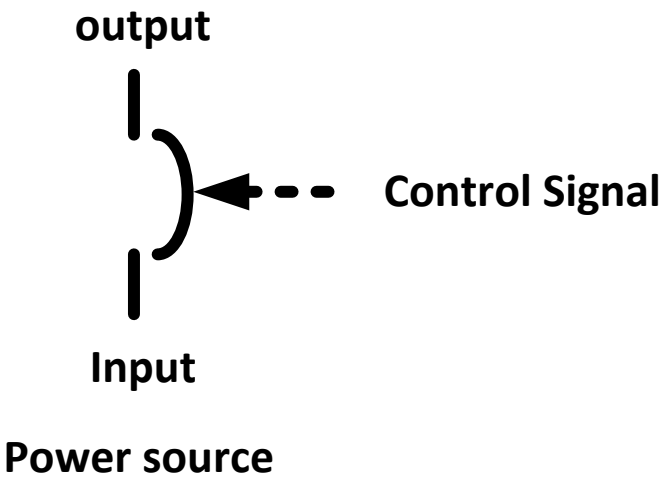
Analogies to and through FTA concept

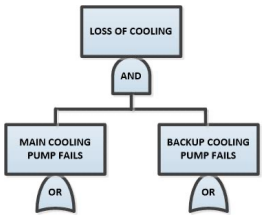


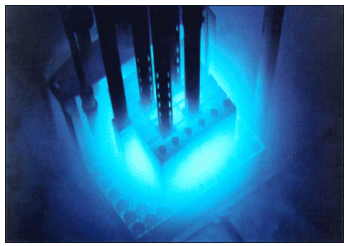
Circuit Breaker Analogy for Manual Switch

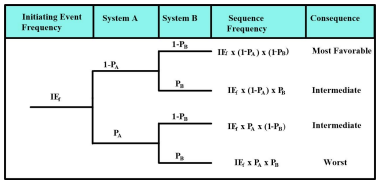


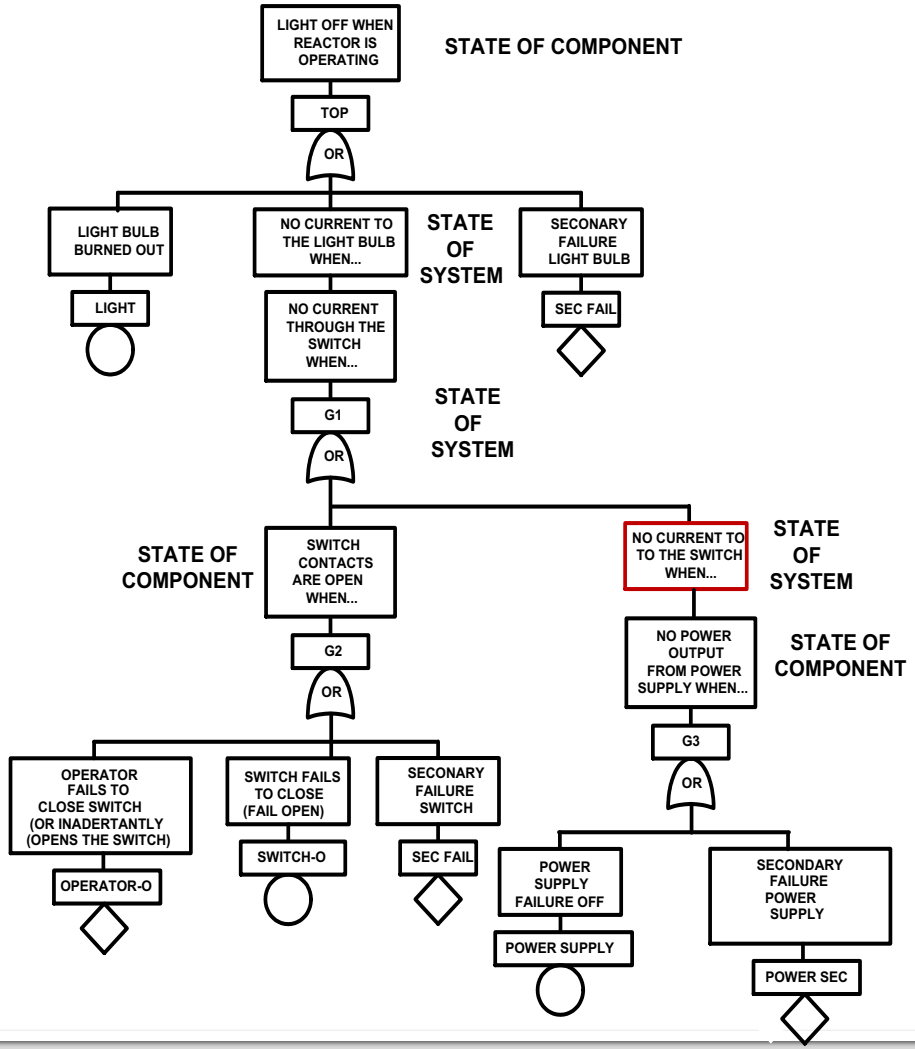


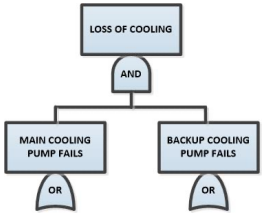



LOSS OF COOLING
AND
MAIN COOLING PUMP FAILS
BACKUP COOLING PUMP FAILS
OR
OR

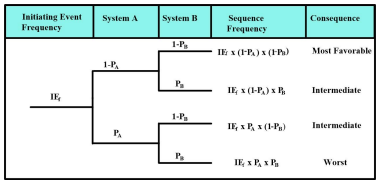



Initiating Event Frequency
System A
System B
Sequence Frequency
Consequence
1-P_B
IE_I x (1-P_A) x (1-P_B)
Most Favorable
1-P_A
P_B
IE_I x (1-P_A) x P_B
Intermediate
IE_I
1-P_B
IE_I x P_A x (1-P_B)
Intermediate
P_A
P_B
IE_I x P_A x P_B
Worst


LIGHT OFF WHEN REACTOR IS OPERATING
STATE OF COMPONENT
TOP
OR
LIGHT BULB BURNED OUT
NO CURRENT TO THE LIGHT BULB WHEN...
STATE OF SYSTEM
SECONARY FAILURE LIGHT BULB
LIGHT
NO CURRENT THROUGH THE SWITCH WHEN...
SEC FAIL
G1
STATE OF SYSTEM
OR
STATE OF COMPONENT
SWITCH CONTACTS ARE OPEN WHEN...
NO CURRENT TO TO THE SWITCH WHEN...
STATE OF SYSTEM
G2
NO POWER OUTPUT FROM POWER SUPPLY WHEN...
STATE OF COMPONENT
OR
G3
OR
OPERATOR FAILS TO CLOSE SWITCH (OR INADERTANTLY (OPENS THE SWITCH)
SWITCH FAILS TO CLOSE (FAIL OPEN)
SECONARY FAILURE SWITCH
POWER SUPPLY FAILURE OFF
SECONDARY FAILURE POWER SUPPLY
OPERATOR-O
SWITCH-O
SEC FAIL
POWER SUPPLY
POWER SEC



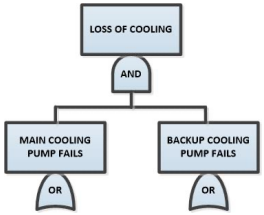
Minimal Cut set



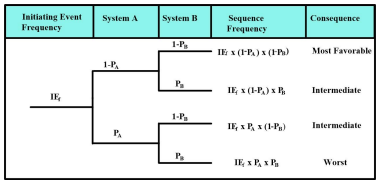
Minimal Cut set: A minimal cut set is defined as the smallest combination of component failures which, if they occur, will cause the top event of a fault tree to occur.

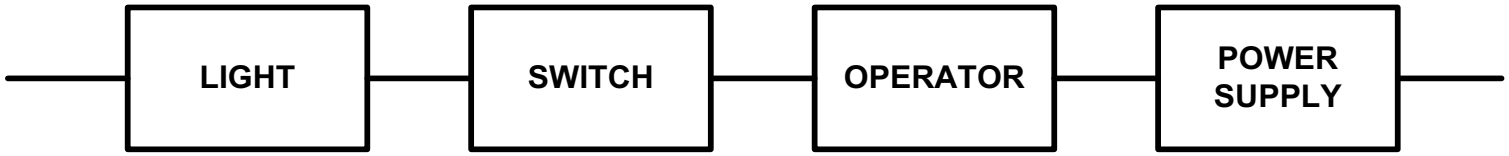
A fault tree consists of a finite number of minimal cut sets, all of which are in series, which are unique for the top event to occur. Since the combination of all minimal cut sets are in series, the failure of any cut set will cause the failure of the top gate.

The minimal cut set list for a fault tree can be obtained using Boolean algebra techniques. These techniques involve representing the gates and basic events in a fault tree with the equivalent Boolean expressions.

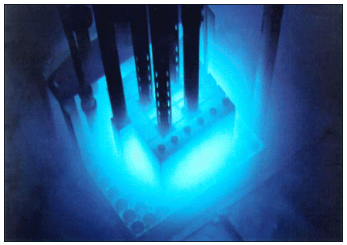


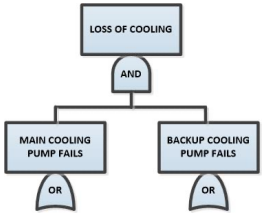
Block Diagram Representation



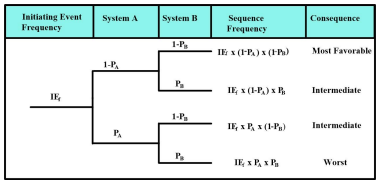


- Reliability type fault tree
- Series System
- One success path of order 4
- 4 min cut sets of order 1
- Lusser's Law

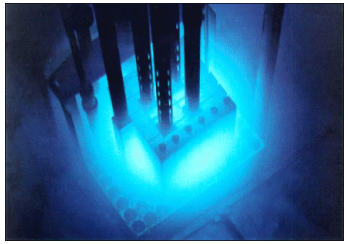




Four Min Cut Sets of Order 1

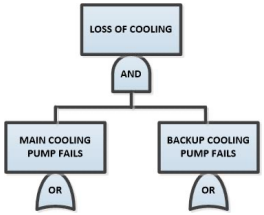


1. Light bulb burned out (LB)
2. Switch fails to close (SW-O)
3. Operator fails to close switch (or inadvertently opens switch) (OP-O)
4. Power Supply Failure off (PS)

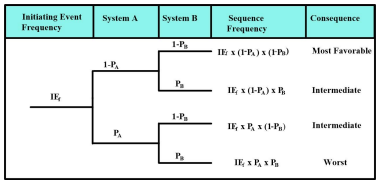


Min Cut Sets -- Alpha Numeric Identifiers

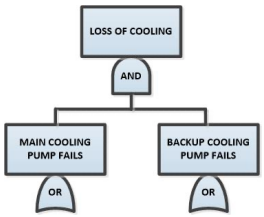
LB,SW-O,OP-O,PS

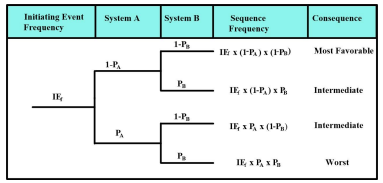


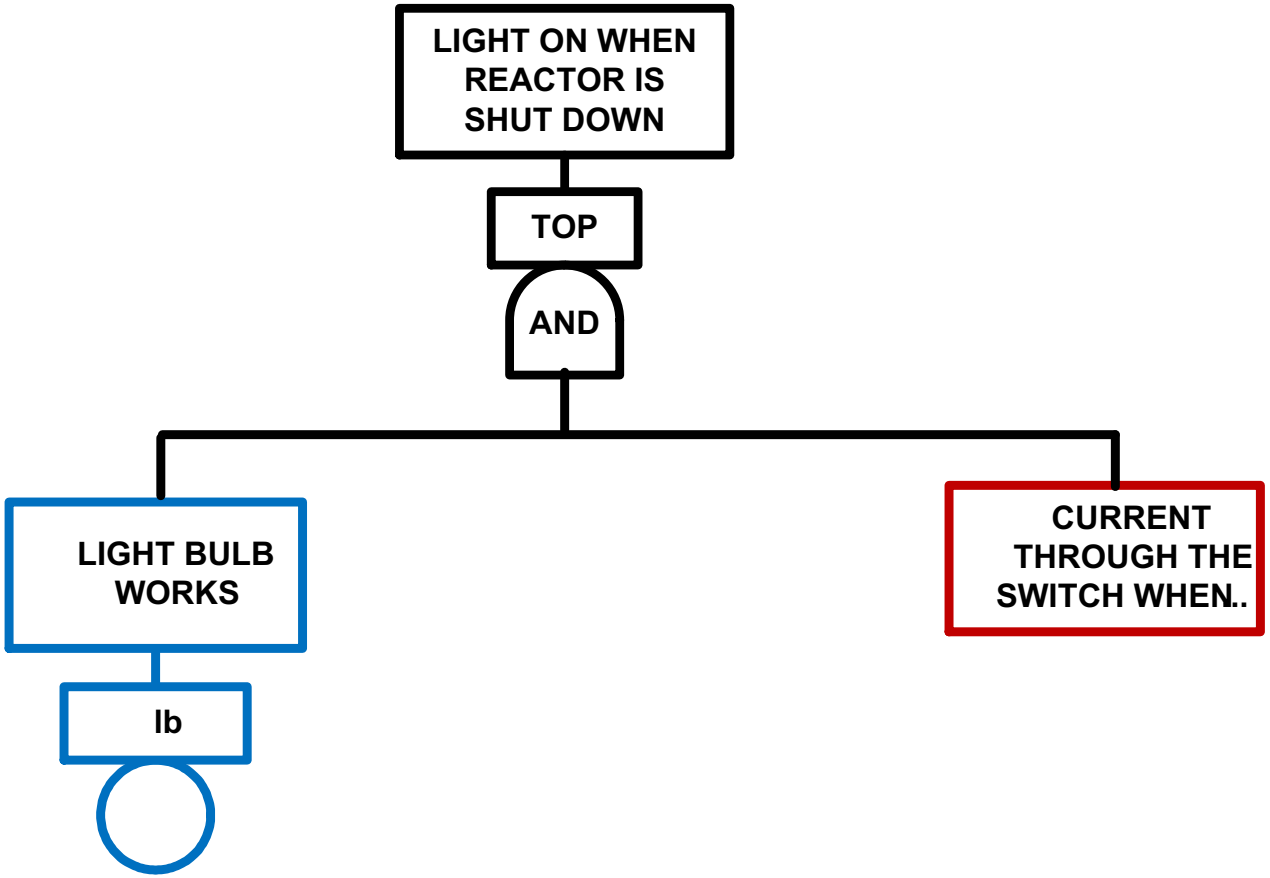
FAULT TREE OPERATOR FOR TYPE 2 FAULT EVENTS

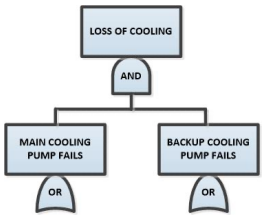


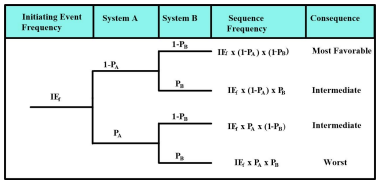
- Component working when it should be off (e.g., light on when reactor is off)
- Include success events in fault trees
- Eliminate them for reliable systems
- Develop operator for type 2 fault events --- include components that can self activate

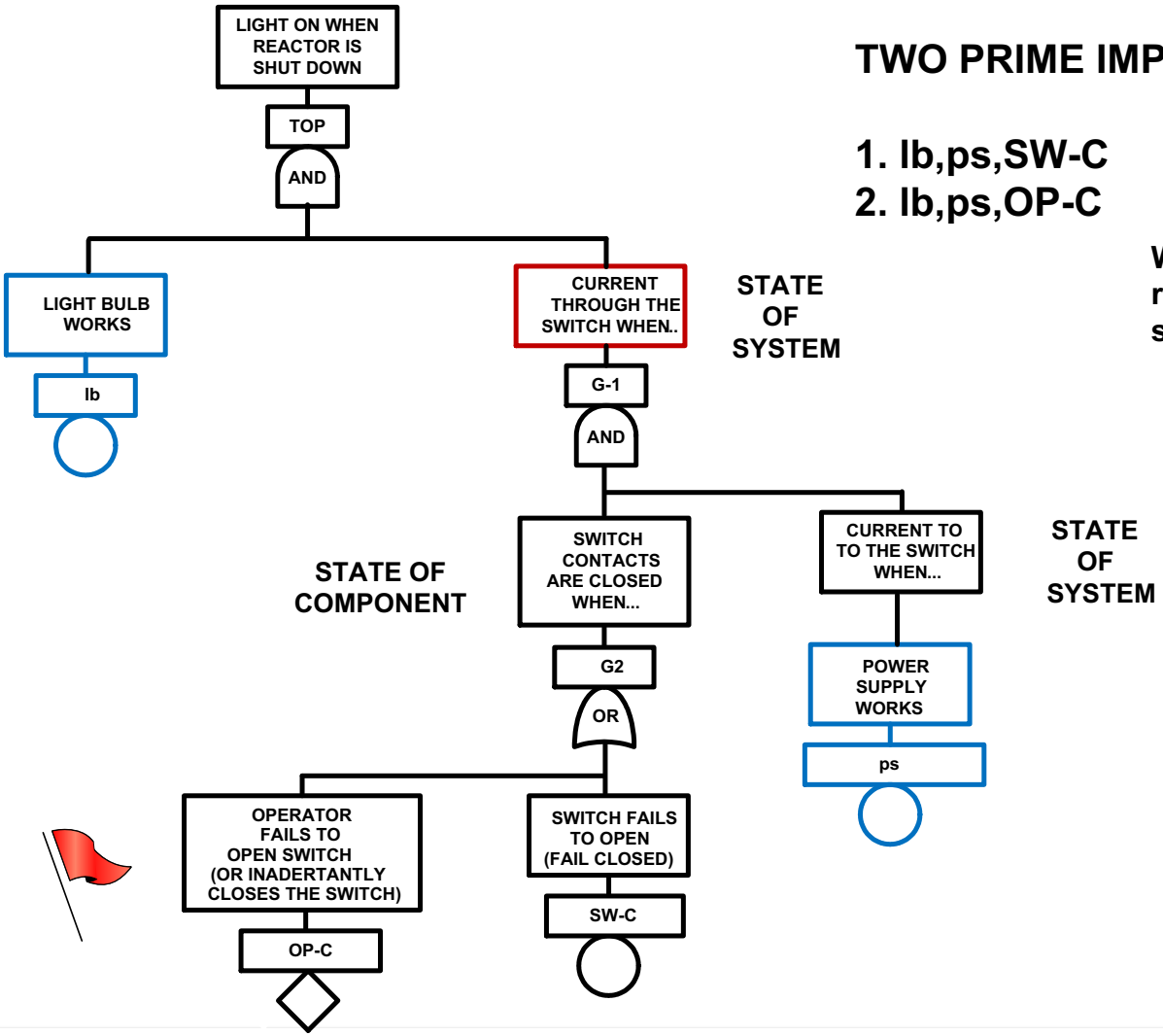

LOSS OF COOLING
AND
MAIN COOLING PUMP FAILS
BACKUP COOLING PUMP FAILS
OR
OR


Initiating Event Frequency
System A
System B
Sequence Frequency
Consequence
1-P_B
IE_F x (1-P_A) x (1-P_B)
Most Favorable
1-P_A
P_B
IE_F x (1-P_A) x P_B
Intermediate
IE_F
1-P_B
P_A
IE_F x P_A x (1-P_B)
Intermediate
P_B
IE_F x P_A x P_B
Worst


LIGHT ON WHEN REACTOR IS SHUT DOWN
TOP
AND
LIGHT BULB WORKS
lb
CURRENT THROUGH THE SWITCH WHEN..



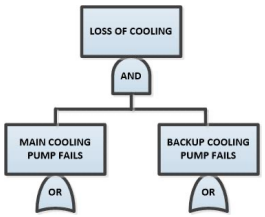




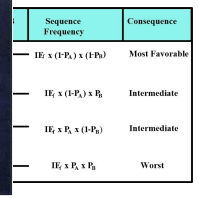
TWO PRIME IMPLICANTS

1. lb,ps,SW-C
2. lb,ps,OP-C

When.. reactor is shut down



Success Criteria

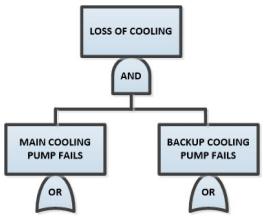


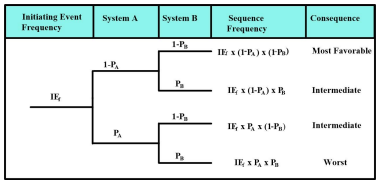
- Include successes
- Min cut sets (called prime implicates)

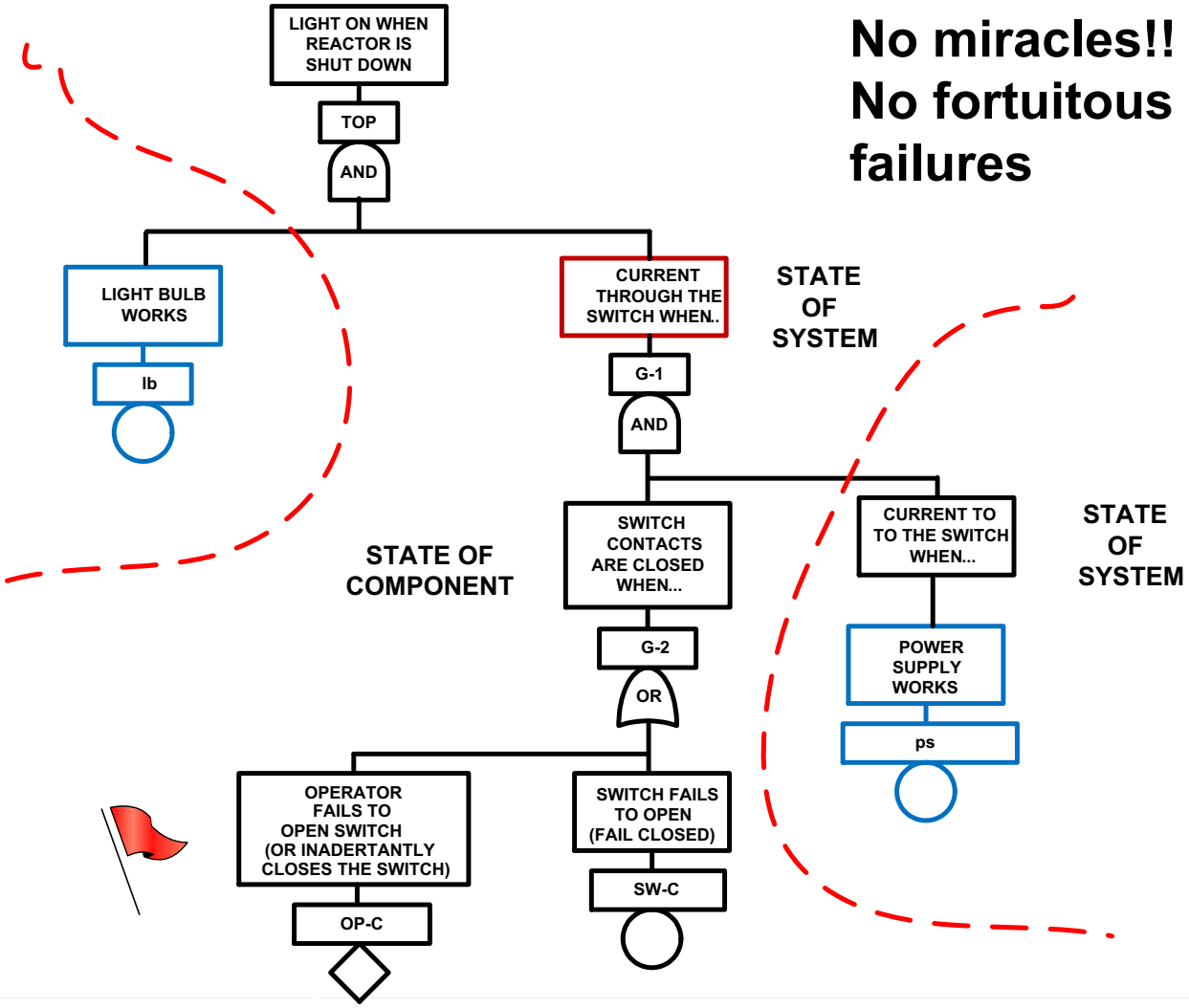
1. Switch Fails to open, light works, power supply works
2. Operator Fails to open switch, light works, power supply works

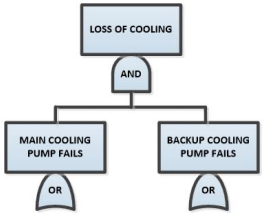
Success Paths

1. Light Fails 
2. Power Supply Fails 
3. Switch works, Operator works

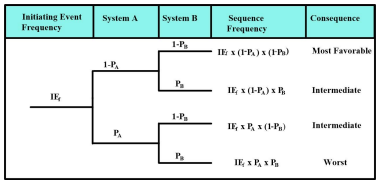

LOSS OF COOLING
AND
MAIN COOLING PUMP FAILS
BACKUP COOLING PUMP FAILS
OR
OR

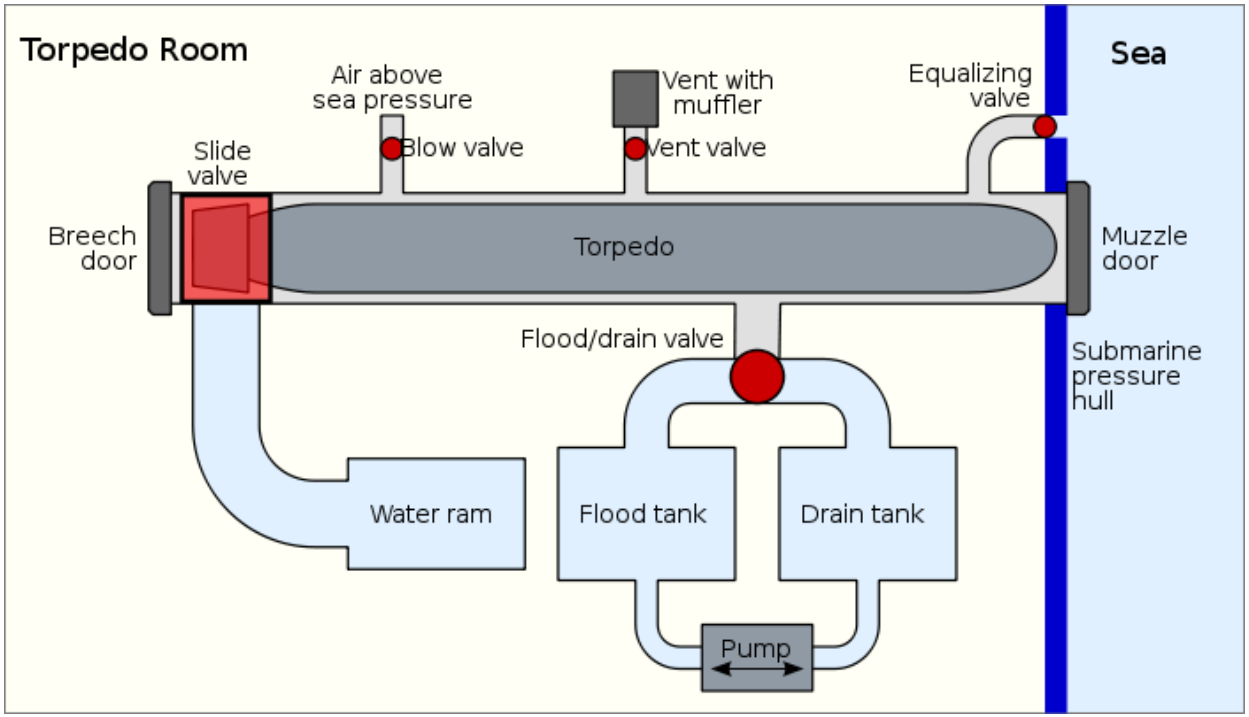

Initiating Event Frequency
System A
System B
Sequence Frequency
Consequence
Most Favorable
Intermediate
Intermediate
Worst


LIGHT ON WHEN REACTOR IS SHUT DOWN
TOP
AND
LIGHT BULB WORKS
lb
CURRENT THROUGH THE SWITCH WHEN..
G-1
AND
SWITCH CONTACTS ARE CLOSED WHEN...
G-2
OR
OPERATOR FAILS TO OPEN SWITCH (OR INADERTANTLY CLOSES THE SWITCH)
OP-C
SWITCH FAILS TO OPEN (FAIL CLOSED)
SW-C
CURRENT TO TO THE SWITCH WHEN...
POWER SUPPLY WORKS
ps
STATE OF COMPONENT
STATE OF SYSTEM
STATE OF SYSTEM
No miracles!!
No fortuitous failures

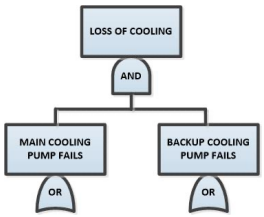


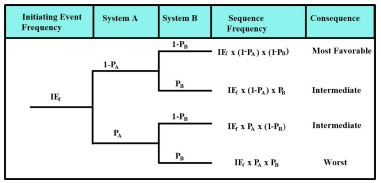
Inadvertent launch signal of torpedo – muzzle door did not open as intended

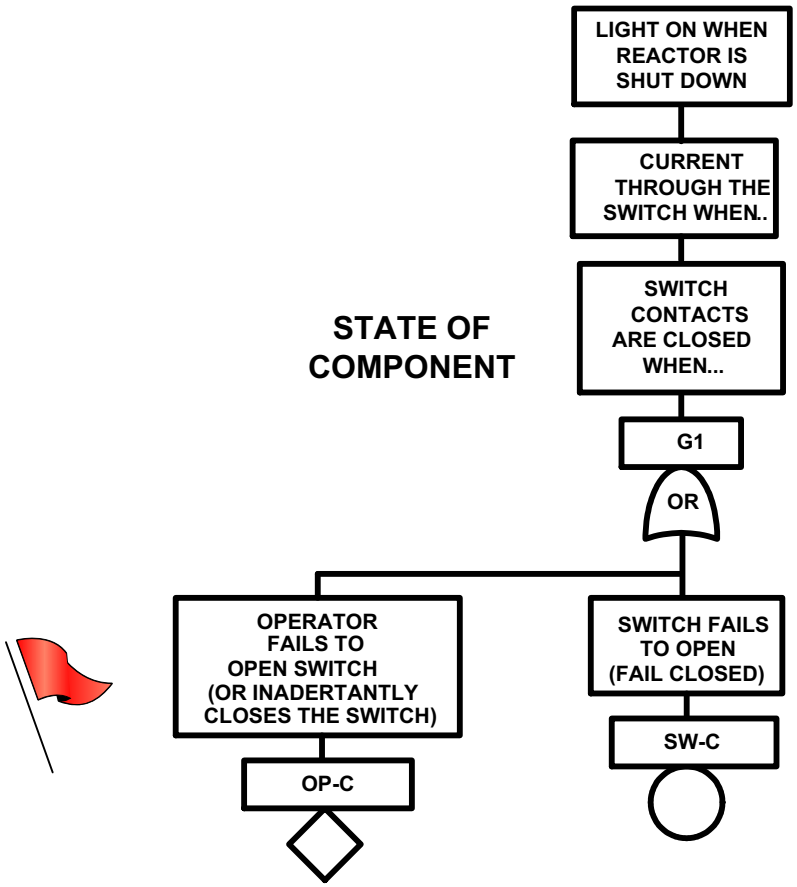




Fortuitous failure!!

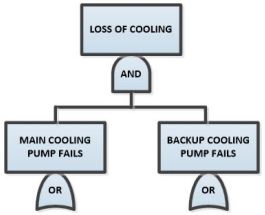




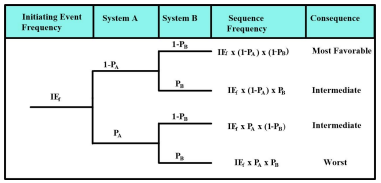


TWO MIN CUT SETS

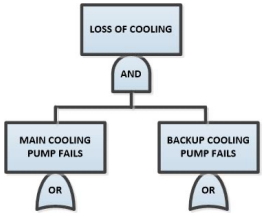
1. SW-C
2. OP-C



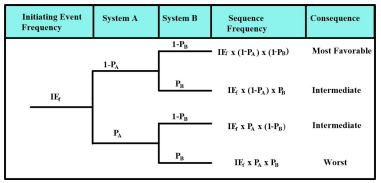
Type 2 events when component has internal energy source (component can self activate)

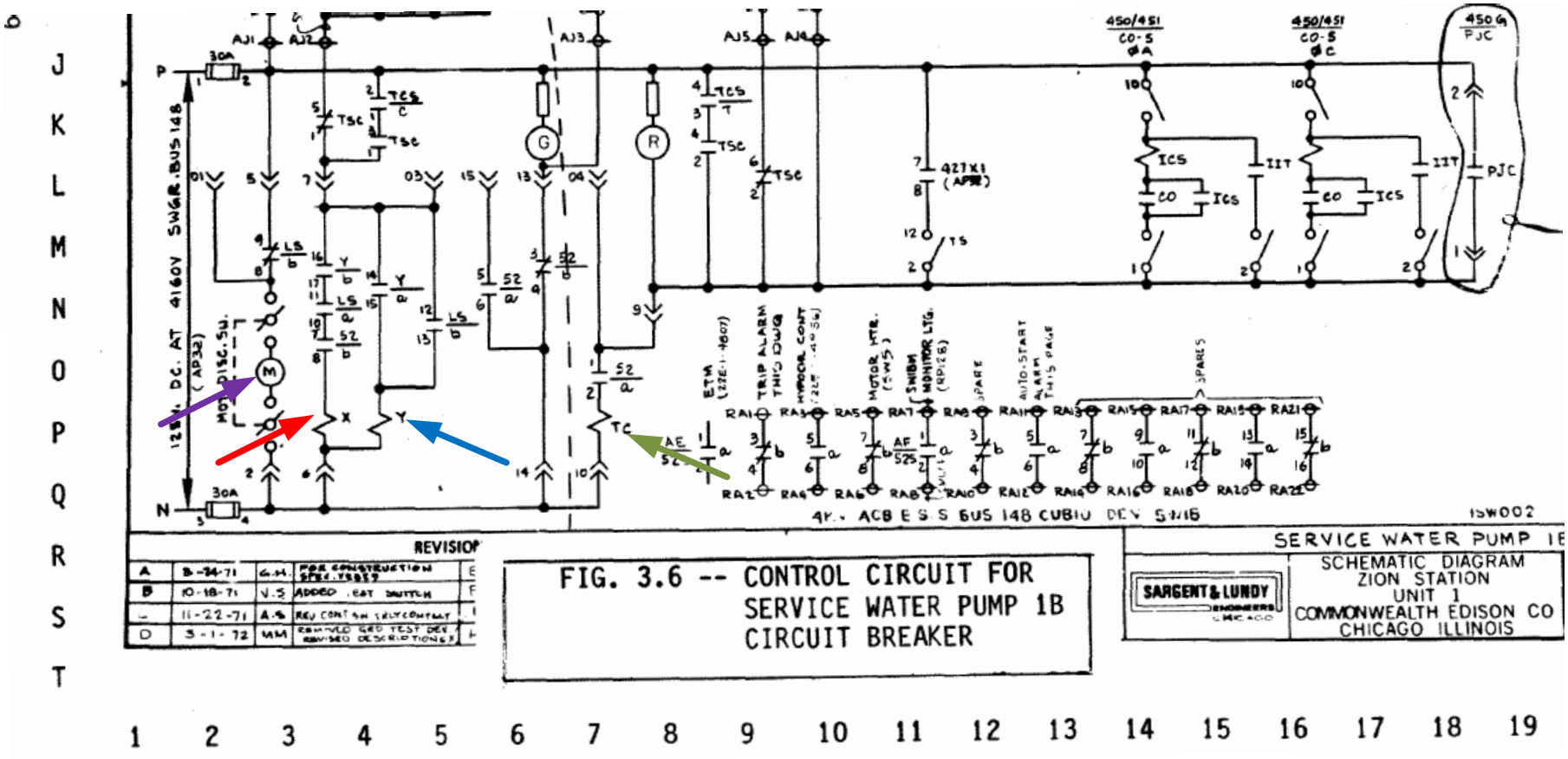


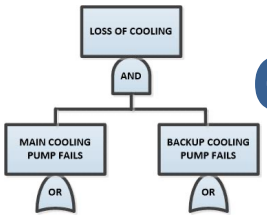
- Industrial circuit breaker with X-Y circuit breaker scheme
- Assume circuit breaker is closed
- Opening spring is charged and opens circuit breaker when latch internal to circuit breaker is released
- Trip coil releases latch
- Top event of interest is advertent trip of the breaker



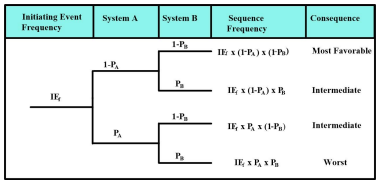
Control Circuit for X-Y circuit breaker scheme

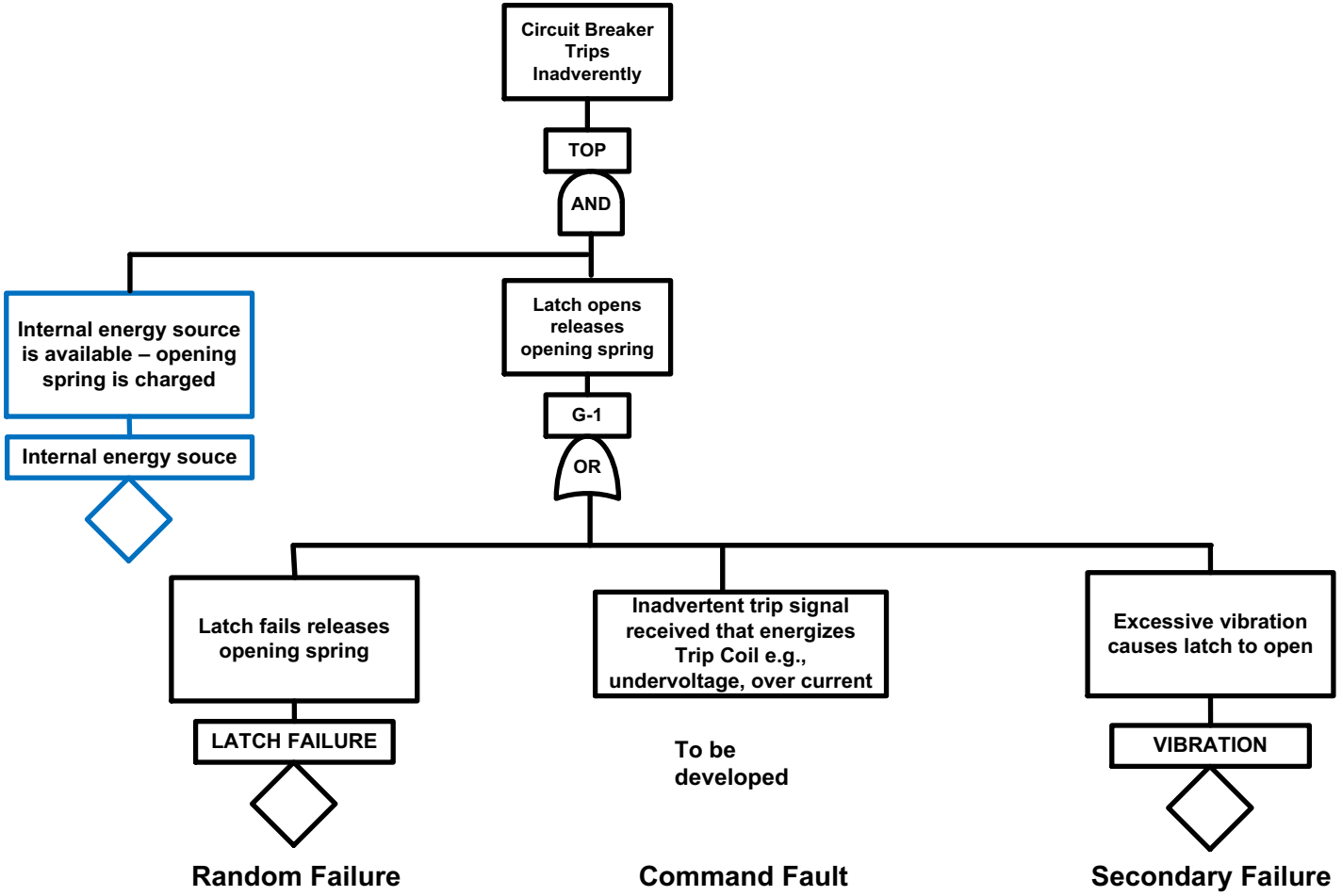


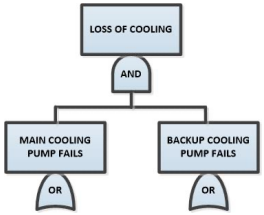




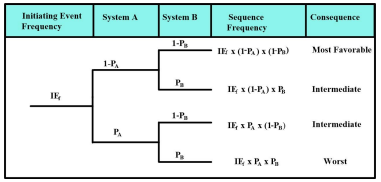
Circuit breaker trips inadvertently -- type 2 fault event

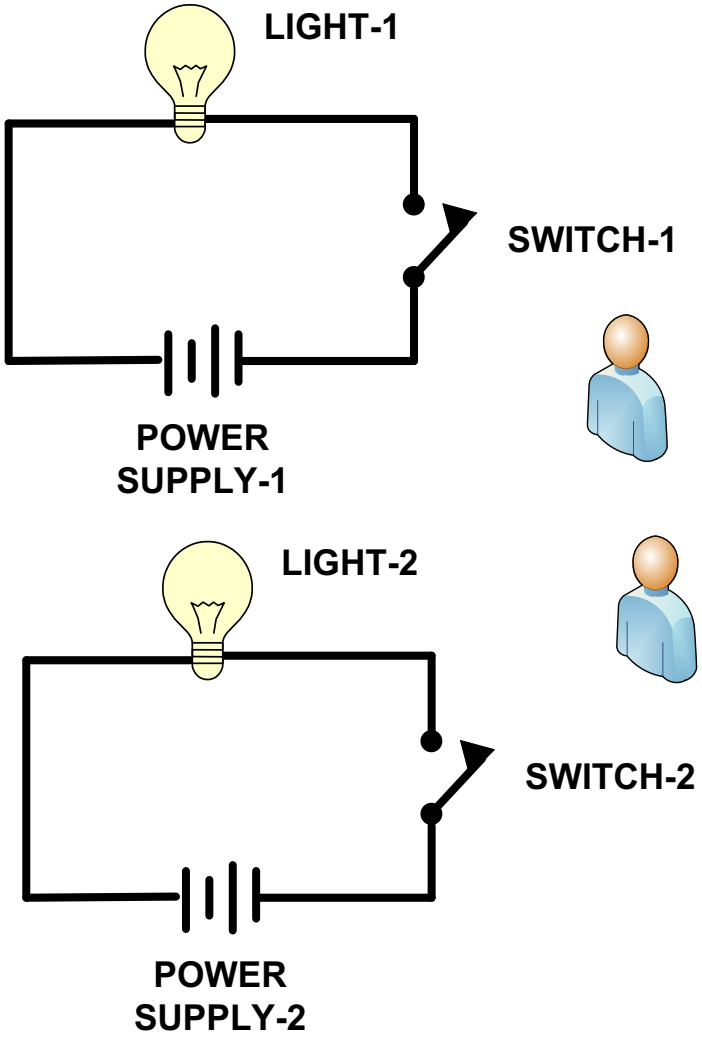






TWO LIGHT BULB SYSTEM

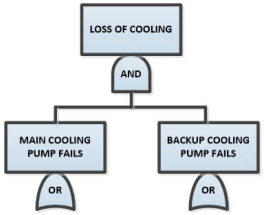




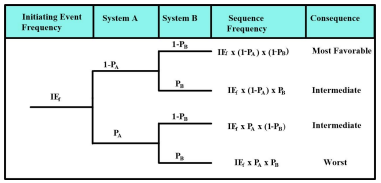
OPERATOR-1

OPERATOR-2

REDUNDANY AT THE SYSTEM LEVEL

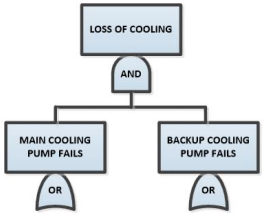


SUCCESS CRITERIA

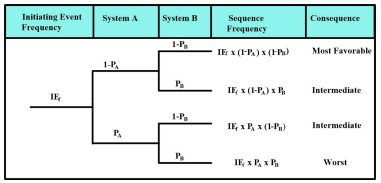


LIGHT 1	LIGHT 2	REACTOR ON	REACTOR OFF
OFF	OFF	FAILURE (1)	SUCCESS
OFF	ON	SUCCESS	FAILURE (2)
ON	OFF	SUCCESS	FAILURE (2)
ON	ON	SUCCESS	FAILURE (2)

(1) WORKER SAFETY ISSUE (type 1 failure)
(2) NUISANCE ISSUE (type 2 failure)

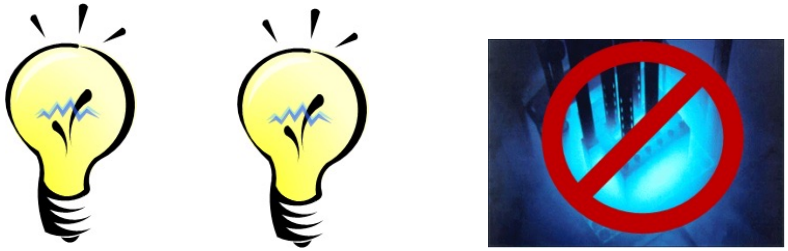


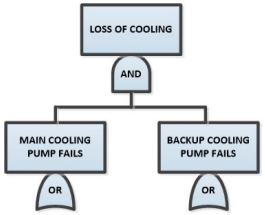
TOP LOGIC GATE FOR TWO TYPES OF EVENTS



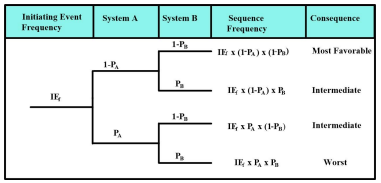
- What is the top logic gate for the top event “No light when reactor is operating?”

- What is the top logic gate for the top event “Light on when reactor is operating?” (At least one light on)

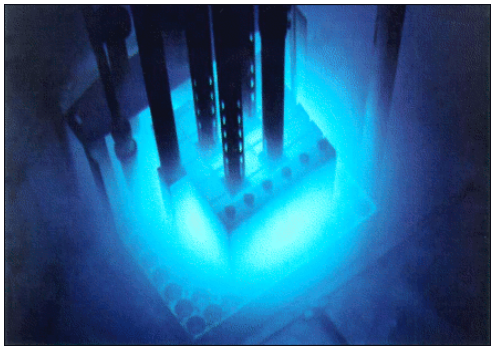


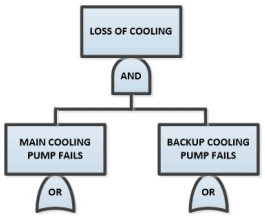


Two Light Bulb System

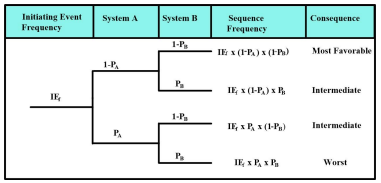


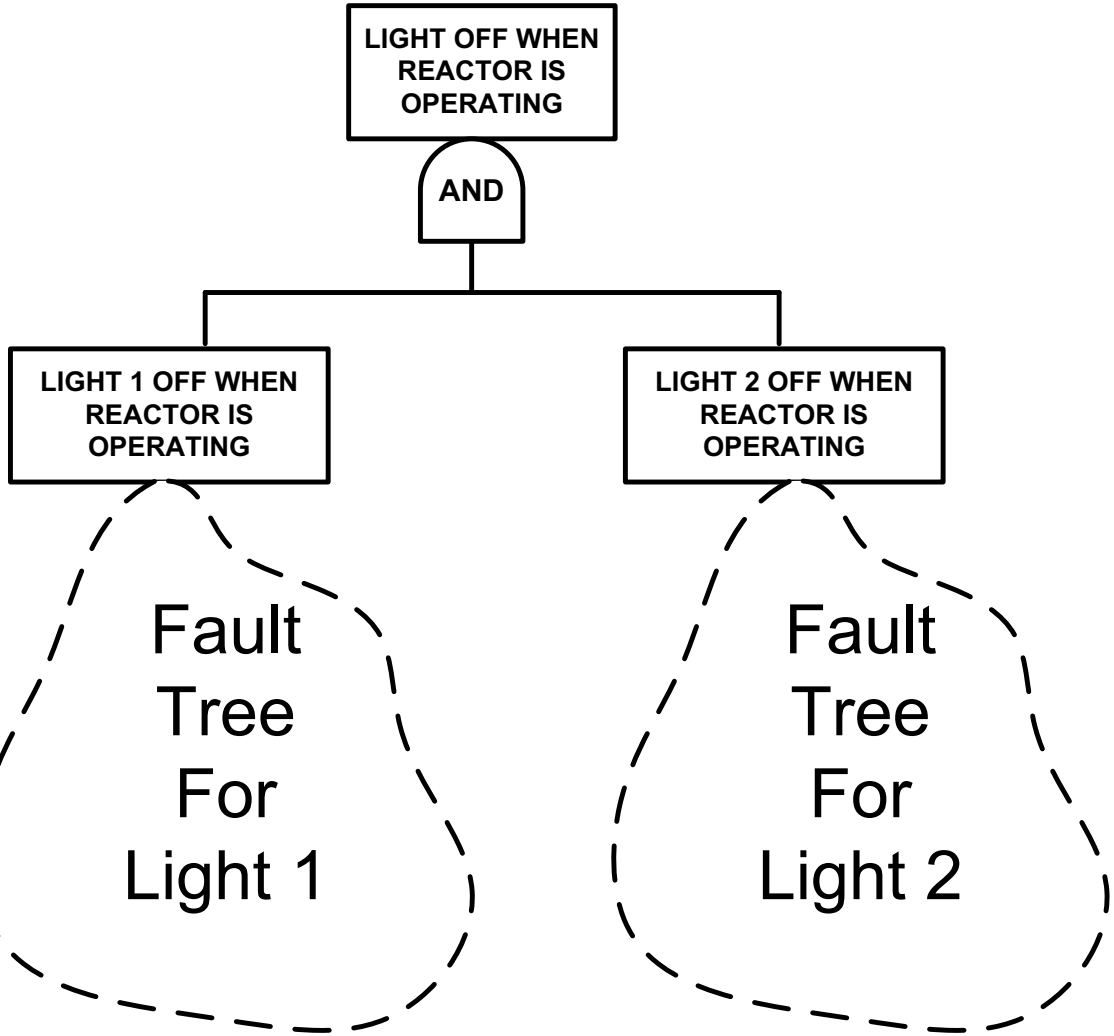
Top Event "Light off when reactor is operating"

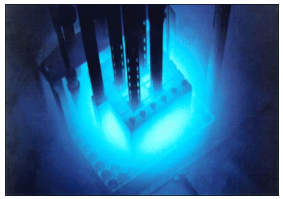


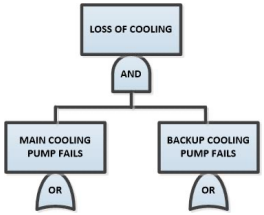


Fault Tree Top Event for two light bulb system

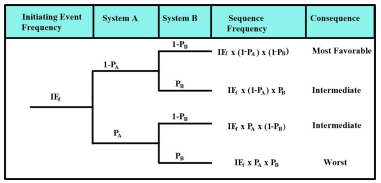




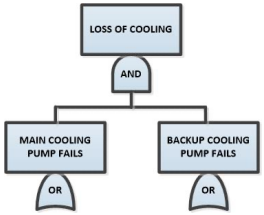




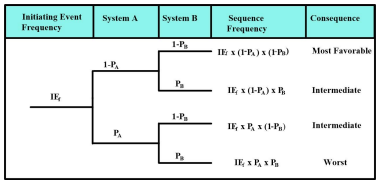
Rules of Boolean Algebra used to simplify logic equations

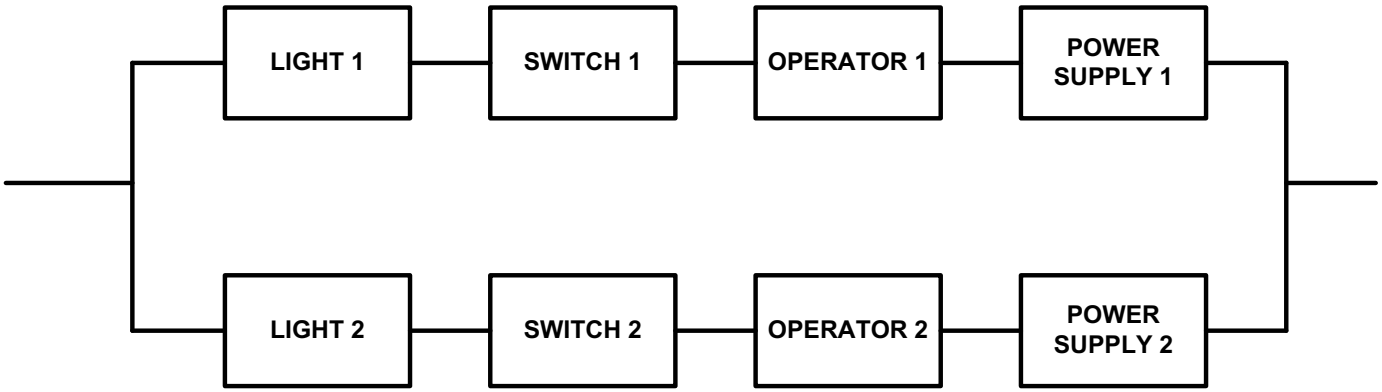


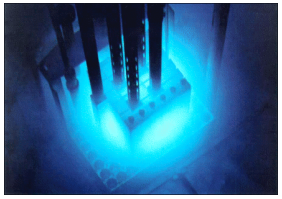
Rule	Equation	Law
1	A·1 = A A·0 = 0	Intersection
2	A+1 = 1 A+0 = A	Union (+ means union)
3	A·A = A A+1 = A	Tautology
4	A· Ā= 0 A+ Ā = 1	Complementation
5	$A = \overline{\overline{A}}$	Double Negative
6	A·B = B·A A+B=B+A	Commutative
7	A·(B+C) = A·B + A·C (A + B)·(A + C) = A + B·C	Distributive
8	(A·B)·C = A·(B·C) = A·B·C (A+B)+C = A+(B+C) = A+B+C	Association
9	A·(A+B) = A A·(Ā+B) = A·B $A \cdot B + \overline{B} = A + \overline{B}$ $A \cdot \overline{B} + B = A + B$	Absorption
10	$\overline{A + B} = \overline{A} \cdot \overline{B}$ $\overline{A \cdot B} = \overline{A} + \overline{B}$	DeMorgan's
Notes : · intersection, + union, 0 empty set, 1 entire set, Ā is complement of A (not A)		



Block Diagram for two light bulb system





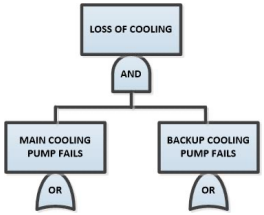


Two success paths
16 min cut sets of order 2 (doubles)

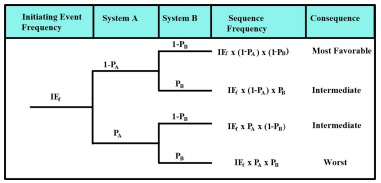
BOOLEAN ALGEBRA REPRESENTATION

(LB1+SW1-O+OP1-O+PS1)● (LB2+SW2-O+OP2-O+PS2)

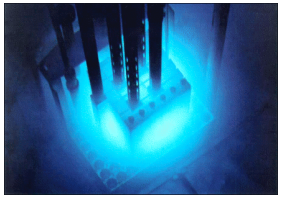
WHERE
+ DENOTES BOOLEAN OR
● DENOTES BOOLEAN AND

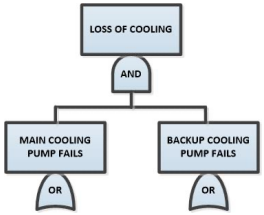


16 min cut sets of order 2 (doubles)

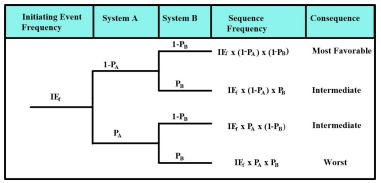


1. Light 1, Light 2 (LB1,LB2)
2. Light 1, Switch 2 (LB1,SW2-O)
3. Light 1, Operator 2 (LB1,OP2-O)
4. Light 1, Power Supply 2 (LB1,PS2)
5. Switch 1, Light 2 (SW1-O,LB2)
6. Switch 1, Switch 2 (SW1-O, SW2-O)
7. Switch 1, Operator 2 (SW1-O, OP2-O)
8. Switch 1, Power Supply 2 (SW1-O, PS2)
9. Operator 1, Light 2 (OP1-O, LB2)
10. Operator 1, Switch 2 (OP1-O, SW2-O)
11. Operator 1, Operator 2 (OP1-O,OP2-O)
12. Operator 1, Power Supply 2 (OP1-O,PS2)
13. Power Supply 1, Light 2 (PS1, LB2)
14. Power Supply 1, Switch 2 (PS1, SW2-O)
15. Power Supply 1, Operator 2 (PS1, OP2-O)
16. Power Supply 1, Power Supply 2 (PS1, PS2)

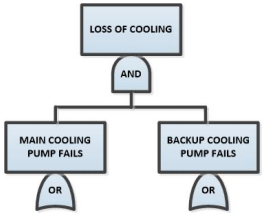




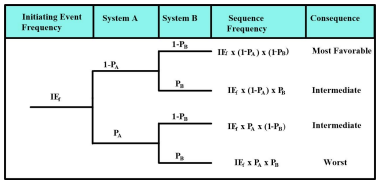
Common Cause Failure Analysis



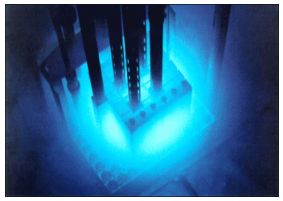
- Common Links Condition
  - Human
  - Hardware
  - Domain
- Parametric Probabilistic Analysis Alpha, Beta and Multiple Greek Factors
- Computer Analysis



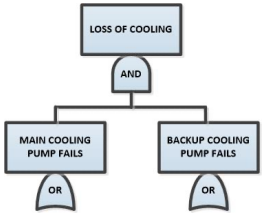
16 min cut sets of order 2 (doubles)



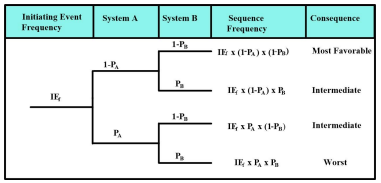
1. Light 1, Light 2 (LB1,LB2)
2. Light 1, Switch 2 (LB1,SW2-O)
3. Light 1, Operator 2 (LB1,OP2-O)
4. Light 1, Power Supply 2 (LB1,PS2)
5. Switch 1, Light 2 (SW1-O,LB2)
6. Switch 1, Switch 2 (SW1-O, SW2-O)
7. Switch 1, Operator 2 (SW1-O, OP2-O)
8. Switch 1, Power Supply 2 (SW1-O, PS2)
9. Operator 1, Light 2 (OP1-O, LB2)
10. Operator 1, Switch 2 (OP1-O, SW2-O)
11. Operator 1, Operator 2 (OP1-O,OP2-O)
12. Operator 1, Power Supply 2 (OP1-O,PS2)
13. Power Supply 1, Light 2 (PS1, LB2)
14. Power Supply 1, Switch 2 (PS1, SW2-O)
15. Power Supply 1, Operator 2 (PS1, OP2-O)
16. Power Supply 1, Power Supply 2 (PS1, PS2)

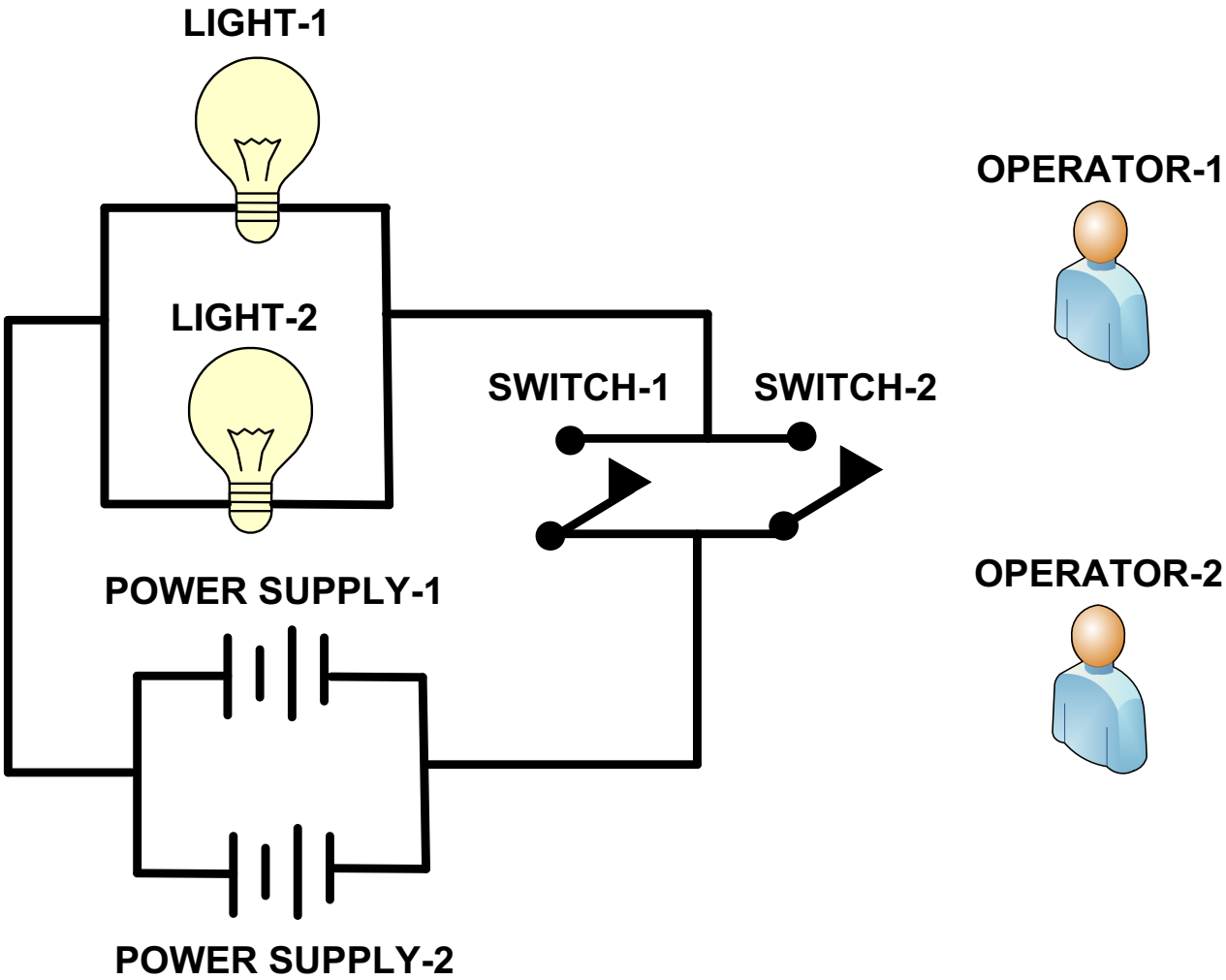


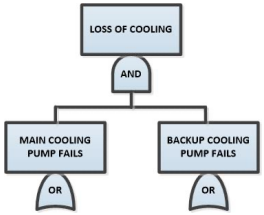
Note: Arrows indicate double failures of similar components candidates for common cause failure analysis



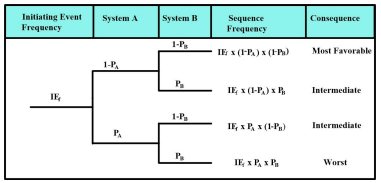
REDUNDANCY AT THE COMPONENT LEVEL



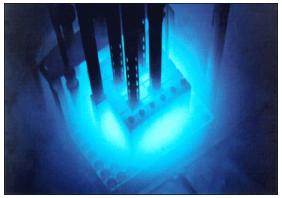


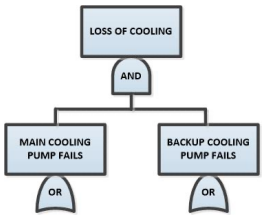


7 min cut sets of order 2 (doubles)

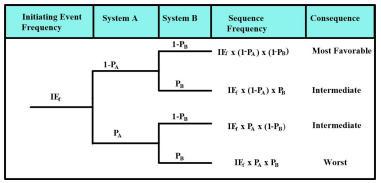


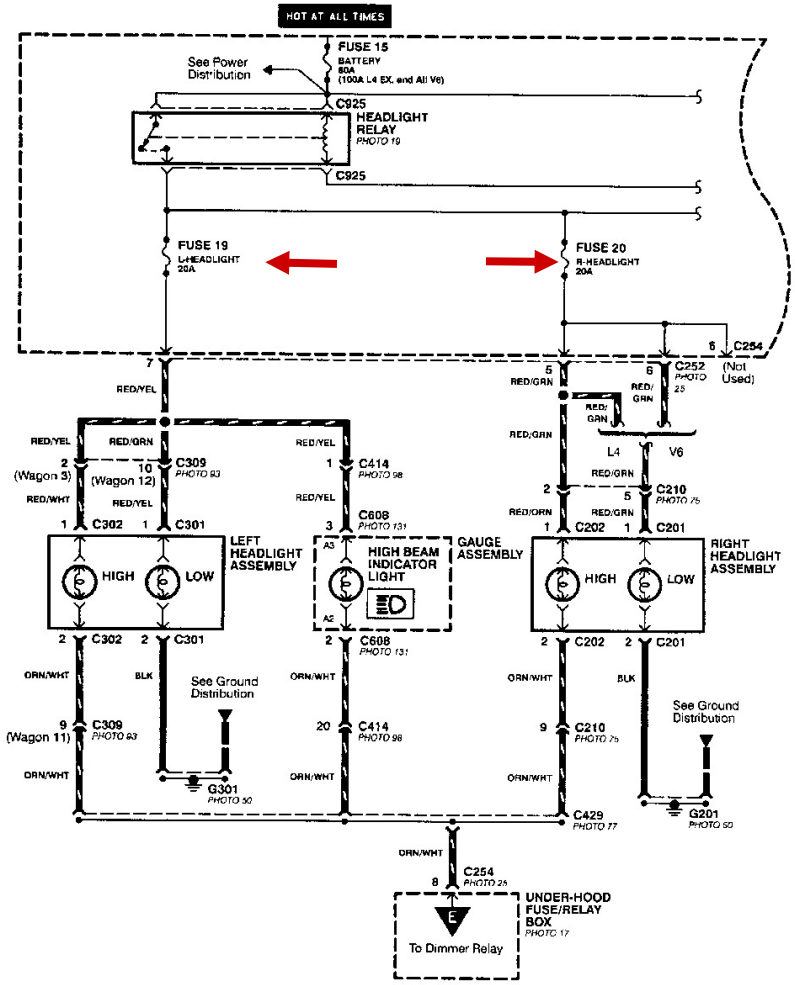
1. Light 1, Light 2 (LB1,LB2)
2. ~~Light 1, Switch 2 (LB1,SW2-O)~~
3. ~~Light 1, Operator 2 (LB1,OP2-O)~~
4. ~~Light 1, Power Supply 2 (LB1,PS2)~~
5. ~~Switch 1, Light 2 (SW1-O,LB2)~~
6. Switch 1, Switch 2 (SW1-O, SW2-O)
7. Switch 1, Operator 2 (SW1-O, OP2-O)
8. ~~Switch 1, Power Supply 2 (SW1-O, PS2)~~
9. Operator 1, Light 2 (OP1-O, LB2)
10. Operator 1, Switch 2 (OP1-O, SW2-O)
11. Operator 1, Operator 2 (OP1-O,OP2-O)
12. ~~Operator 1, Power Supply 2 (OP1-O,PS2)~~
13. ~~Power Supply 1, Light 2 (PS1, LB2)~~
14. ~~Power Supply 1, Switch 2 (PS1, SW2-O)~~
15. ~~Power Supply 1, Operator 2 (PS1, OP2-O)~~
16. Power Supply 1, Power Supply 2 (PS1, PS2)





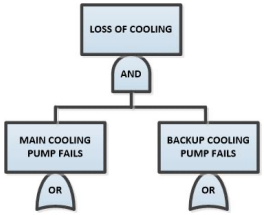
Auto Headlight Circuit



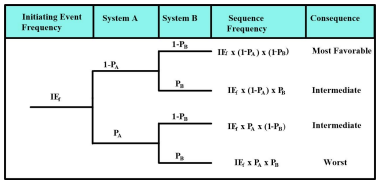


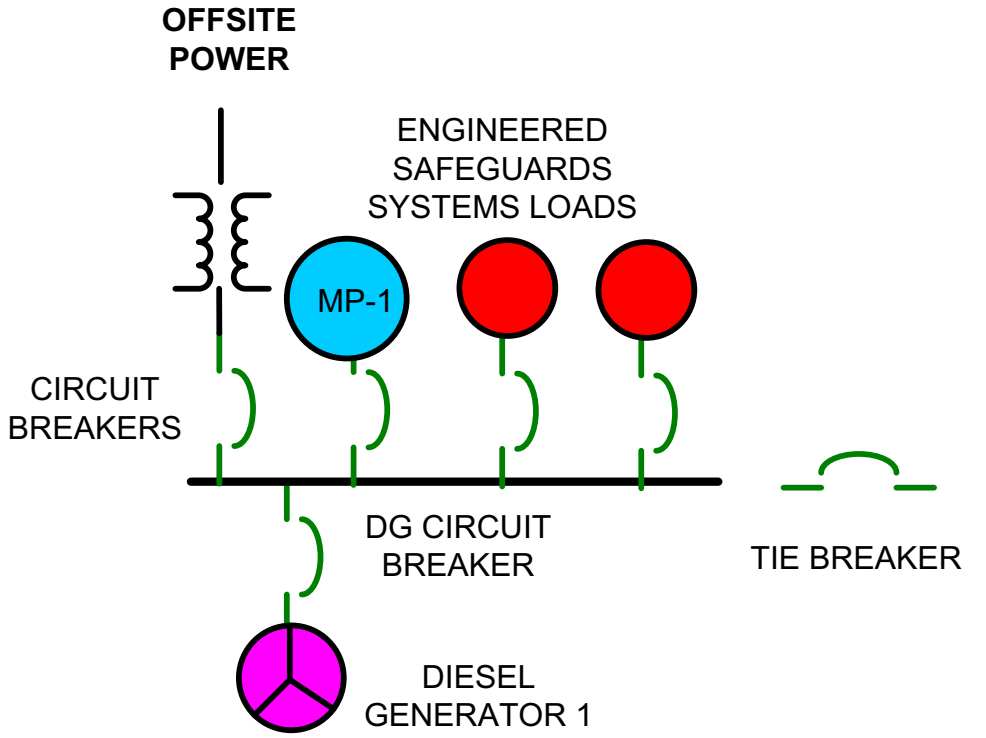
Headlights - USA (Part 1 Of 2)

Note a single fuse failure will not disable **both** head lights Redundancy at the system level



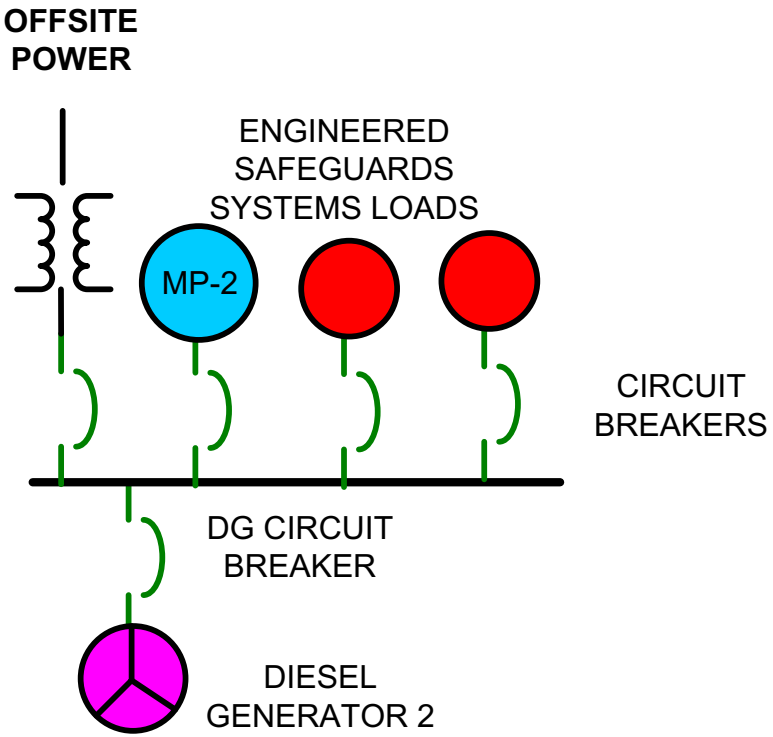
Min Cut Sets without and with tie breaker





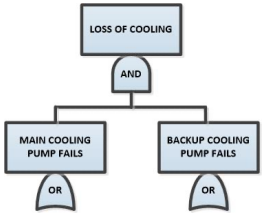
Min Cut Sets without tie breaker

1. MP-1, MP-2
2. DG-1, DG-2
3. MP-1, DG-1
4. MP-2,DG-2

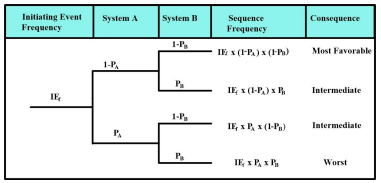


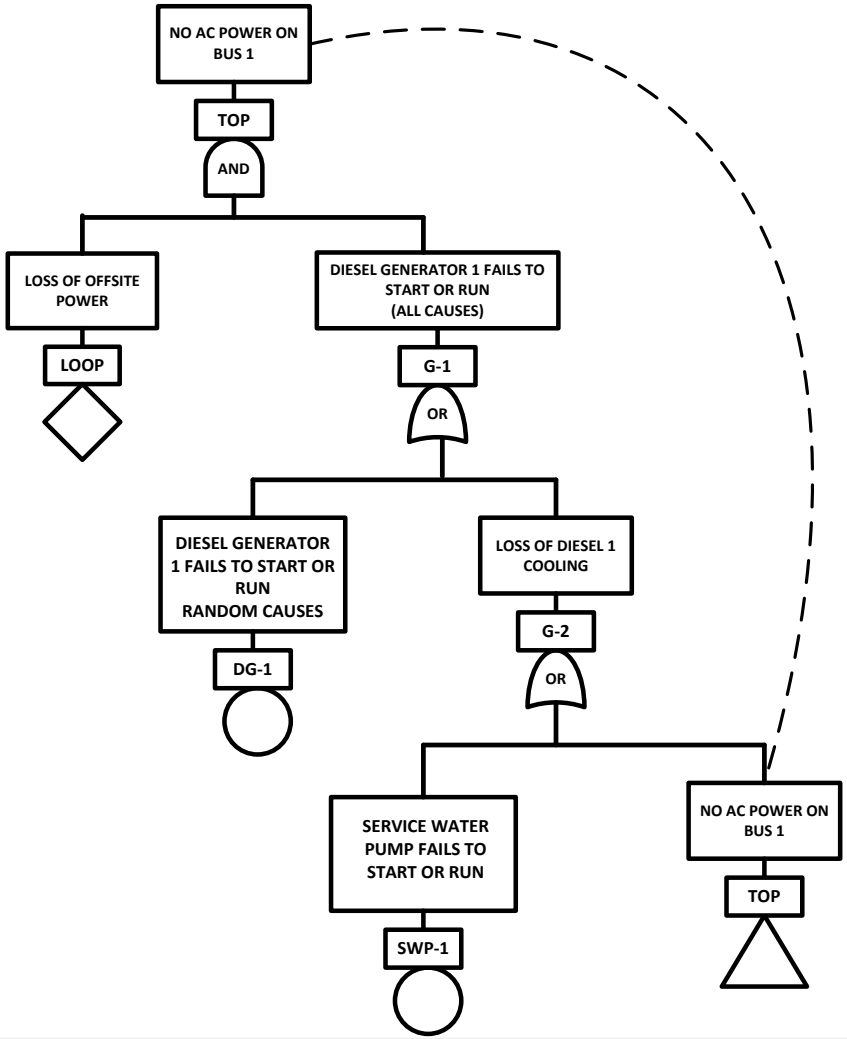
Min Cut Sets with tie breaker

1. MP-1, MP-2
2. DG-1, DG-2



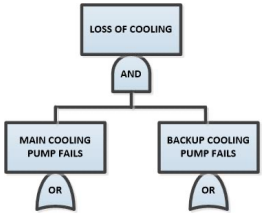
Logic Loops -- Cause Circular Logic in Fault Trees



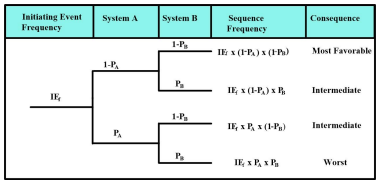


Service Water Pump Cools Diesel Engine

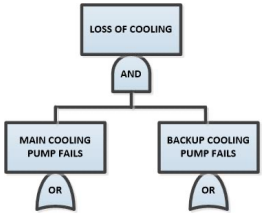
Logic loops is also considered for FTA of control systems



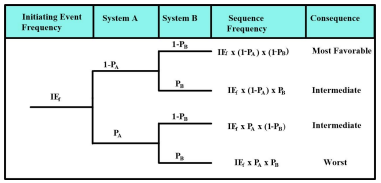
ACTIVE VERSUS PASSIVE COMPONENTS

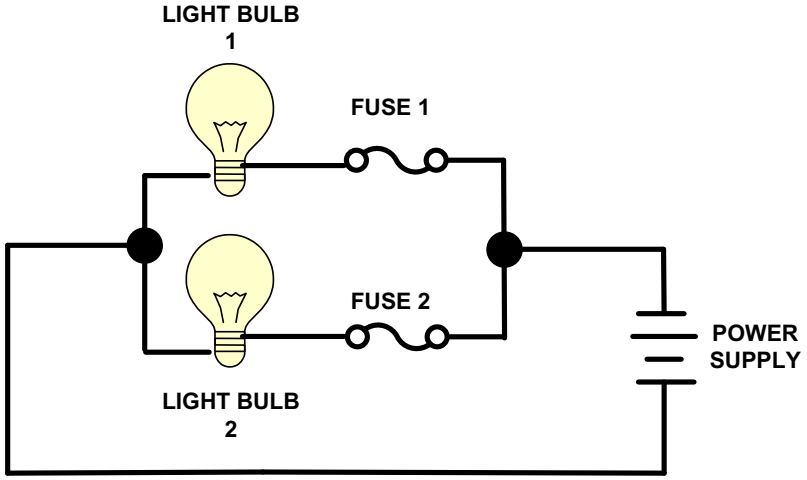


- ACTIVE COMPONENT MUST CHANGE STATE TO OPERATE
  - SWITCHES
  - VALVES
  - PUMPS
- PASSIVE COMPONENTS SUPPORT OR CONTAIN ENERGY
  - WIRES
  - PIPES
- Generally active component failures have a much higher failure probability than passive components
- INTERNAL VERSUS EXTERNAL EVENTS



LIGHT BULB SYSTEM WITH TWO SEPARATE FUSES





CUT SET NO.	ORDER	DESCRIPTION
1	1	POWER SUPPLY FAILURE
2	2	FUSE 1 OPEN FUSE 2 OPEN
3	2	LIGHT BULB 1 BURNED OUT LIGHT BULB 2 BURNED OUT
4	2	FUSE 1 OPEN LIGHT BULB 2 BURNED OUT
5	2	FUSE 2 OPEN LIGHT BULB 1 BURNED OUT

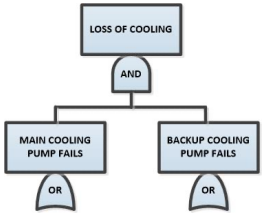
There are a total of 5 min cut sets

There is one min cut set of order 1

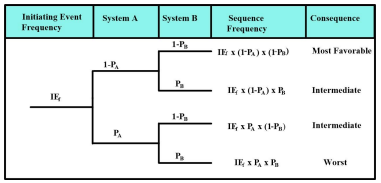
There are 4 min cut sets of order 2

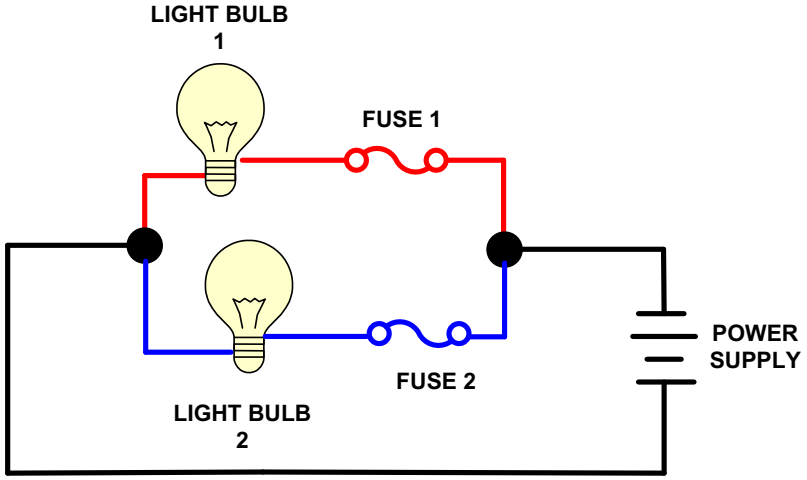
$2^N = 4$ where $N = 2$

Enabling events for min cut sets of order 2



Considering shorts and open circuits (passive failures)

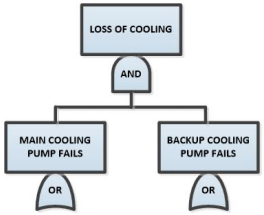




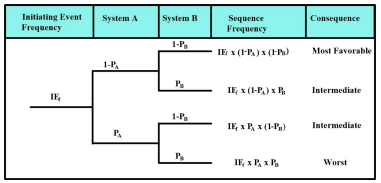
17 min cut sets --1 of order 1--16 of order 2

1. Power supply failure
2. Fuse 1 open & fuse 2 open
3. Fuse 1 open & light bulb 2 burned out
4. Fuse 1 open & wire 2 open circuit
5. Fuse 1 open & wire 2 short circuit
6. Fuse 2 open & light bulb 1 burned out
7. Fuse 2 open & wire 1 open circuit
8. Fuse 2 open & wire 1 short circuit
9. Light bulb 1 burned out & light bulb 2 burned out
10. Light bulb 1 burned out & wire 2 open circuit
11. light bulb 1 burned out & wire 2 short circuit
12. light bulb 2 burned out & wire 1 open circuit
13. light bulb 2 burned out & wire 1 short circuit
14. wire 1 open circuit & wire 2 open circuit
15. wire 1 open circuit & wire 2 short circuit
16. wire 1 short circuit & wire 2 open circuit
17. wire 1 short circuit & wire 2 short circuit

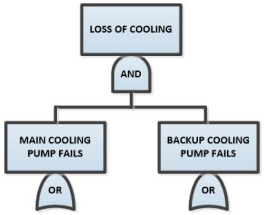
note, creates more min cut sets when passive failures are considered



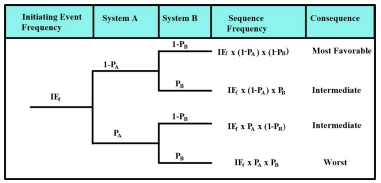
Common Cause Failure Analysis



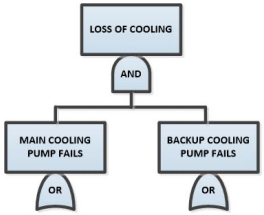
- Common Links Condition
  - Human
  - Hardware
  - Domain
- Maintenance Policies
- Alpha and Beta Factors
- System Configuration
  - Redundancy at the System Level
  - Redundancy at the Component Level
- Computer Analysis



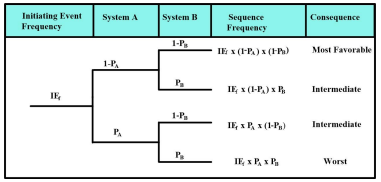
Common Cause Failure Analysis Human Dependency



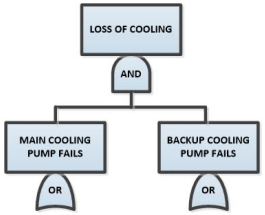
- No real redundancy for double light bulb system (Same person doing the same thing)
- Incorporate two person rule – checker
  - **1.0E-2** x **0.1** = **1.0E-3** (probability both fail)
- Testing, Maintenance and Calibration
  - Semi annual test (same technician/team each time)
  - Multi train system (same technician/team each time)
- Walk down and Inspections (First second and third try, i.e., repetitive actions)
  - **1.0E-2** x **0.1** x **1** = **1.0E-3** (probability three attempts fail)
- Automate turning on and off switches (Engineered Controls)



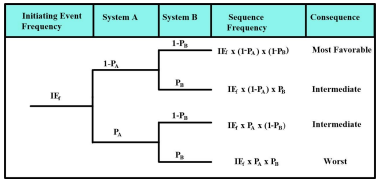
Performance Influencing Factors for Human Failure Events



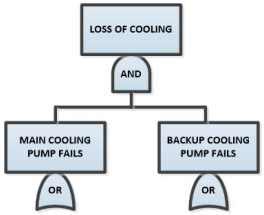
- Vulnerabilities are quite often associated with performance influencing factors (PIF)
  - Design of procedures and/or training
  - Job aids (e.g., special tools, remote cameras, binoculars)
  - Time pressure
  - Environmental conditions (e.g., noise, temperature extremes, protective clothing)
  - Prevention devices (e.g., limit switches, interlocks, mechanical stops)
  - Warning devices (e.g., alarms)
  - Task challenge (i.e., level of stimulation and interest)
  - Oversight/feedback (i.e., level of teamwork)



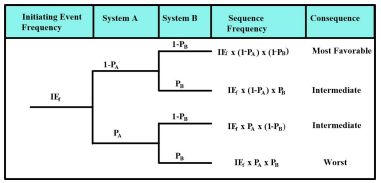
Human Error precursors



Work	Individual
• Distractions / Interruptions	• Unfamiliarity with task / First time
• Changes / Departures from routine	• Lack of knowledge (mental model)
• Confusing displays or controls	• New technique not used before
• Workarounds / Out-of-service instruments	• Imprecise communication habits
• Hidden system response	• Lack of proficiency / Inexperience
• Unexpected equipment conditions	• Indistinct problem-solving skills
• Lack of alternative indication	• "Hazardous" attitude for critical task
• Personality conflicts	• Illness / Fatigue
Task	**Human**
• Time pressure (in a hurry)	• Stress (limits attention)
• High workload (memory requirements)	• Habit patterns
• Simultaneous, multiple tasks	• Assumptions (inaccurate mental picture)
• Repetitive actions, monotonous	• Complacency / Overconfidence
• Irrecoverable acts	• Mindset ("tuned" to see)
• Interpretation requirement	• Inaccurate risk perception (Pollyanna)
• Unclear goals, roles and responsibilities	• Mental shortcuts (biases)
• Lack of clear standards	• Limited short-term memory



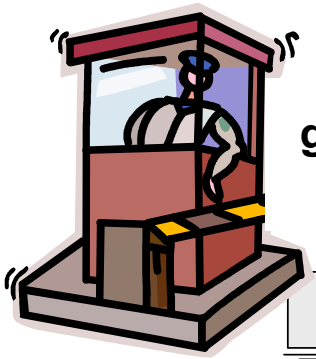
Trench incident December 1979



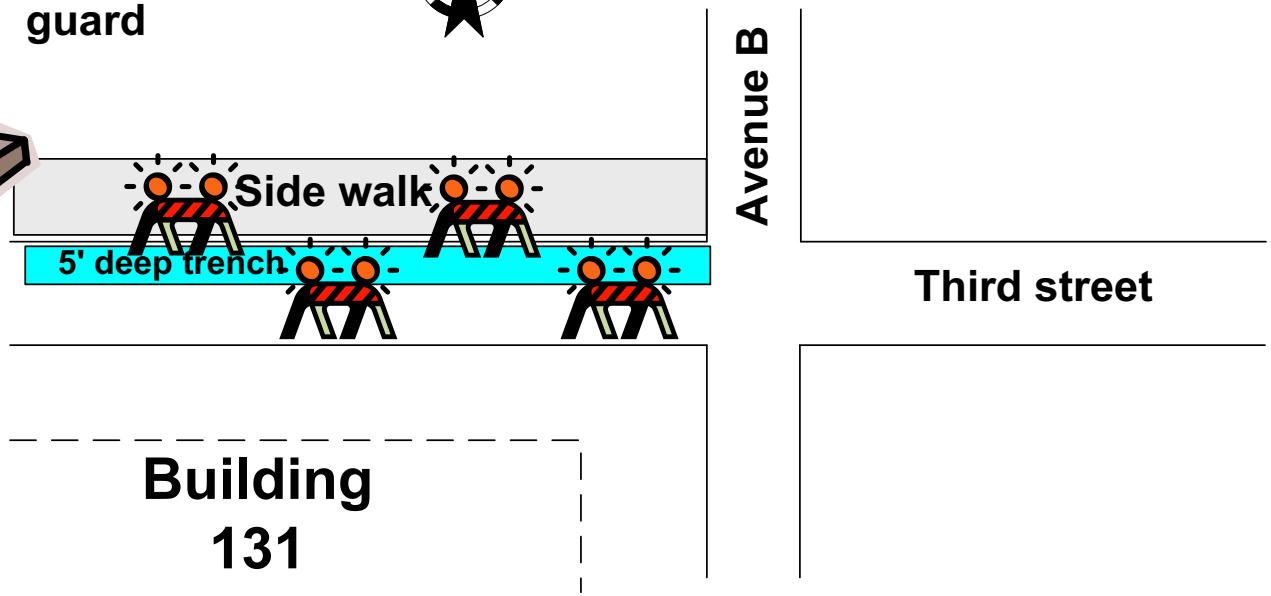
December 1979
5:40 PM
5:50 PM
5:59 PM

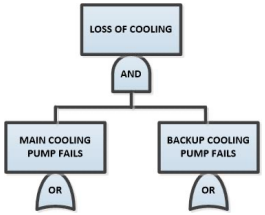
CONTROLS:

1. GUARD
2. BARRICADES WITH LIGHTS
3. YELLOW TAPE (NOT SHOWN)

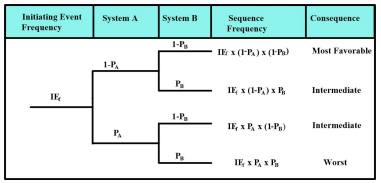


guard



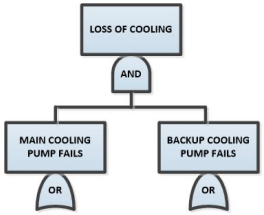


Overview – Dependent and Common Cause Failures

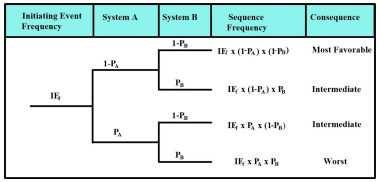


- Dependent failures are often significant contributors to the overall risk results.

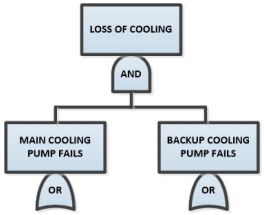
- Examples of dependent failures:
  - Common Cause Failures (CCFs)
  - Shared equipment (e.g., support system) failures
  - Physical / spatial interactions (e.g., common location, fire and flood area)
- Human interactions (instrument miscalibration, valve mispositioning)
- Dependency matrices are typically used to identify system/component dependence on support systems such as power and cooling.
- Dependent failures & common cause events are modeled explicitly in the fault trees by inclusion of appropriate external Fault Tree transfers and CCF basic events.



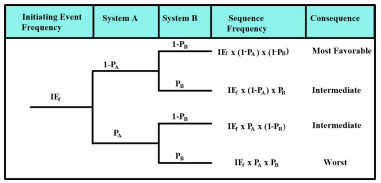
Common Cause Failure Analysis Hardware Dependency



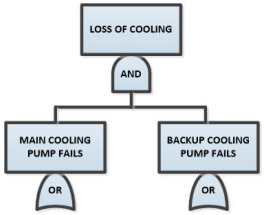
- Common Manufacturer
- Physical Domains (can involve dissimilar components in same min cut set)
  - — Internal events (e.g., flooding, cold weather, missiles)
  - — External events
    - Seismic (foundation bolts missing or deficient)
    - Seismic (Fire Wall falls down)
    - Fire (cables erroneously located in same cable tray)



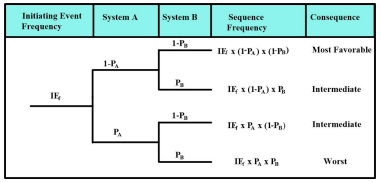
Generic Causes of dependent failures



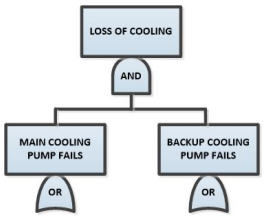
Generic cause	Example of source
Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure
Vibration	Machinery in motion, earthquake
Pressure	Explosion, out-of-tolerance system changes (pump overspeed, flow blockage)
Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from control system
Moisture	Condensation, pipe rupture, rainwater
Stress	Thermal stress at welds of dissimilar metals
Temperature	Fire, lightning, welding equipment, cooling-system faults, electrical short-circuits
Freezing	Water freezing
Electromagnetic interference	Welding equipment, rotating electrical machinery, lightning, power supplies, transmission lines
Radiation damage	Neutron sources, charged-particle radiation
Conducting medium	Conductive gases
Out-of-tolerance voltage	Power surge
Out-of-tolerance current	Short-circuit, power surge
Corrosion (acid)	Boric acid from chemical control system, acid used in maintenance for rust removal and cleaning
Corrosion (oxidation)	In a water medium or around high-temperature metals (e.g., filaments)
Other chemical reactions	Galvanic corrosion; complex interactions of fuel cladding, water, oxide fuel, and fission products
Biological hazards	Poisonous gases, explosions, missiles



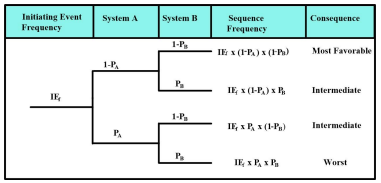
Special conditions

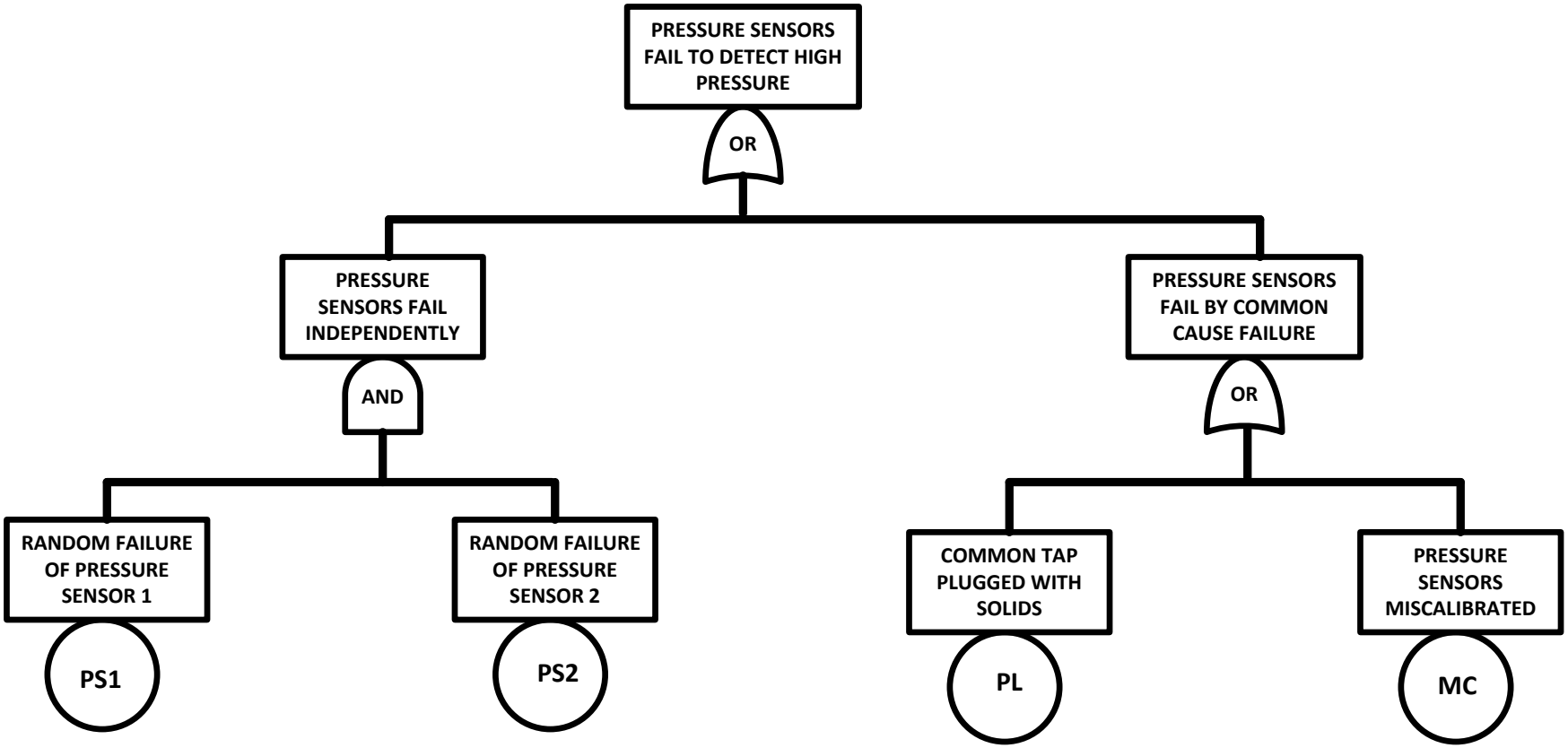


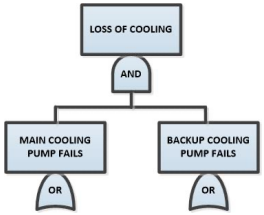
Special conditions	Example of source
Calibration	Misprinted calibration instructions
Installation contractor	Same subcontractor or crew
Maintenance	Incorrect procedure, inadequately trained personnel
Operator or operation	Operator disabled or overstressed, faulty operating procedures
Proximity	Location of components in one cabinet (common location exposes all of the components to many unspecified common causes)
Test procedure	Faulty test procedures that may affect all components normally tested together



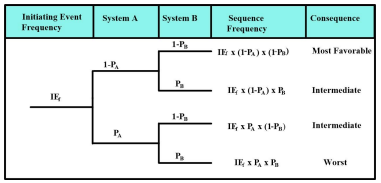
Explicit Modeling
Common Cause Failure Analysis



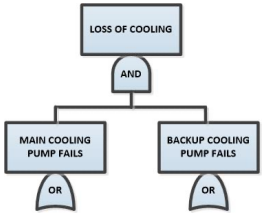




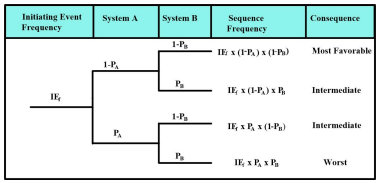
Alpha Factor Analysis (implicit modeling)



- Probability diesel generator fails to start upon demand
  $q_d = 8 \times 10^{-3}$
- Probability that two diesel generators fail to start upon demand (assuming independence) $q_d^2 = (8 \times 10^{-3})^2 = 6 \times 10^{-5}$
- Alpha analysis allows for dependency based upon observing actual data for a system with 2 or more trains



Example -- Alpha Factor Analysis Two Diesel Generator System



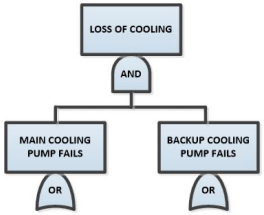
$N_t = N_0 + N_1 + N_2$

N_t = total number of starts (trials) for the two train system (a trial requires the start of two diesel generators)

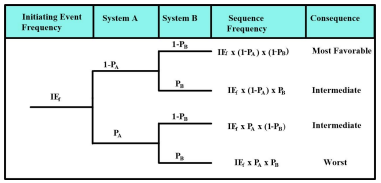
N_0 = total number of starts with no failures

N_1 = total number of starts with exactly one failure or two independent failures

N_2 = total number of starts with two common cause failures



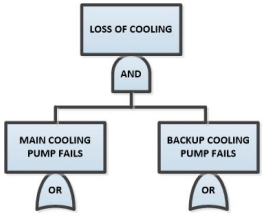
Alpha Factor Analysis Two Diesel Generator System



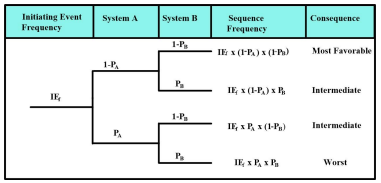
$q_d = (N_1 + N_2)/N_t$ (Probability that a diesel generator will fail to start on demand all causes)

$\alpha_1 = N_1/(N_1 + N_2) = 0.95$ (failure due to independent causes)

$\alpha_2 = N_2/(N_1 + N_2) = 0.05$ (failure due to common cause failures)



Alpha Factor Analysis
Two Diesel Generator System



Probability that both diesels fail upon demand using alpha factors
= Probability that two diesels fail to start
= P(independent causes + common causes)

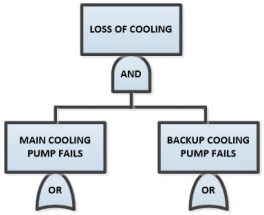
$= (q_d \times \alpha_1)^2 + q_d \times \alpha_2$

$= (8 \times 10^{-3} \times .95)^2 + 8 \times 10^{-3} \times .05$

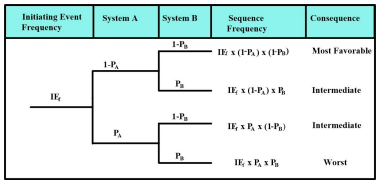
$= 5.8 \times 10^{-5} + 4.0 \times 10^{-4}$

$= 4.6 \times 10^{-4}$

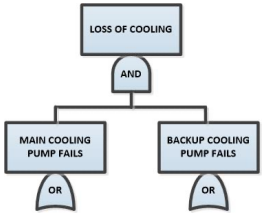
A factor of $4.6 \times 10^{-4} / 5.9 \times 10^{-5} \approx 7$ greater than assuming independence only



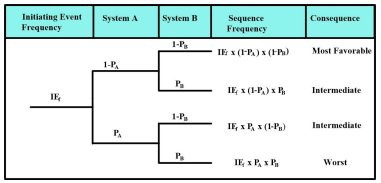
Common Cause Failure Analysis



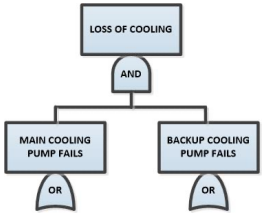
- Generally common Cause Failure Analysis considers failure components in standby
- The analysis should also consider the effect of the initiating event on failure of components in standby, e.g., secondary failures



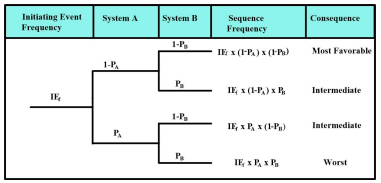
COMPARISON OF CCF DATABASES



Database Parameter	EPRI-NP-3967	NUREG/CR-6268
Data Recording Period	1972-83	1980-95
Sources of Data	LERs	LERs and NPRDS
Number of Data Records Analyzed	2,654	39,910
Number of Independent Failures	2,232	16,586
Number of Common Cause Events	113	1,533
Number of Common Cause Failure Events in which all redundant components failed	68	235

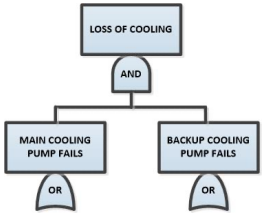


Maintenance Unavailability Data

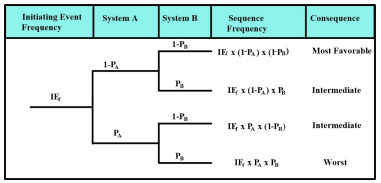


Component Type	Unavailability Mode	Demand / Hourly	Code	Mean Value	Error Factor
Emergency Diesel Generator	Emergency Diesel Generator Test or Maintenance	**d**	**M**	1.2E-02	**2.1**
Heat Exchanger	Heat Exchanger Test or Maintenance (CCW)	**d**	**M**	7.0E-03	**4.3**
	Heat Exchanger Test or Maintenance (RHR-PWR) "	**d**	**M**	5.0E-03	**2.5**
Motor-driven Pump	Motor-Driven Pump Test or Maintenance (AFWS)	**d**	**M**	4.0E-03	**2.5**
	Motor-Driven Pump Test or Maintenance (CCW)	**d**	**M**	6.0E-03	**3.8**
	Motor-Driven Pump Test or Maintenance (ESW)	**d**	**M**	1.2E-02	**4.3**
	Motor-Driven Pump Test or Maintenance (Other)	**d**	**M**	8.0E-03	**4.3**
Turbine-driven Pump	Turbine-Driven Pump Test or Maintenance (AFWS)	**d**	**M**	5.0E-03	**2.8**

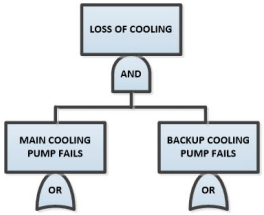
Ref. Data Derived from NUREG/CR-6928



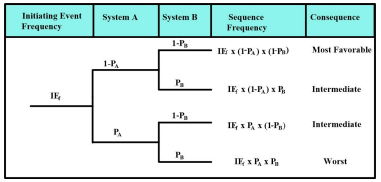
Calculation Types for Computer Code CAFTA



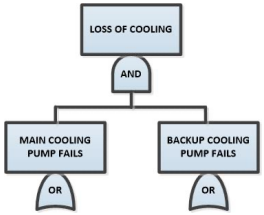
Calculation Type	Form	Equation	Notes
0	Probability	Q	Used when there is no failure rates. Often used for human error probabilities.
1	Ratio	$\lambda * \tau$	Failure rate times a factor. E.g. failure rate per meter times the number of meters. Sometimes used as an approximation to calculation types 3 and 4
2	Approximate Average Unavailability	$\frac{\lambda * \tau}{2}$	Approximation of average unavailability between tests. Calculation type 5 is preferred.
3	Mission Time	$1 - e^{-\lambda t}$	Probability of failure during a mission (unreliability), t = mission time.
4	Detectable and Repairable	$\frac{\lambda \tau}{\lambda \tau + 1}$	Asymptotic unavailability, given repair. Assumes that the failure is detectable, x = average repair time
5	Tested Equipment	$1 + \frac{1}{\lambda \tau}(e^{-\lambda \tau} - 1)$	Average unavailability between tests. Assumes the component is known to be "perfect" after each test. T = test interval. Sometimes calculation type 2 ($\lambda * t/2$) is used to approximate this.
6	Repair and Mission	$\frac{\lambda \tau}{\lambda \tau + 1}(1 - e^{-(\lambda + \frac{1}{\tau})t})$	Probability of failure during a mission with repair, λ = average repair time
9	Initiator	F	Initiating Event frequency
+/-	True/False	1.0/0.0	Sets the probability of the event to 1 or 0 in all locations



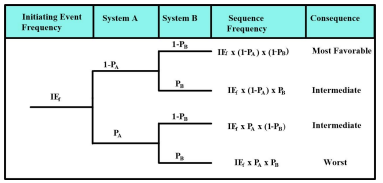
Two types of Failure



- Two lights for reactor – one off and one on? Is the reactor on or off?
- Toyota 2004 Camry
  - Air Bag Status
    - No display when no one is sitting in the seat
    - Display “air bag off” sign when light weight passenger sits in seat
    - Display “air bag on” sign when heavy weight passenger sits in seat
  - For my car “air bag off sign” appears all the time
    - Mechanic says that weight sensor system failed low
    - Air bag is disabled in this case
    - No preferred failure mode for this weight sensor



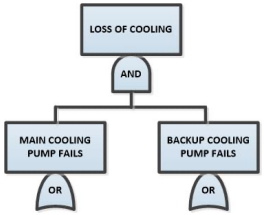
Failure Modes and Effects Analysis



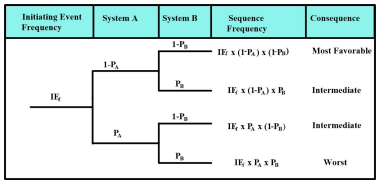
Sys-tem	Sub-system	Compon-ent Identi-fication	Function	Failure Mode (How does it fail)	Failure Mechanism (Why does it fail)	Effect on Subsystem /System (Is failure in safe or unsafe direction)	Method of Detection	Criticality	Remarks (What inherent provisions are provided in the design to compensate for the failure.)
Auto	Pass-enger side Air Bag System	Weight Sensor	Activates system when passenger weight exceeds 70lb	False Low Reading	Fatigue Out of calibration Connector failure	Air bag always disabled	Air bag light warning light always indicates "Off"	Marginal	Passenger wears seat belt no fail safe (preferred) failure mode for weight sensor
				False High Reading	Fatigue Out of calibration	Air bag always enabled	Air bag light warning light always indicates "On"	Marginal	Light weight passenger can sit in back seat

Criticality Ranking:

1. Catastrophic – Loss of life/system
2. Critical – potential for Loss of life/system-- requires immediate action
3. Marginal – Degradation of a system safety function
4. Negligible – no or little effect



K out N systems (Duality Principle)



- Success Criteria
  - K = number of components that must work for system success
  - N = Number of system components
  - C(N,K) = N!/K!(N-K)!] = Number of Path Sets
  - K = order of the path sets
- Failure Criteria
  - N-K+1 = number of components that must fail for system for system failure
  - C(N,N-K+1) = N!/[(N-K+1)!(K-1)!] = Number of Cut Sets
  - N-K+1 = order of min cut sets

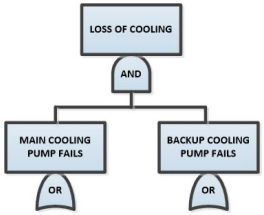
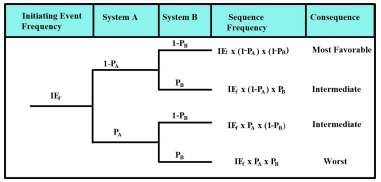
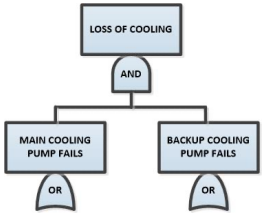


Table for a 2,3 and 4 component system

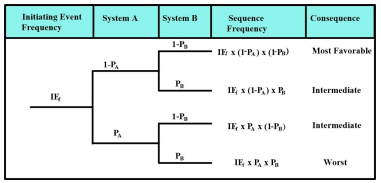


Number of components	System	Success Criteria	Success Logic	No. of Path Sets	Order of min Path Sets	Failure Criteria	Failure logic	No. of min cut sets	Order of Min Cut sets
2	Parallel	1 out of 2	OR	2	1	2 out of 2	AND	1	2
2	Series	2 out of 2	AND	1	2	1 out of 2	OR	2	1
3	Parallel	1 out of 3	OR	3	1	3 out of 3	AND	1	3
3	**K out of N**	**2 out of 3**	**K out of N**	**2**	**2**	**2 out of 3**	**K out of N**	**2**	**2**
3	Series	3 out of 3	AND	1	3	1 out of 3	OR	3	1
4	Parallel	1 out of 4	OR	4	1	4 out of 4	AND	1	4
4	**K out of N**	**2 out of 4**	**K out of N**	**6**	**2**	**3 out of 4**	**K out of N**	**4**	**3**
4	K out of N	3 out of 4	K out of N	4	3	2 out of 4	K out of N	6	2
4	Series	4 out of 4	AND	1	4	1 out of 4	OR	4	1

Path Set Also indicates how the system can spuriously activate



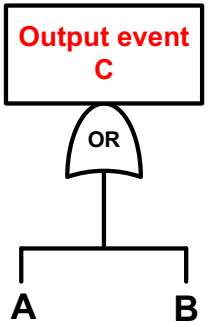
AND and OR GATES WITH TWO INPUT EVENTS



RELIABILITY NETWORK REPRESENTATION (SYSTEM)

SERIES SYSTEM 2 COMPONENTS

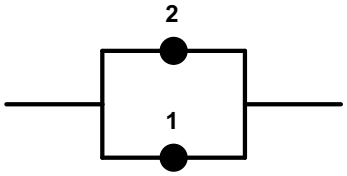
OR GATE TWO INPUTS



TRUTH TABLE

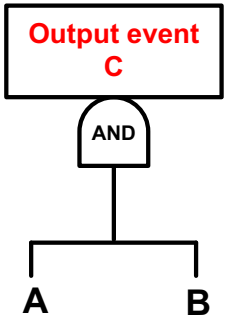
A	B	C
FALSE	FALSE	FALSE
FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	TRUE

A	B	C
0	0	0
0	1	1
1	0	1
1	1	1

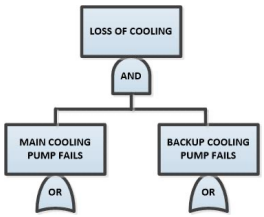


PARALLEL SYSTEM 2 COMPONENTS

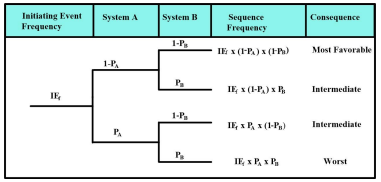
AND GATE TWO INPUTS



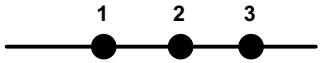
A	B	C
0	0	0
0	1	0
1	0	0
1	1	1



THREE EVENT OR THREE COMPONENT SYSTEM

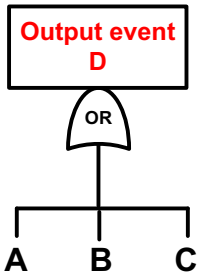


RELIABILITY NETWORK REPRESENTATION (SYSTEM)



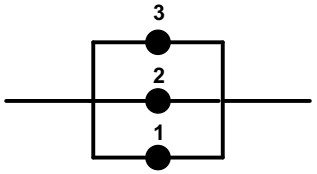
SERIES SYSTEM
3 COMPONENTS

OR GATE THREE INPUTS



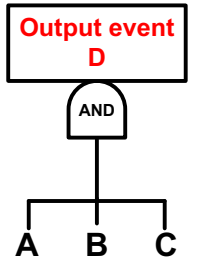
TRUTH TABLE

A	B	C	D
0	0	0	0
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
1	0	1	1
0	1	1	1
1	1	1	1

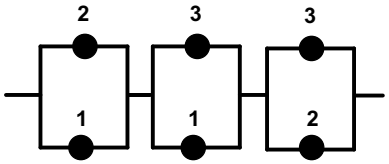


PARALLEL SYSTEM
2 COMPONENTS

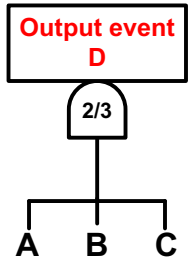
AND GATE THREE INPUTS



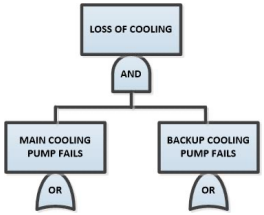
A	B	C	D
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	0
1	1	0	0
1	0	1	0
0	1	1	0
1	1	1	1



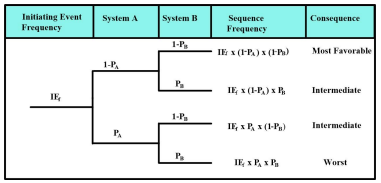
2 OUT OF 3 GATE
K=2
N=3



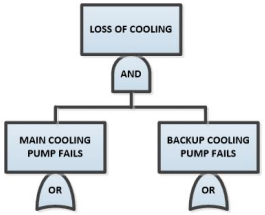
A	B	C	D
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	0
1	1	0	1
1	0	1	1
0	1	1	1
1	1	1	1



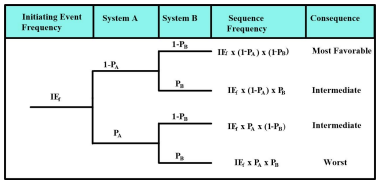
Initiating event fault tree analysis



- Initial conditions
- Initiating events
- Enabling events
- System Unavailability
- Critical system state
- Top Event occurrence frequency
- Assumptions
- Two and three component systems

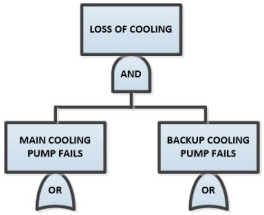


System Failure Frequency W_s

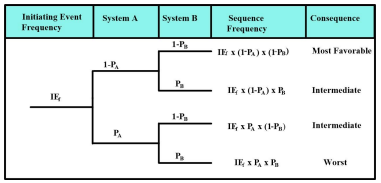


$$W_s = \sum_{i=1}^{n} \left[\text{Probability that the system is in a critical system state for component i} \right] \left[\text{Failure frequency for component i} \right]$$

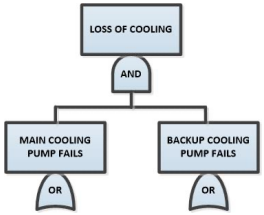
where n = number of components (initiating events)



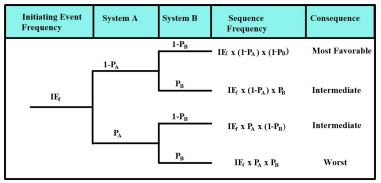
Initiating Event importance measures



- Determined by a ratio
- Denominator is $W_S(T)$
- Conditional probability
- Initiating events
- Enabling events
- Min cut sets

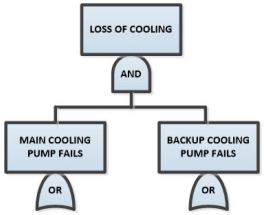


Assumptions and Nomenclature

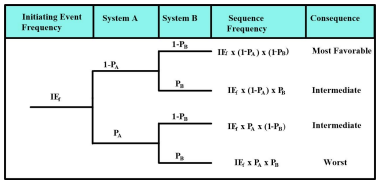


- Component failures are s-independent
- Two states success and failure
- Probability of component success is p
  - p_1 component A works, A_W
  - p_2 component B works, B_W
  - p_3 component C works, C_W
- Probability of component failure is q
  - q_1 component A fails, A_F
  - q_2 component B fails, B_F
  - q_3 component C fails, C_F

- Initial conditions system runs at steady state



Component Basic Event Data

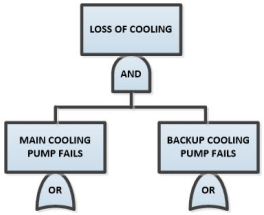


- Time Related
- Demand Related

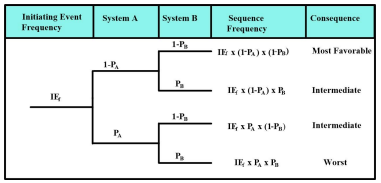
Two Types

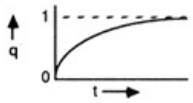
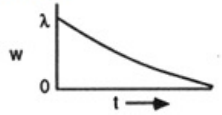
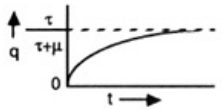
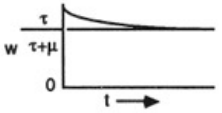
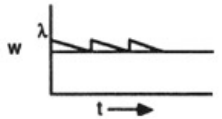
Enabling Event Unavailability q

Initiating Event Failure Frequency λ



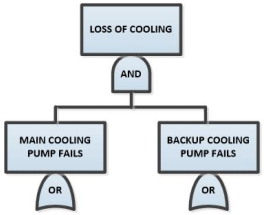
Time Related Component Unavailability q and Failure frequency λ



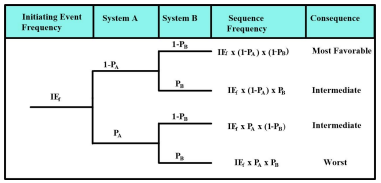
MAINTEN-ANCE POLICY	COMPONENT UNAVAILABILITY q*	ASYMPTOTIC VALUE	COMPONENT UNAVAILABILITY VERSUS TIME	COMPONENT FAILURE FREQUENCY w	ASYMP-TOTIC VALUE	COMPONENT FAILURE FREQUENCY VERSUS TIME
1. No Repair	$1 - e^{-\lambda t} < \lambda t$	1		$\lambda e^{-\lambda t}$	0	
2. Repair Announced Failure	$\frac{\tau}{\mu+\tau}\left(1 - e^{\left(-\frac{\mu+\tau}{\mu\tau}t\right)}\right)$	$\frac{\tau}{\mu+\tau} < \lambda\tau$		$\frac{1}{\mu+\tau}\left[1 - \frac{\tau}{\mu}e^{-\left(\frac{\mu+\tau}{\mu\tau}\right)t}\right]$	$\frac{1}{\mu+\tau}$	
3. Repair Unannounced Failure	$1 - e^{\left[-\lambda(t-(n-1)\phi\right]}$ $(n-1)\phi \le t \le n\theta$ $n = 1, 2, 3, \ldots$	$\frac{\lambda\phi}{2} + \frac{\tau}{\tau+\phi}$ (Average Unavailability)		$\lambda e^{\left[-\lambda(t-(n-1)\phi\right]}$ $(n-1)\phi \le t \le n\theta$ $n = 1, 2, 3, \ldots$	$\lambda e^{-\frac{\lambda\phi}{2}} < \lambda$	

*μ = mean time to failure
τ = mean time to restore
θ = Scheduled Inspection Interval

λ in many cases is an accurate approximation for component failure frequency



OR gate with two inputs

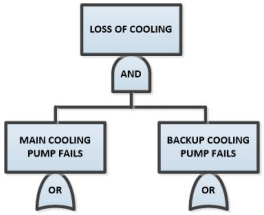


SYSTEM STATE	A	B	C TOP EVENT	TOP EVENT PROBABILITY
1	WORKS	WORKS	FALSE	p_1p_2
2	WORKS	FAILS	TRUE	p_1q_2
3	FAILS	WORKS	TRUE	q_1p_2
4	FAILS	FAILS	TRUE	q_1q_2

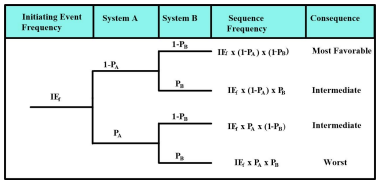
SYSTEM STATE	A	B	C TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	p_1p_2
2	0	1	1	p_1q_2
3	1	0	1	q_1p_2
4	1	1	1	q_1q_2

Two min cut sets of order 1 $\{A_f\}, \{B_f\}$

TOP EVENT PROBABILITY $Q_T = q_1 + q_2 - q_1q_2 < q_1 + q_2$



OR gate with two inputs -- critical system state



SYSTEM STATE	B	CRITICAL SYSTEM STATE?	PROBABILITY
1	0	YES	p_2
2	1	NO	q_2

- Probability that the system in a critical system state for component A = $p_2 = 1 - q_2$ --
- Birnbaum's measure of component importance $\partial Q/\partial q$, $Q_T(q_1=1) - Q_T(q_1=0)$
- Assume that either component A or B can be initiating events,
- Assume that their failure frequency is given by their failure rates

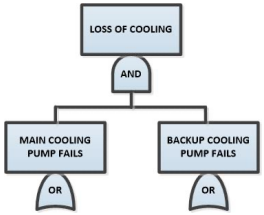
  $w_1(t) = \lambda_1$ Component A

  $w_2(t) = \lambda_2$ Component B
- Top event failure frequency $W_T(t)$ is

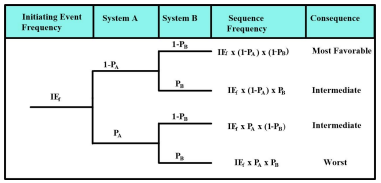
  $W_T(t) = \lambda_1 p_2 + \lambda_2 p_1 < \lambda_1 + \lambda_2$
- Initiating event importance

  $I_1(t) = \lambda_1/(\lambda_1 + \lambda_2)$ Component A

  $I_2(t) = \lambda_2/(\lambda_1 + \lambda_2)$ Component B



Exclusive OR gate with two inputs



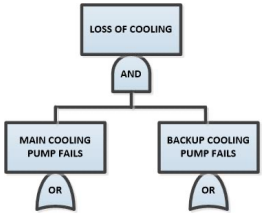
SYSTEM STATE	A	B	C TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	p_1p_2
2	0	1	1	p_1q_2
3	1	0	1	q_1p_2
4	1	1	0	q_1q_2

Two prime implicants of order 2 $\{A_F B_W\}$ $\{A_W B_F\}$

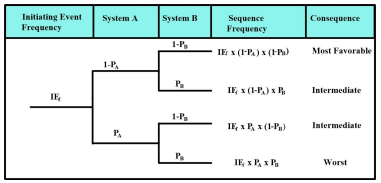
- Top event probability

  $Q_T = q_1 + q_2 - 2q_1q_2 < q_1 + q_2$
- Critical system state unavailability component A = p_2
- Birnbaum's measure of importance does not work since the logic is not coherent
- Top Event Occurrence frequency

  $W_T(t) = p_2 \lambda_1 + p_1 \lambda_2 < \lambda_1 + \lambda_2$



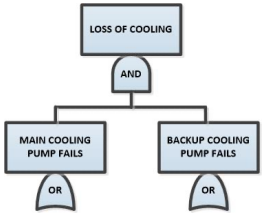
AND gate with two inputs



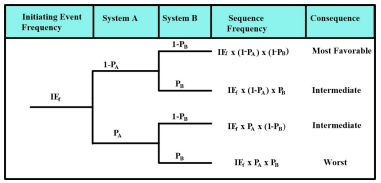
SYSTEM STATE	A	B	C TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	p_1p_2
2	0	1	0	p_1q_2
3	1	0	0	q_1p_2
4	1	1	1	q_1q_2

One min cut set of order 2 $\{A_F, B_F\}$

Top event probability = q_1q_2



AND gate with two inputs -- critical system state



SYSTEM STATE	B	CRITICAL SYSTEM STATE?	PROBABILITY
1	0	NO	p_2
2	1	**YES**	q_2

- Probability that the system in a critical system state for component A = q_2
- Top Event Occurrence Frequency

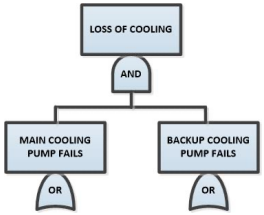
  $W_T(t) = \lambda_1 q_2 + \lambda_2 q_1$
- Initiating event importance

  $I_1(t) = \lambda_1 q_2/(\lambda_1 q_2 + \lambda_2 q_1)$ component A

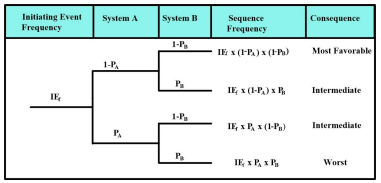
  $I_2(t) = \lambda_2 q_1/(\lambda_1 q_2 + \lambda_2 q_1)$ component B
- Enabling event importance

  $E_1(t) = \lambda_2 q_1/(\lambda_1 q_2 + \lambda_2 q_1)$ Component A

  $E_2(t) = \lambda_1 q_2/(\lambda_1 q_2 + \lambda_2 q_1)$ Component B



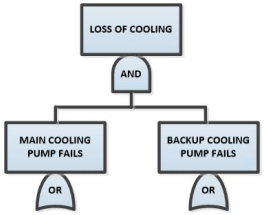
OR gate with three inputs



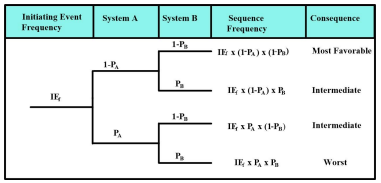
SYSTEM STATE	A	B	C	D TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	0	$p_1p_2p_3$
2	1	0	0	1	$q_1p_2p_3$
3	0	1	0	1	$p_1q_2p_3$
4	0	0	1	1	$p_1p_2q_3$
5	1	1	0	1	$q_1q_2p_3$
6	1	0	1	1	$q_1p_2q_3$
7	0	1	1	1	$p_1q_2q_3$
8	1	1	1	1	$q_1q_2q_3$

Three min cut sets of order 1 $\{A_F\}$ $\{B_F\}$ $\{C_F\}$

Top event probability = $q_1 + q_2 + q_3 - q_1q_2 - q_1q_3 - q_2q_3 + q_1q_2q_3 < q_1 + q_2 + q_3$



OR gate with three inputs -- critical system state



SYSTEM STATE	B	C	CRITICAL SYSTEM STATE?	TOP EVENT PROBABILITY
1	0	0	YES	p_2p_3
2	0	1	NO	p_2q_2
3	1	0	NO	q_2p_3
4	1	1	NO	q_1q_2

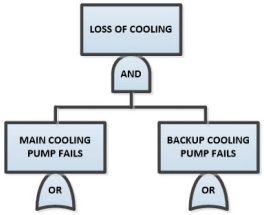
- Probability that the system in a critical system state for component A = $p_2p_3 < 1$
- Top Event Occurrence Frequency

  $W_T(t) = p_2p_3\lambda_1 + p_1p_3\lambda_2 + p_1p_2\lambda_3 < \lambda_1 + \lambda_2 + \lambda_3$
- Initiating event importance

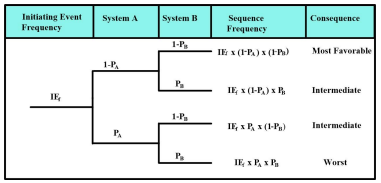
  $I_1(t) = \lambda_1/(\lambda_1 + \lambda_2 + \lambda_3)$ component A

  $I_2(t) = \lambda_2/(\lambda_1 + \lambda_2 + \lambda_3)$ component B

  $I_3(t) = \lambda_3/(\lambda_1 + \lambda_2 + \lambda_3)$ component C

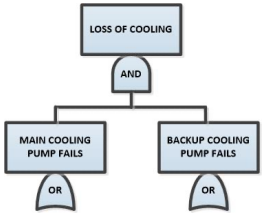


AND gate with three inputs

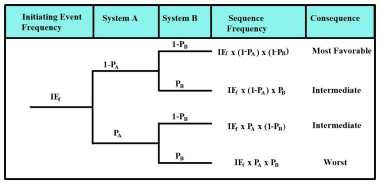


SYSTEM STATE	A	B	C	D TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	0	$p_1p_2p_3$
2	1	0	0	0	$q_1p_2p_3$
3	0	1	0	0	$p_1q_2p_3$
4	0	0	1	0	$p_1p_2q_3$
5	1	1	0	0	$q_1q_2p_3$
6	1	0	1	0	$q_1p_2q_3$
7	0	1	1	0	$p_1q_2q_3$
8	1	1	1	1	$q_1q_2q_3$

TOP EVENT PROBABILITY = $q_1q_2q_3$



Critical System State AND gate with three inputs



SYSTEM STATE	B	C	CRITICAL SYSTEM STATE?	TOP EVENT PROBABILITY
1	0	0	NO	p_2p_3
2	0	1	NO	p_2q_2
3	1	0	NO	q_2p_3
4	1	1	**YES**	q_1q_2

- Probability that the system in a critical system state for component A= $q_2\ q_3$
- Top Event Occurrence Frequency

  $W_T(t) = \lambda_1 q_2 q_3 + \lambda_2 q_1 q_3 + \lambda_3 q_1 q_2$
- Initiating Event Importance

  $I_1(t) = \lambda_1 q_2 q_3 / W_T(t)$ component A

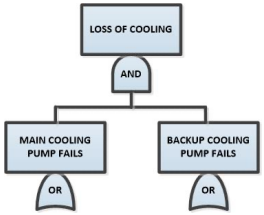
  $I_2(t) = \lambda_2 q_1 q_3 / W_T(t)$ component B

  $I_3(t) = \lambda_3 q_1 q_2 / W_T(t)$ component C
- Enabling Event Importance

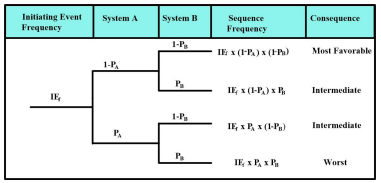
  $E_1(t) = (\lambda_2 q_1 q_3 + \lambda_3 q_1 q_2) / W_T(t)$ component A

  $E_2(t) = (\lambda_1 q_2 q_3 + \lambda_3 q_1 q_2) / W_T(t)$ component B

  $E_3(t) = (\lambda_1 q_2 q_3 + \lambda_2 q_1 q_3) / W_T(t)$ component C



Two out of three gate



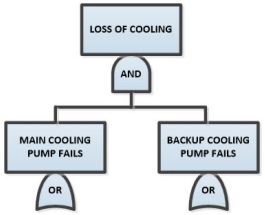
SYSTEM STATE	A	B	C	D TOP EVENT	TOP EVENT PROBABILITY
1	0	0	0	0	$p_1p_2p_3$
2	1	0	0	0	$q_1p_2p_3$
3	0	1	0	0	$p_1q_2p_3$
4	0	0	1	0	$p_1p_2q_3$
5	1	1	0	**1**	$q_1q_2p_3$
6	1	0	1	**1**	$q_1p_2q_3$
7	0	1	1	**1**	$p_1q_2q_3$
8	1	1	1	**1**	$q_1q_2q_3$

Three min cut sets of order 2 $\{A_FB_F\}$ $\{A_FC_F\}$ $\{B_FC_F\}$

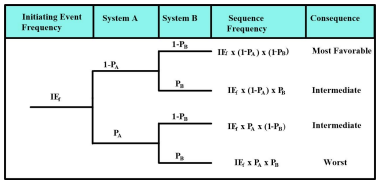
- Top event probability = $q_1q_2 + q_1q_3 + q_2q_3 - 2\,q_1q_2q_3 < q_1q_2 + q_1q_3 + q_2q_3$
- Min cut set upper bound

$$1 - (1 - q_1q_2)(1- q_1q_3)(1- q_2q_3) = q_1q_2 + q_1q_3 + q_2q_3 - q_1q_2\,q_1q_3 - q_1q_2\,q_2q_3 - q_1q_3\,q_2q_3 + q_1q_2\,q_1q_3\,q_2q_3 =$$

$$q_1q_2 + q_1q_3 + q_2q_3 - q_1^2q_2q_3 - q_1q_2^2q_3 - q_1q_2q_3^2 + q_1^2q_2^2q_3^2$$

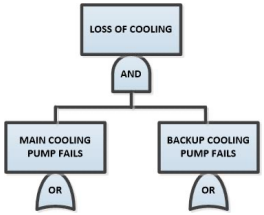


Two out of three gate with three inputs -- critical system state

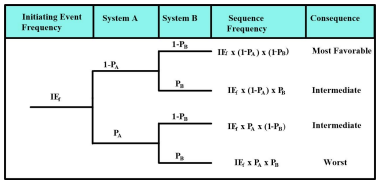


SYSTEM STATE	B	C	CRITICAL SYSTEM STATE?	TOP EVENT PROBABILITY
1	0	0	NO	p_2p_3
2	0	1	YES	p_2q_2
3	1	0	YES	q_2p_3
4	1	1	NO	q_1q_2

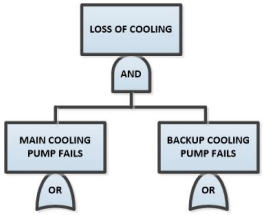
- Probability that the system in a critical system state for component A =
  $q_2(1-q_3) + q_3(1-q_2) = q_2+ q_3 - 2q_2q_3 < q_2+ q_3 - q_2q_3 < q_2+ q_3$
- Top Event Occurrence Frequency
  $W(t) = \lambda_1(q_2 +q_3) + \lambda_2 (q_1 + q_3) + \lambda_3 (q_1 +q_2)$
- Initiating Event Importance
  $I_1(t) = \lambda_1(q_2 +q_3)/W_T(t)$ component A
  $I_2(t) = \lambda_2(q_1 + q_3)/W_T(t)$ component B
  $I_3(t) = \lambda_3 (q_1 + q_2)/W_T(t)$ component C
- Enabling Event Importance
  $E_1(t) = q_1(\lambda_2 + \lambda_3) /W_T(t)$ component A
  $E_2(t) = q_2(\lambda_1 + \lambda_3) /W_T(t)$ component B
  $E_3(t) = q_3(\lambda_1 + \lambda_2) /W_T(t)$ component C
- Min Cut Set Importance
  $MCS_1 = (\lambda_1q_2 + \lambda_2 q_1) /W_T(t)$ $\{A_FB_F\}$
  $MCS_2 = (\lambda_1q_3 + \lambda_3 q_1)/W_T(t)$ $\{1,3\}$ $\{A_FC_F\}$
  $MCS_3 = (\lambda_2q_3 + \lambda_3 q_2)/W_T(t)$ $\{B_FC_F\}$



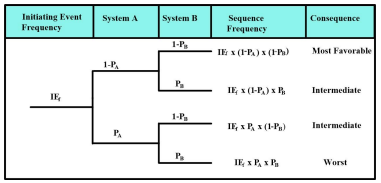
Bounds to Probability of the Boolean Union of Min Cut Sets



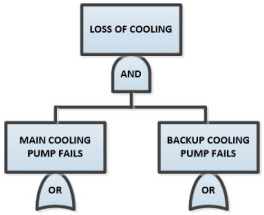
- Assume Basic Events are statistically independent
- Probability of the top event
- Pr(Exact Solution) ≤ Min Cut set Upper Bound<Rare Event Approximation
- Min Cut set Upper Bound = $1- \prod_{k} (1-Pr\{MCS_k\})$
- Rare Event Approximation = $\sum_{k} Pr(MCS_k)$



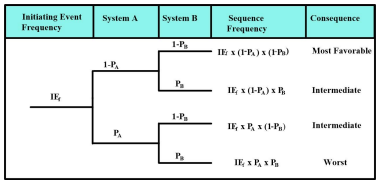
NIF Reliability Goals -- 1997



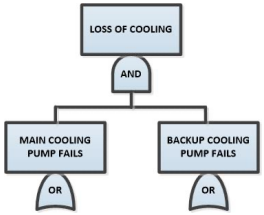
- the facility shall be available for three shift operations at least 284 days per year,
- the facility shall be available for at least 616 no-yield shots per year, and
- that the lasers perform within specification for 80% of all shots (a shot reliability goal of 80%)
- a plant availability goal of 90%



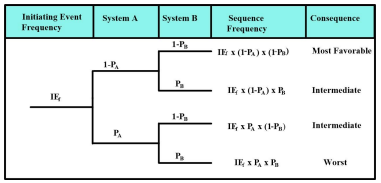
Laser Systems WBS 1.3



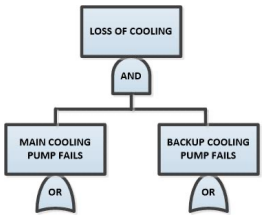
- optical pulse generation system, WBS 1.3.1
- amplifier system, WBS 1.3.2
- pockels cell system, WBS 1.3.3
- amplifier power conditioning system, WBS 1.3.4
- laser auxiliary systems, WBS 1.3.5
- Reliability Goal .887 (.1122) for WBS 1.3
- Availability Goal Unplanned maintenance 68 hours (0.99)



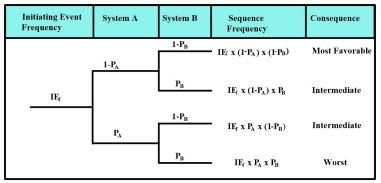
amplifier system, WBS 1.3.2

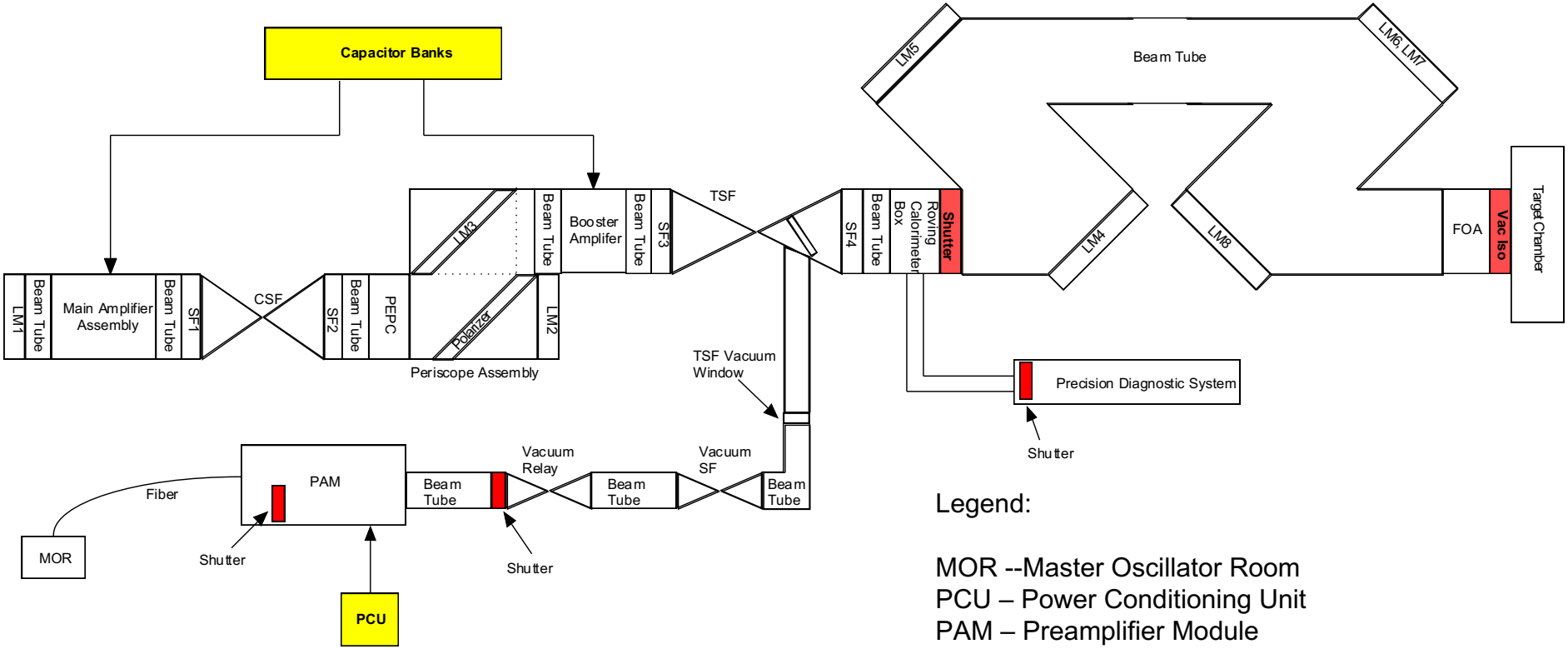


- Reliability Goal .9941 (0.0059) for WBS 1.3
- Availability Goal Unplanned maintenance 14 hours 0.9979 (0.0059)
- Assume flash lamp failures are statically independent



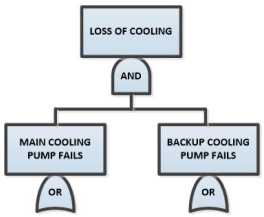
National Ignition Facility, LLNL



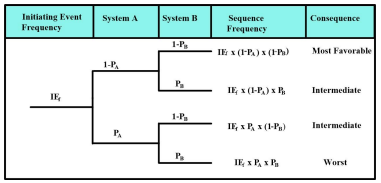


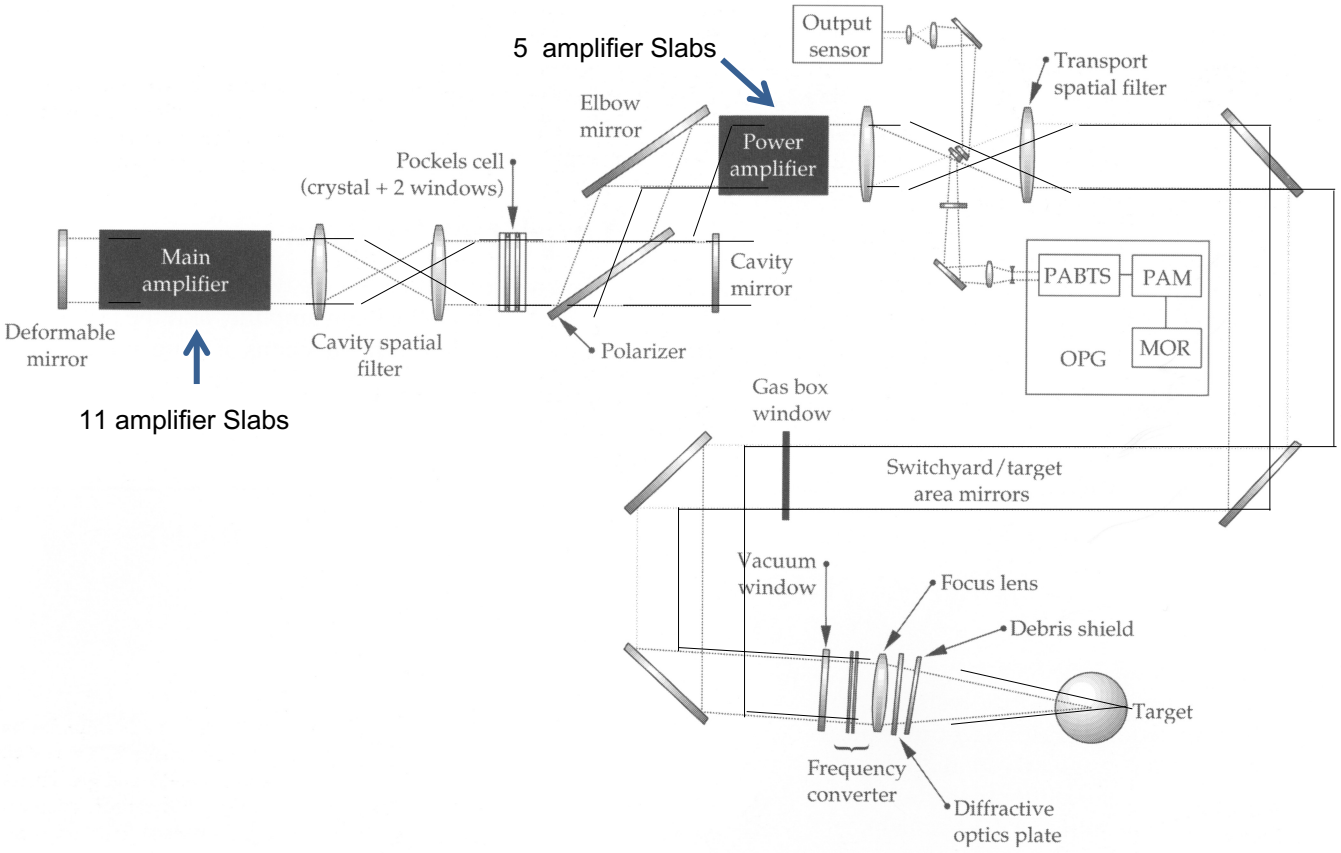
Legend:

MOR --Master Oscillator Room
PCU – Power Conditioning Unit
PAM – Preamplifier Module
SF – Spatial Filer
TSF – Transport Spatial Filter
FOA – Final Optics Assembly
LM – Laser Mirror
CSF – Cavity Spatial Filter
PEPC – Plasma Electrode Pockels Cell



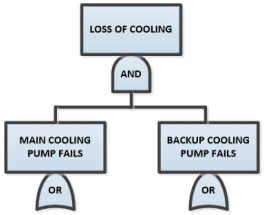
National Ignition Facility



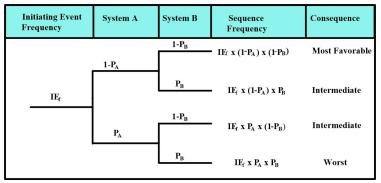


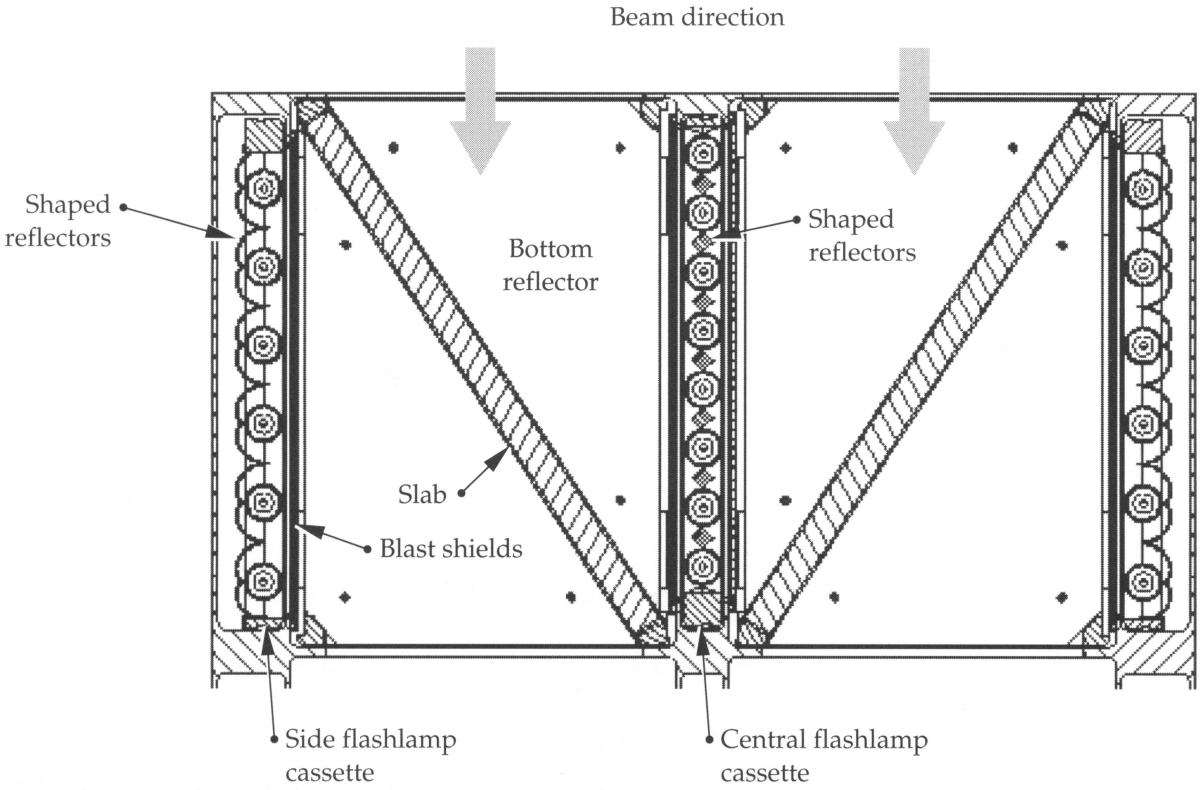
OPG Optical Pulse Generation

MOR Master oscillator room
PABTS Preamplifier Beam Transport System
PAM Preamplifier Module

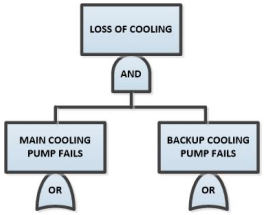


NIF FLASHLAMPS

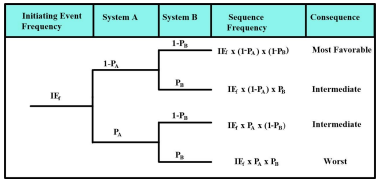


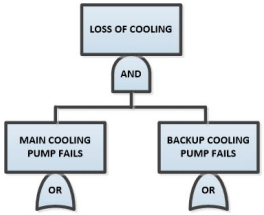


Each amplifier has a glass slab cassette, a side flashlamp cassette, and glass blast shields with antireflection coatings. A central flashlamp cassette runs between two beamlines.

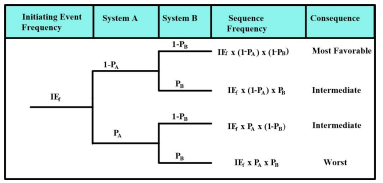


Frame Assembly Unit (FAU)

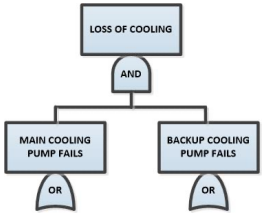




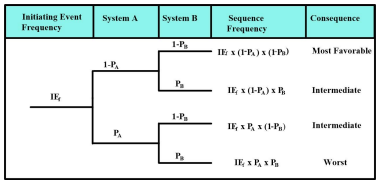
Flashlamp failure modes



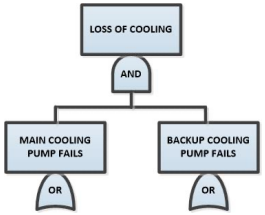
FAILURE MODE	FAILURE CAUSE	EFFECT
Fails to trigger	Glass Quartz Envelop Cracked , Electrode Broke, Nicked Or Blown Lead, Xenon Gas Contamination, Seal failure,	one flashlamp pair will not light œbeam balance criteria is still achieved
Sputters	nicked lead, electrode defective, Xenon Gas Contamination	Degraded failure mode
Base Short	Base Insulation resistance low	can cause several flash lamps to fail to trigger resulting in ruined shot
Explosion	Glass Quartz Envelop cracked, pulse power system fault too much energy	May affect NIF availability, requires cleanup and lamp replacement
Loss of flashlamp transmissivity	Burn spots, sputtering, degradation of the internal surface of the quartz	Degraded failure mode, reduces lamp output/efficiency



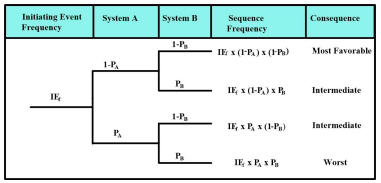
Flash lamp Fails to Trigger



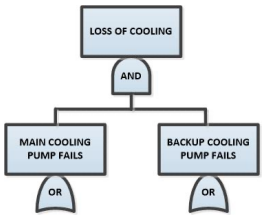
- Nova Data 233 failures out of 2.39 x 10^{7} shots
- Failure Probability =1.0 x 10^{-5} per shot
- NIF 8,640 flash lamps each pair connected in series
- NIF 4320 Flash lamp pairs
- Each pair has failure probability of 2.0 x 10^{-5} per shot
- Failure is achieved if two or more flash lamps fail to illuminate (violate NIF power balance criteria)
- Probability{k of n lamp pairs failing on the same shot}
  - = $n!/[(n-k)!k!]\ q^{k}\ p^{n-k}$
- Probability of two or more failures
- 1 - probability of zero failures - probability of exactly one failure
  - 1 - 0.917227 - 0.079250 = 0.00352
- 1- binom(4320,4320,1-2.0e-5) - binom(4319,4320,0.99998)



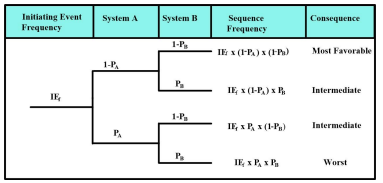
Upper bounds on the probability of failing to trigger



- Probability of two pair flash lamps failing to trigger
  - 2.0E-5
- Probability of any two pair failing to trigger
  - 2.0E-5*2.0E-5 = 4.0E-10
- Number of flash lamp pairs
  - Combination(4320,2) = 9,329,040 min cut sets of order 2
- Min Cut set upper bound
  - 1 – (1-4.0E-10)^9,329,040 ≤ 1
  - = 0.00372
- Rare Event Approximation
  - = 9,329,040*4.0E-10 = 0.00373
- Inequities
  - 0.00352 < 0.00372 < 0.00373
  - Exact < Min Cut Set Upper Bound (5.7%)< Rare Event Approximation(5.9%)



Flameout at a refinery gas furnace – 3 flame detectors 2 out of 3 logic



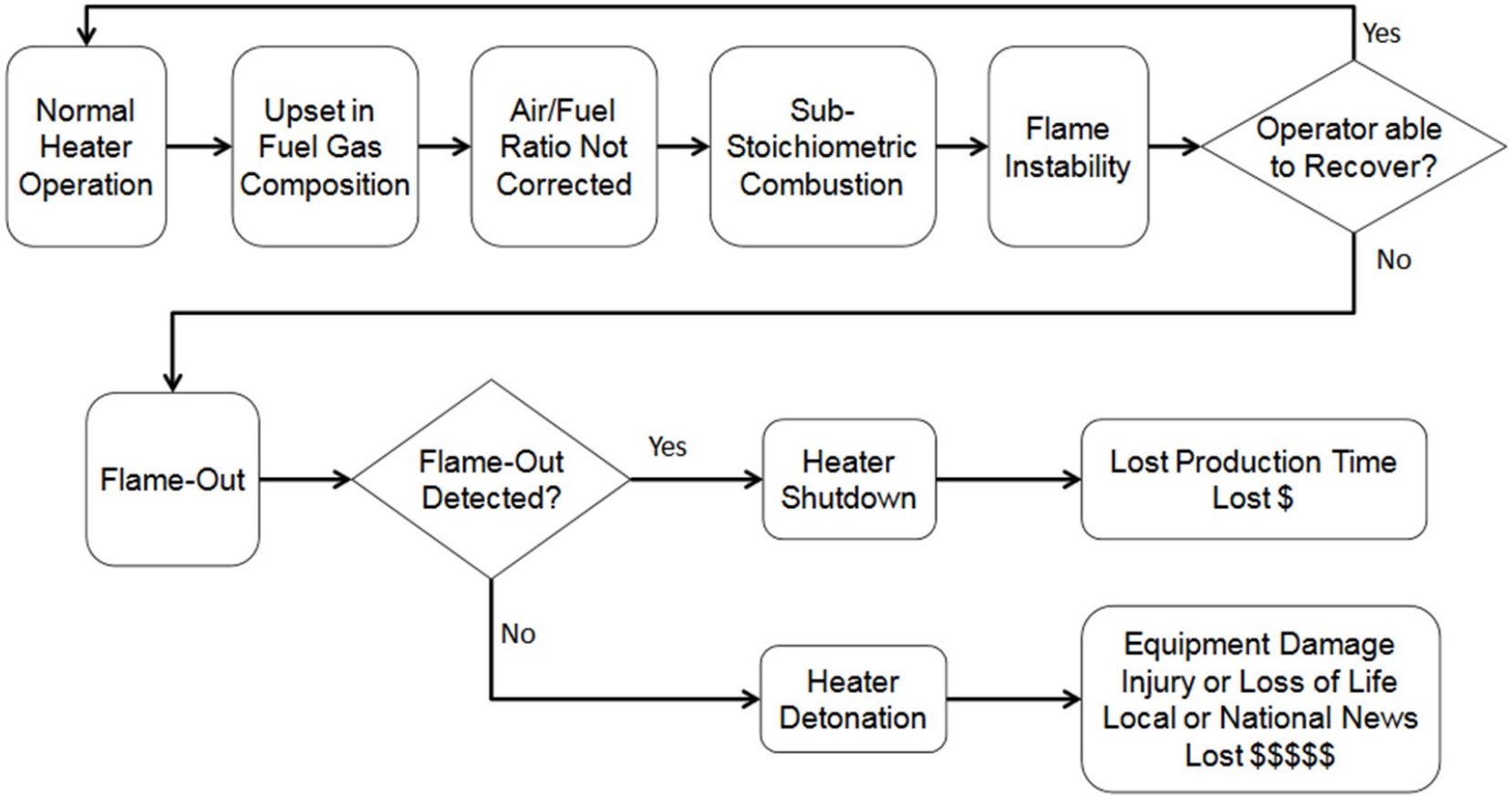
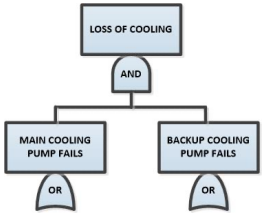
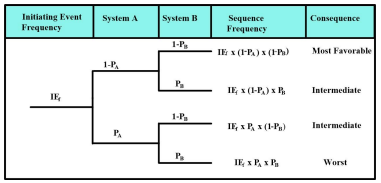


Figure 2 – Example Sequence of Events before and after a Flame out

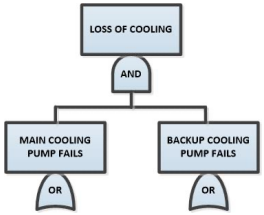


Fault tree top events

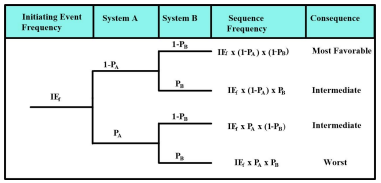


1. Heater Shutdown
2. Detonation

- Assumptions
  - The event “unrecoverable flameout” is an initiating event
  - Reliability of main gas valve is one.
  - Consider only two types of sensor failure
- Use 2-out-of 3 logic described previously



Notation

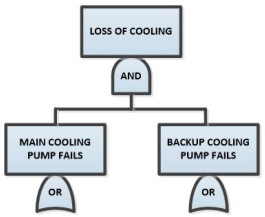


Inactive failure mode

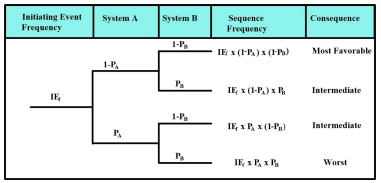
q_i = flame sensor fails to detect flameout

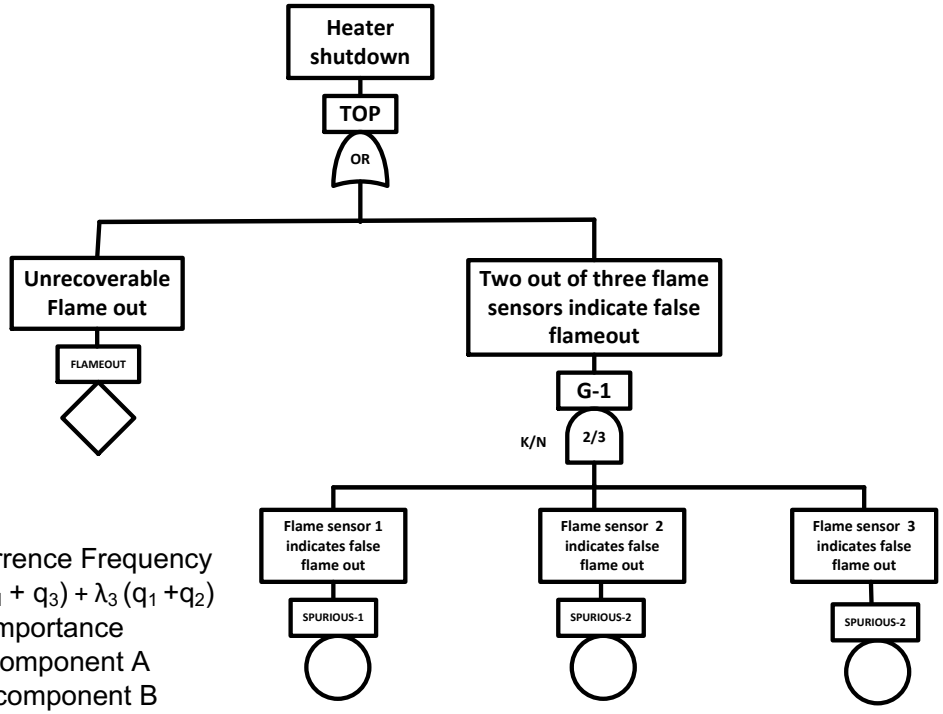
Spurious failure mode

q_s = flame detector detects spurious flameout (existence probability)
λ_s = rate at which flame detector detects spurious flameout
λ_f = initiating event frequency flameout



Heater Shutdown – Type 2 for fault event for flame sensor failures





- Top Event Occurrence Frequency

$W(t) = \lambda_1(q_2 + q_3) + \lambda_2(q_1 + q_3) + \lambda_3(q_1 + q_2)$

- Initiating Event Importance

$I_1(t) = \lambda_1(q_2 + q_3)/W_T(t)$ component A

$I_2(t) = \lambda_2(q_1 + q_3)/W_T(t)$ component B

$I_3(t) = \lambda_3(q_1 + q_2)/W_T(t)$ component C

- Enabling Event Importance

$E_1(t) = q_1(\lambda_2 + \lambda_3)/W_T(t)$ component A

$E_2(t) = q_2(\lambda_1 + \lambda_3)/W_T(t)$ component B

$E_3(t) = q_3(\lambda_1 + \lambda_2)/W_T(t)$ component C

- Min Cut Set Importance

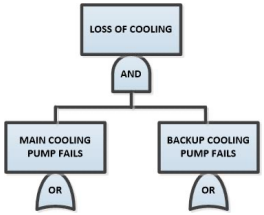
$MCS_1 = (\lambda_1 q_2 + \lambda_2 q_1)/W_T(t)$ $\{A_F B_F\}$

$MCS_2 = (\lambda_1 q_3 + \lambda_3 q_1)/W_T(t)$ {1,3} $\{A_F C_F\}$

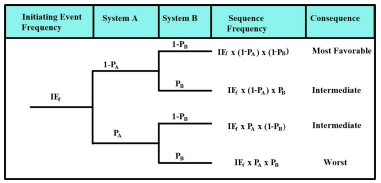
$MCS_3 = (\lambda_2 q_3 + \lambda_3 q_2)/W_T(t)$ $\{B_F C_F\}$

Min Cut Sets

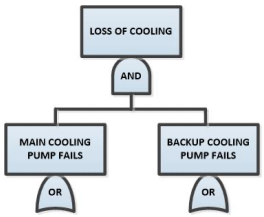
1. {FLAMEOUT}
2. {SPURIOUS-1, SUPRIOUS-2}
3. {SPURIOUS-1, SUPRIOUS-3}
4. {SPURIOUS-2, SUPRIOUS-3}



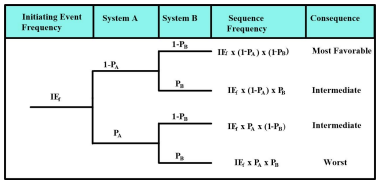
Importance Measures – Heater Shutdown

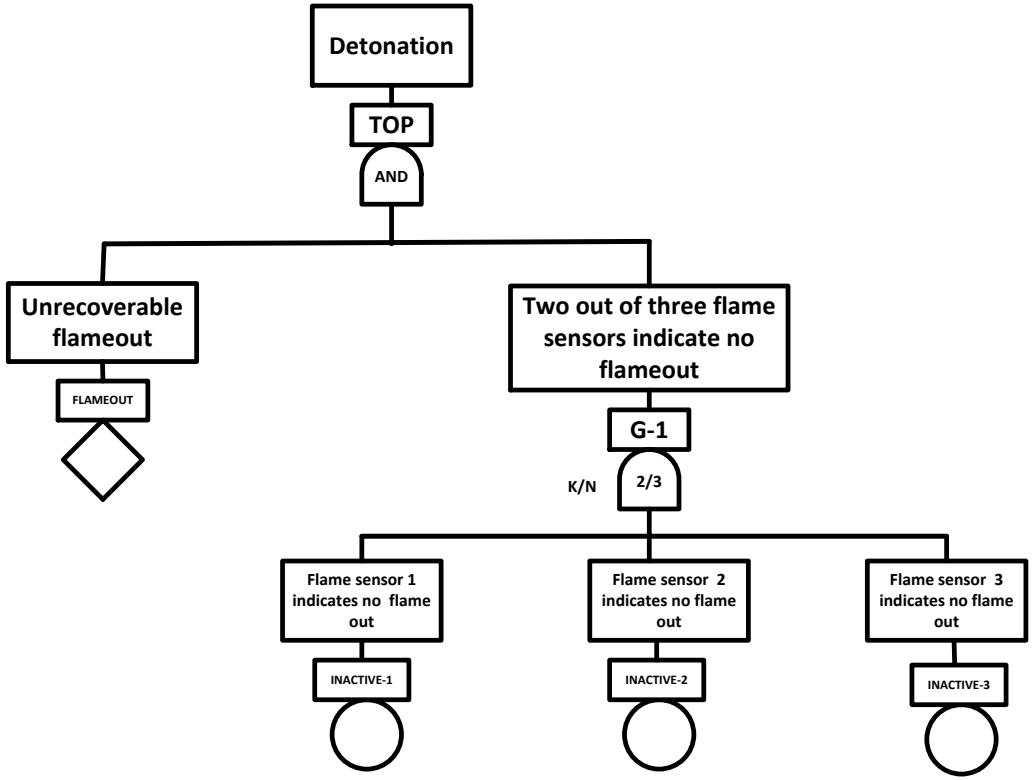


- Top Event Occurrence Frequency
  - $W(t) = \lambda_F + \lambda_{1,S}(q_{2,S} + q_{3,S}) + \lambda_{2,S}(q_{1,S} + q_{3,S}) + \lambda_{3,S}(q_{1,S} + q_{2,S})$
- Initiating Event Importance
  - $I_1(t) = \lambda_{1,S}(q_{2,S} + q_{3,S})/W_T(t)$ Flame sensor A
  - $I_2(t) = \lambda_{2,S}\,(q_{1,S} + q_{3,S})/W_T(t)$ Flame sensor B
  - $I_3(t) = \lambda_{3,S}\,(q_{1,S} + q_{2,S})/W_T(t)$ Flame sensor C
  - $I_4(t) = \lambda_F/W_T(t)$ Initiating event flameout
- Enabling Event Importance
  - $E_1(t) = q_{1,S}(\lambda_{2,S} + \lambda_{3,S})\,/W_T(t)$ Flame sensor A
  - $E_2(t) = q_{2,S}(\lambda_{1,S} + \lambda_{3,S})\,/W_T(t)$ flame sensor B
  - $E_3(t) = q_{3,S}(\lambda_{1,S} + \lambda_{2,S})\,/W_T(t)$ flame sensor C
- Min Cut Set Importance
  - $MCS_1 = \lambda_F/W_T(t)$
  - $MCS_2 = (\lambda_{1,S}q_{2,S} + \lambda_{2,S}\,q_{1,S})\,/W_T(t)\;\; \{A_{F,S}\;B_{F,S}\}$
  - $MCS_3 = (\lambda_{1,S}q_{3,S} + \lambda_{3,S}q_{1,S})/W_T(t)\;\{A_{F,S}\;C_{F,S}\}$
  - $MCS_4 = (\lambda_{2,S}q_{3,S} + \lambda_{3,S}q_{2,S})/W_T(t)\;\{B_{F,S}\;C_{F,S}\}$



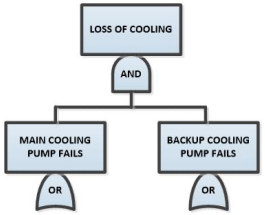
Detonation – Type 1 fault event for fault event for flame sensor failures



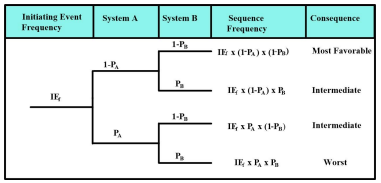


Min Cut Sets

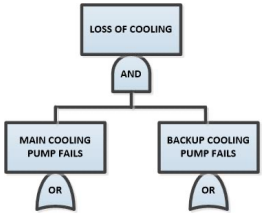
1. {FLAMEOUT, INACTIVE-1,INACTIVE-2}
2. {FLAMEOUT, INACTIVE-1,INACTIVE-3}
3. {FLAMEOUT, INACTIVE-2,INACTIVE-3}



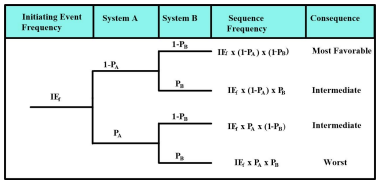
Importance Measures for top event "Detonation"



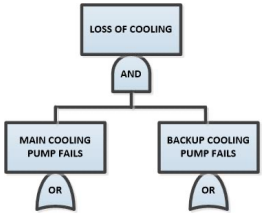
- Top Event Occurrence Frequency
  - $W(t) = \lambda_F(q_{1,I}q_{2,I} + q_{1,I}q_{3,I} + q_{2,I}q_{1,3})$
- Initiating Event Importance
  - = 1 for flameout
- Enabling Importance
  - $\lambda_F(q_{1,I}q_{2,I} + q_{1,I}q_{3,I})/W(t)$ Flame sensor 1
  - $\lambda_F(q_{1,I}q_{2,I} + q_{2,I}q_{3,I})/W(t)$ Flame sensor 2
  - $\lambda_F(q_{1,I}q_{3,I} + q_{2,I}q_{3,I})/W(t)$ Flame sensor 3
- Min Cut Set Importance
  - $MCS_1 = \lambda_F q_{1,I}q_{2,I}/W_T(t)$
  - $MCS_2 = \lambda_F q_{1,I}q_{3,I}/W_T(t)$
  - $MCS_1 = \lambda_F q_{2,I}q_{3,I}/W_T(t)$



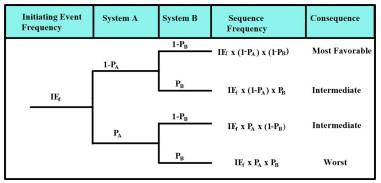
Initiating and Enabling Events



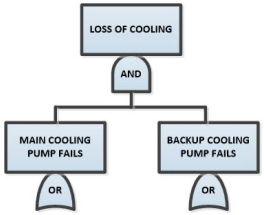
- The identification of initiating and enabling events is based upon a reliability engineering analysis
- For recoverable flameouts (a different initiating event), there are two events: “Recoverable flameout” (initiating event) AND “the operator fails to recover,” is an enabling event
- The role of initiating and enabling events can change for type 1 versus type 2 events
- Initiating and Enabling event importance for basic events and min cut sets is computed by the computer code IMPORTANCE



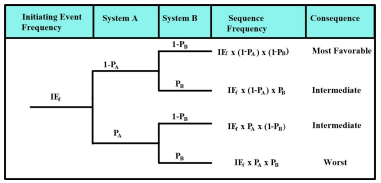
Initiating and Enabling Events Continued



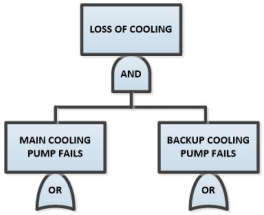
- For this presentation, importance measures are ratios and are conditional probabilities
- Sum of initiating event importance measures always equals unity
- Sum of enabling event importance usually exceeds unity because of double counting min cut sets
- Sum of min cut set importance equals unity if rare event approximation is valid otherwise may exceed unity
- Min Cut sets (AND gates) can have multiple basic events that can function as initiating events
- Other example is a 2-out-of-3 configuration for Undervoltage relays



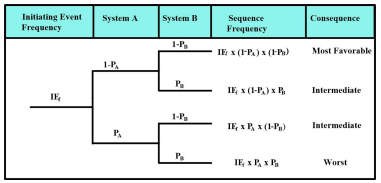
Initiating and Enabling Events Continued



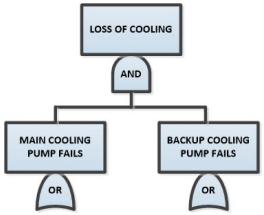
- Identification on initiating and enabling events is important for the FTA of control systems
- For example, for a negative feedback loop (NFBL) to cause or pass a disturbance two types of initiating events are considered
  - Failure of components on NFBL cause the upset condition
    - e.g., sensor, controller or actuator
  - External disturbances e.g., loss of cooling water, electricity, purge system, instrument air etc.
- Digraph analysis is useful in FTA of control systems – advantages, the digraph displays topology of system failures and identifies control loops
- Failure of protective systems is generally considered as enabling events for type 1 failure events.
- However, failure of protective systems can be initiators for type 2 fault events.



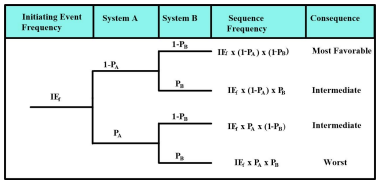
Special Initiators in FTA

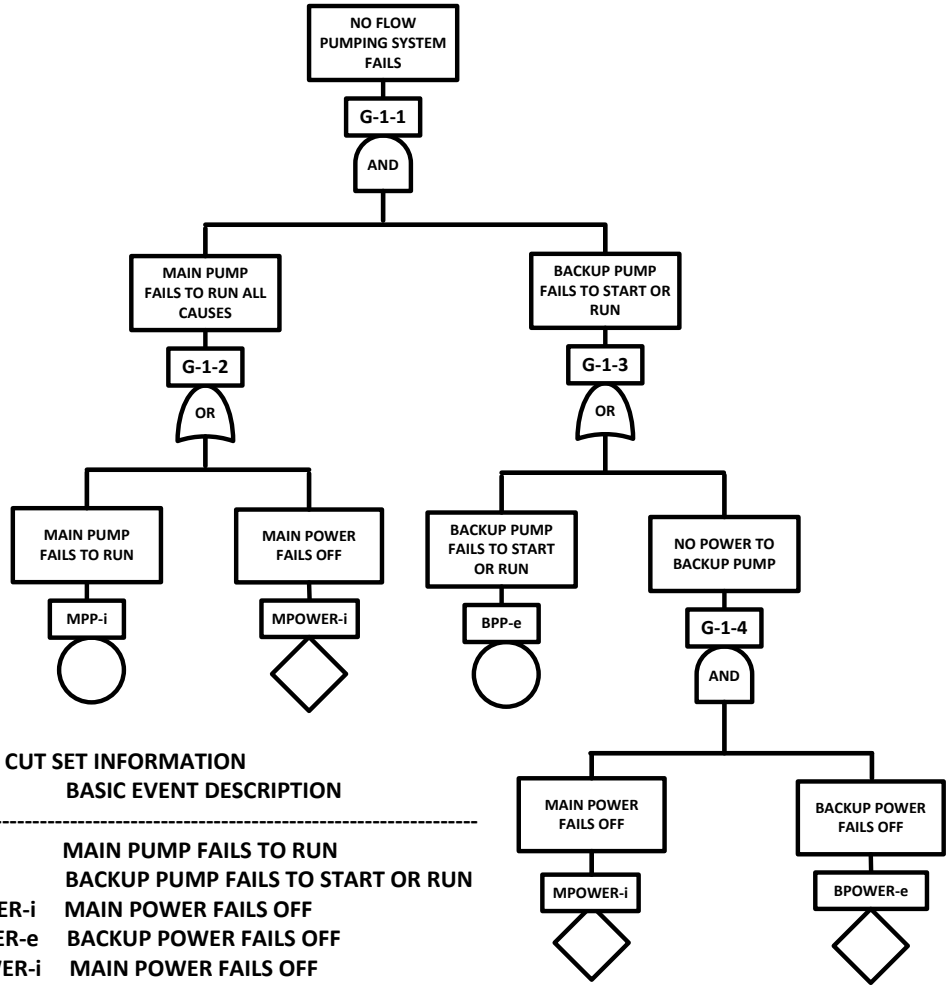


- Failure of systems may involve support systems such as electric power, instrument air and cooling water. As an example, consider a pumping system with a main pump and backup pump (next slide). The main pump is powered solely by the main power system and the backup pump is powered by both the main power supply and backup power supply. The fault tree for no flow is shown. Each basic event is labeled with an ID and corresponding basic event description. Initiating events are indicated by the basic event identifier –i, enabling events with identifier –e. There are three min cut sets of order 2. The failure of the main pump and electric power is a cut set of order 3 but is not a min cut set. Failure of the main power supply is a special initiator since it fails the main pump and fails part of the power supply to the backup pump. Even though gate event G-1-2 is an enabling condition, gate G-1-3 is within the domain of this gate and contains an initiating event. It is important to develop fault trees in enough detail to describe this functional dependency involving initiating events otherwise systems may be thought to be independent when in fact they are not. This means that the interaction between the initiating event logic and mitigating event logic needs to be considered. This is also true for control systems that simultaneously use control elements for both control and shutdown.



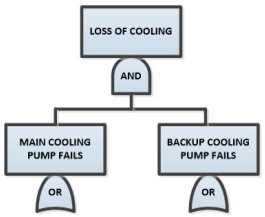
Pumping System Special Initiator



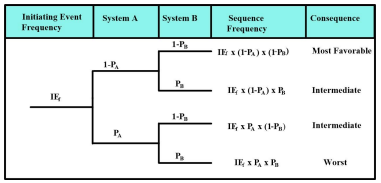


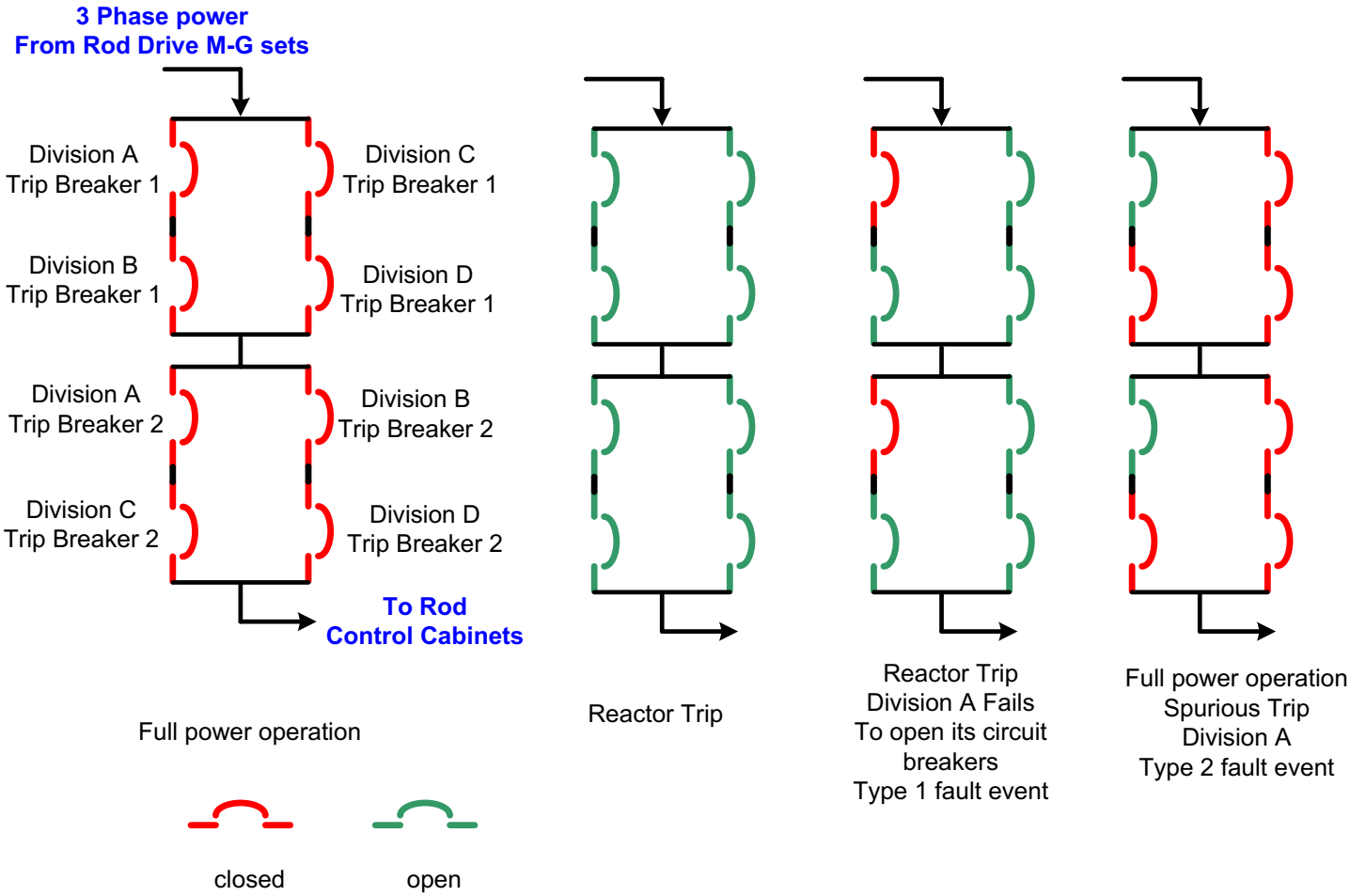
MIN CUT SET INFORMATION

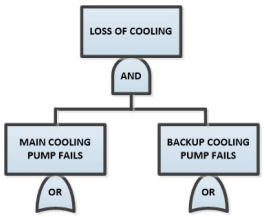
ORDER	ID	BASIC EVENT DESCRIPTION
2	MPP-i	MAIN PUMP FAILS TO RUN
	BPP-e	BACKUP PUMP FAILS TO START OR RUN
2	MPOWER-i	MAIN POWER FAILS OFF
	BPOWER-e	BACKUP POWER FAILS OFF
2	MPOWER-i	MAIN POWER FAILS OFF
	BPP-e	BACKUP PUMP FAILS TO START OR RUN



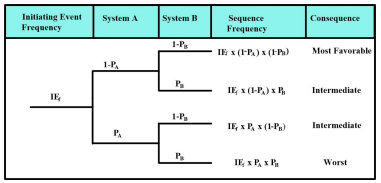
2-out-of-4 system reactor trip 2 types of failure – single train failure

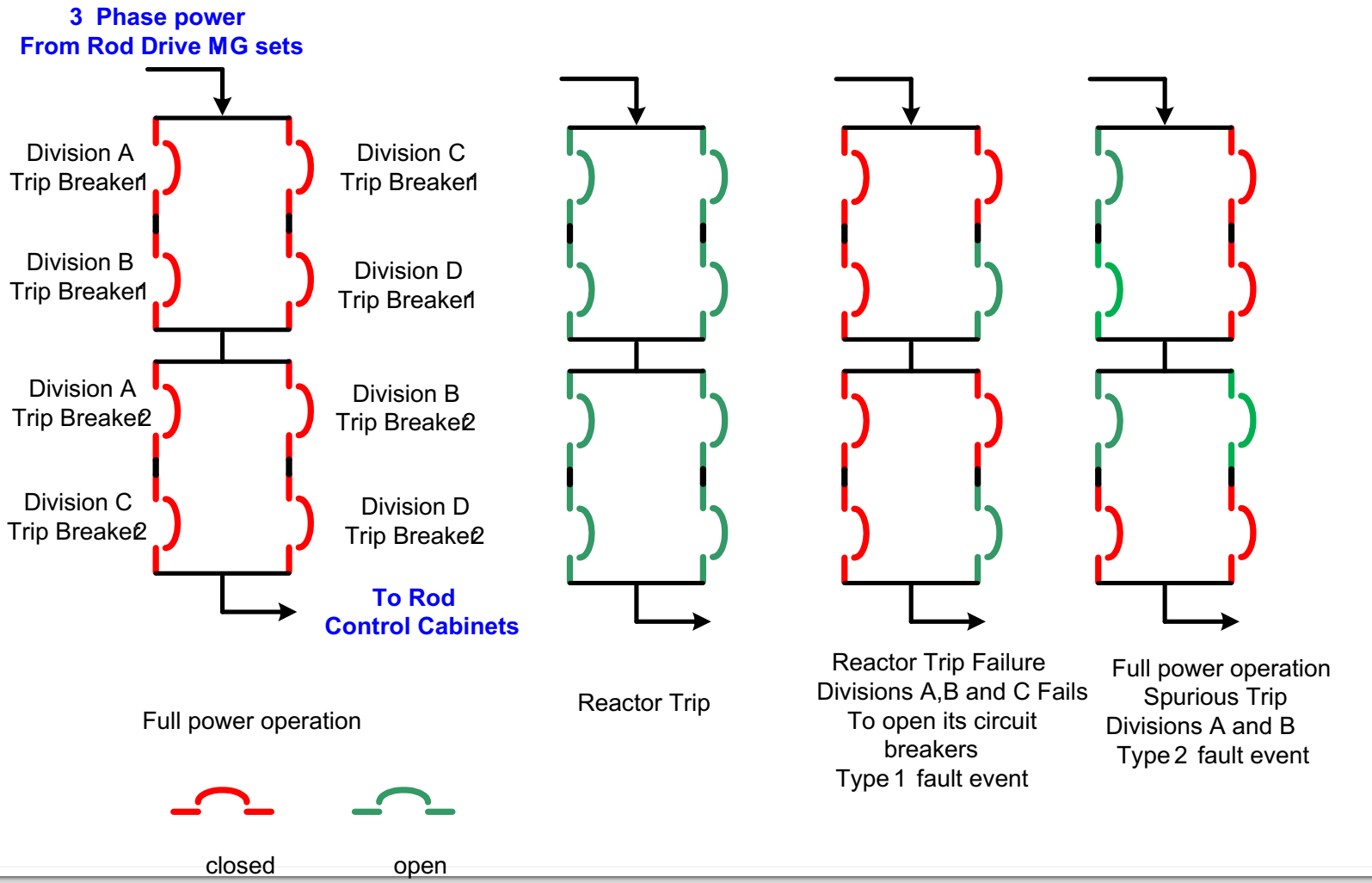


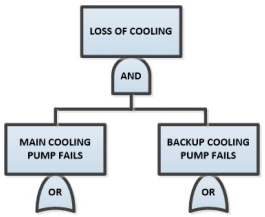




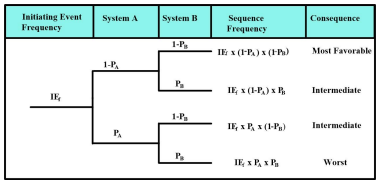
2-out-of-4 system reactor trip
2 types of failure – multiple train failures







High and Low Pressure Injection System



Piping to primary coolant system

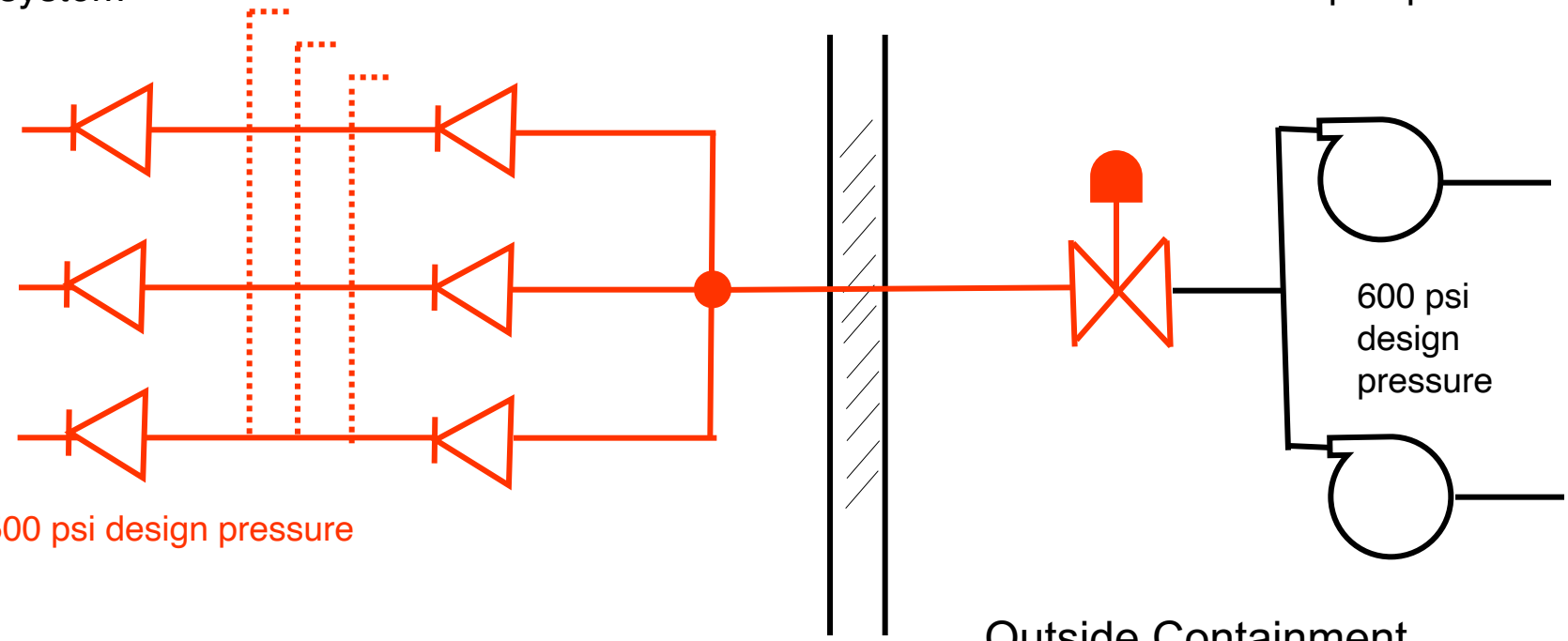
High Pressure Injection lines

Check Valves

Containment Building

Manual Valve Locked Open

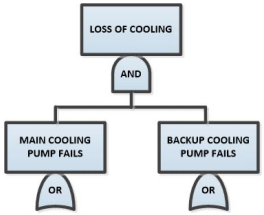
Low Pressure Injection pumps



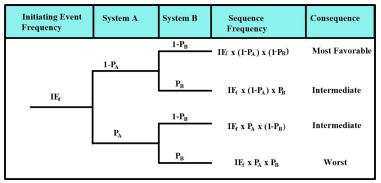
2500 psi design pressure

Inside Containment

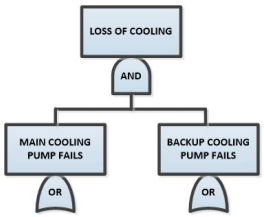
Outside Containment
Inside safeguards building



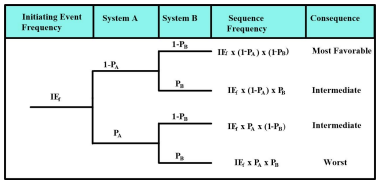
Safety Injection Signal

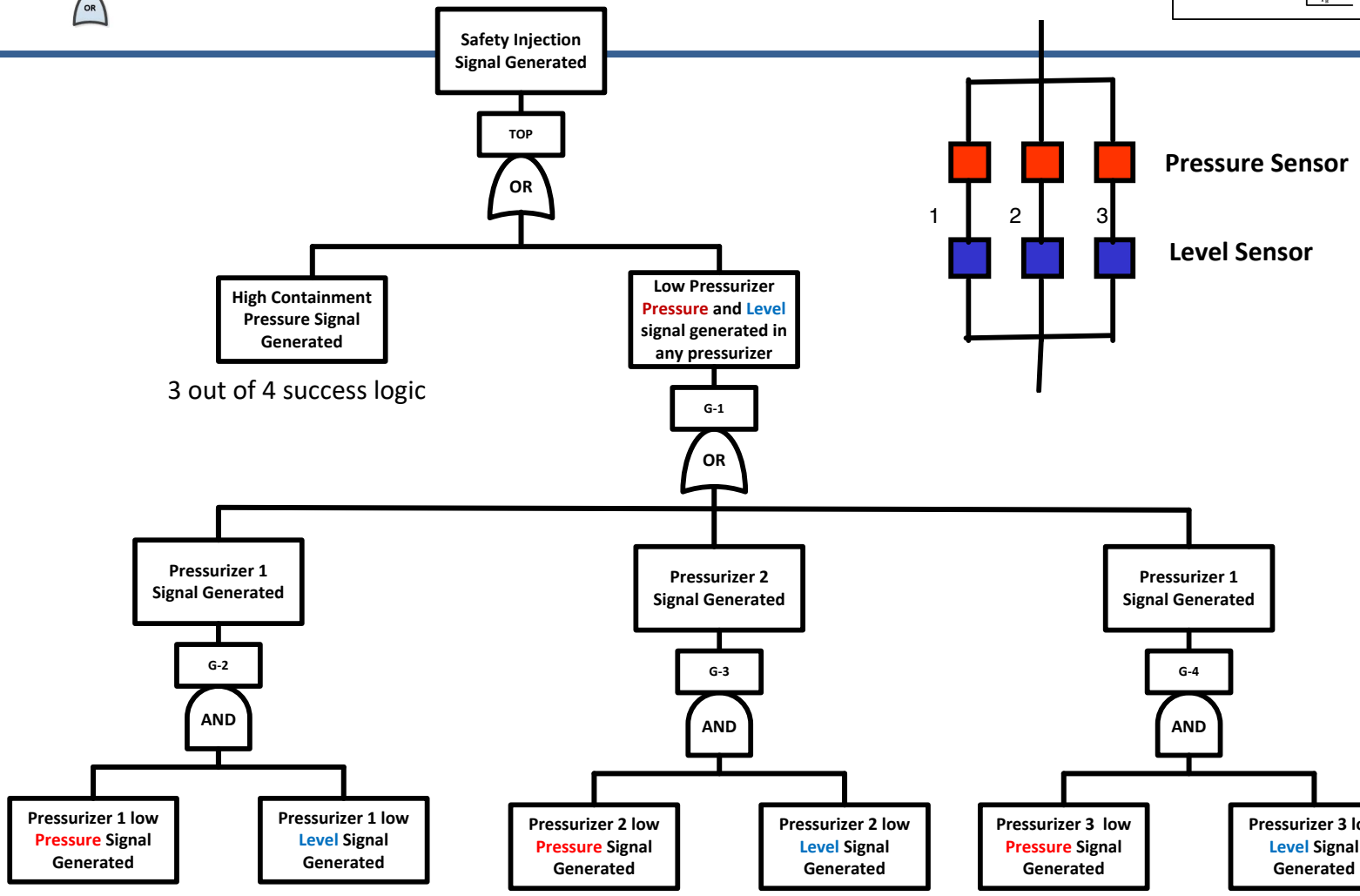


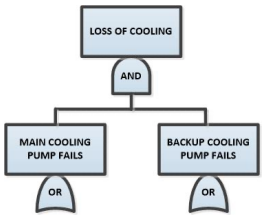
- Low Pressurizer Pressure (3 Sensors)
  - False Low Pressure
  - False High Pressure (include stuck mode)
- Low Pressurizer Level (3 Sensors)
  - False Low Pressure
  - False High Pressure (include stuck mode)
- High Containment Pressure (4 Sensors)
  - False Low Pressure (include stuck mode)
  - False High Pressure



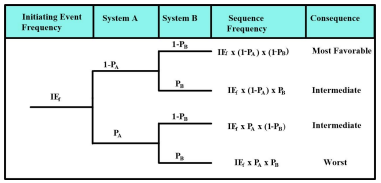
SIS GENERATION SUCCESS LOGIC



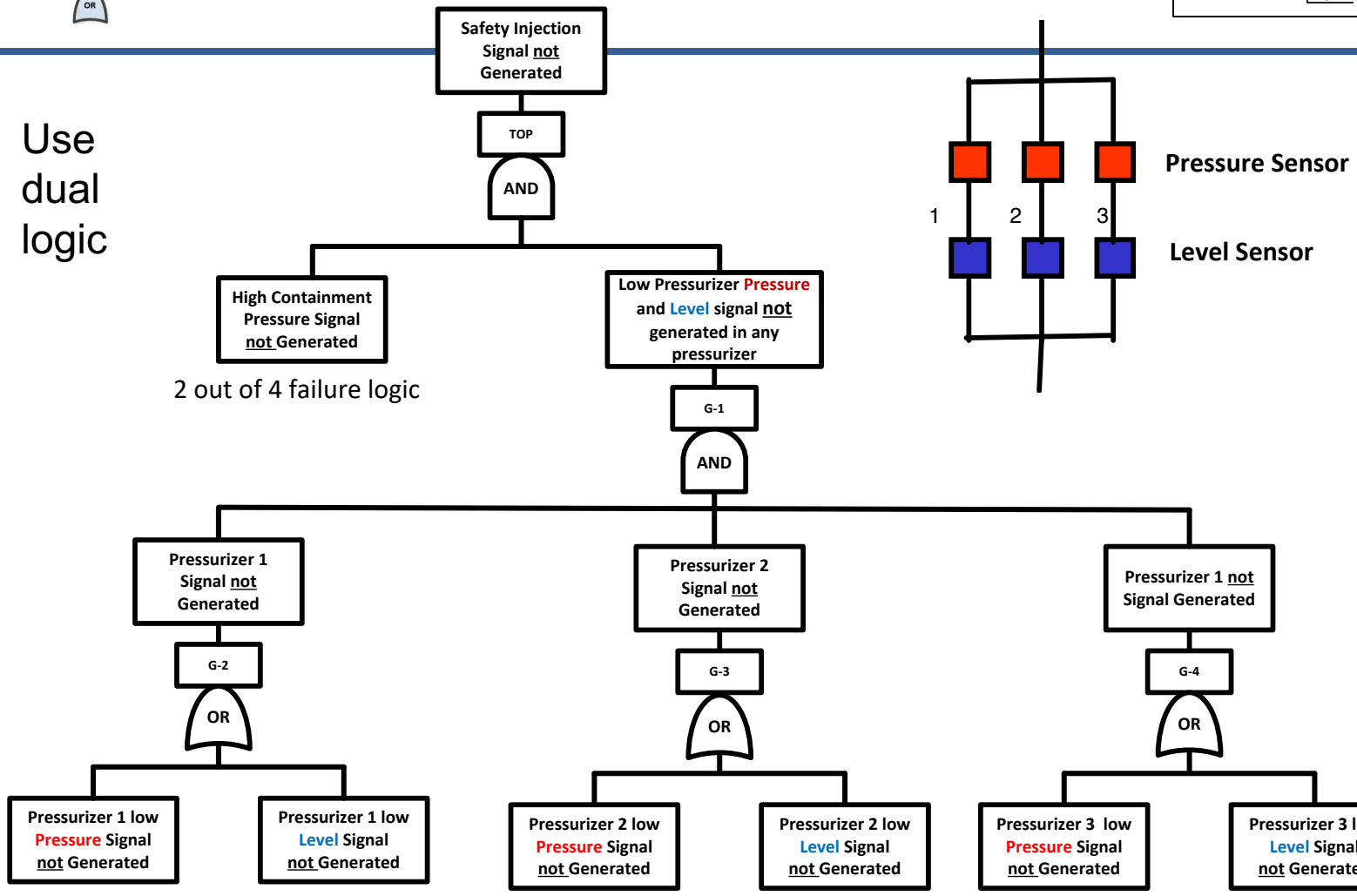




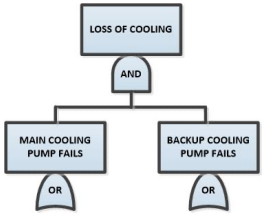
SIS GENERATION FAILURE LOGIC



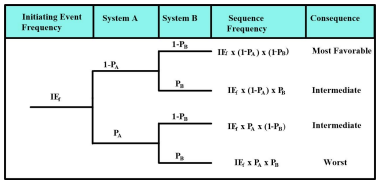
Use dual logic



2 out of 4 failure logic

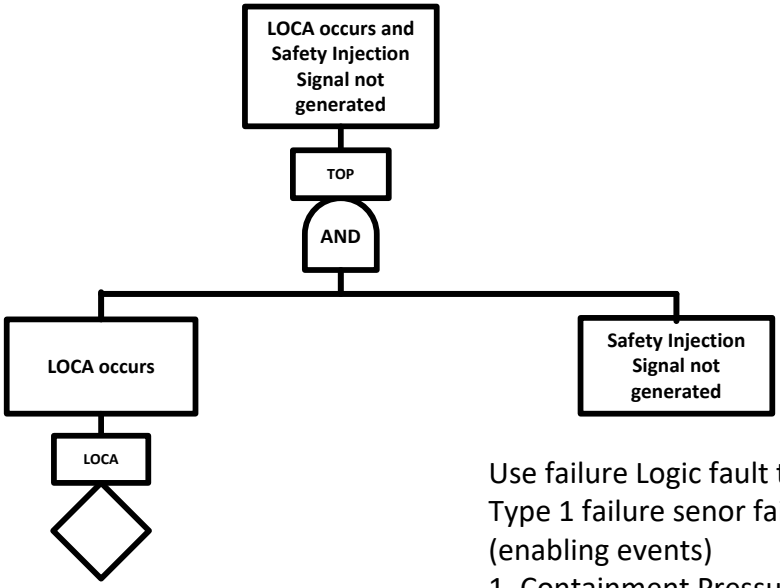


Fault Tree Top Events

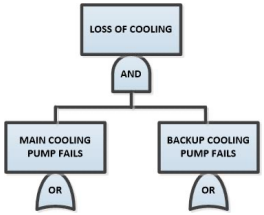


Inadvertent Safety Injection

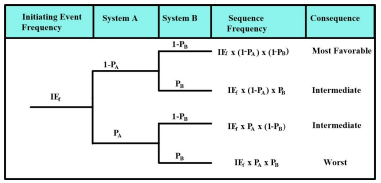
Use success Logic fault tree
Type 2 failure senor failure modes (initiating/enabling events)
1. Containment Pressure Sensor generates false high signal (CPS-H)
2. Pressurizer level sensor generates false low pressure (PLS-L)
3. Pressurizer pressure sensor generates false low pressure (PPS-L)



Use failure Logic fault tree
Type 1 failure senor failure modes (enabling events)
1. Containment Pressure Sensor generates false low signal (CPS-L)
2. Pressurizer level sensor generates false high pressure (PLS-H)
3. Pressurizer pressure sensor generates false high pressure (PP-H)



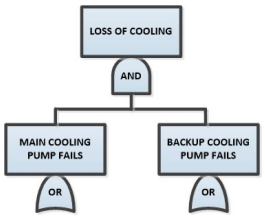
Min Cut Sets Inadvertent Safety Injection



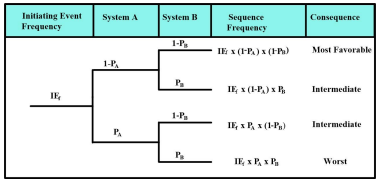
INADVERTENT SAFETY INJECTION
REFERENCE TABLE FOR MIN CUT SETS (TOTAL 7)

ORDER	1	2	3
NO. OF MIN CUT SETS	0	3	4

MIN CUT SET NO	ORDER	8-DIGIT NAME	FULL BASIC EVENT DESCRIPTION
1		PLS2-L	PRESSURIZER LEVEL SENSOR 2 FAILS LOW
		PPS2-L	PRESSURIZER PRESSURE SENSOR 2 FAILS LOW
2		PLS3-L	PRESSURIZER LEVEL SENSOR 3 FAILS LOW
		PPS3-L	PRESSURIZER PRESSURE SENSOR 3 FAILS LOW
3		PLS1-L	PRESSURIZER LEVEL SENSOR 1 FAILS LOW
		PPS1-L	PRESSURIZER PRESSURE SENSOR 1 FAILS LOW
4		CPS1-H	CONTAINMENT PRESSURE SENSOR 1 FAILS HIGH
		CPS2-H	CONTAINMENT PRESSURE SENSOR 2 FAILS HIGH
		CPS3-H	CONTAINMENT PRESSURE SENSOR 3 FAILS HIGH
5		CPS1-H	CONTAINMENT PRESSURE SENSOR 1 FAILS HIGH
		CPS2-H	CONTAINMENT PRESSURE SENSOR 2 FAILS HIGH
		CPS4-H	CONTAINMENT PRESSURE SENSOR 4 FAILS HIGH
6		CPS1-H	CONTAINMENT PRESSURE SENSOR 1 FAILS HIGH
		CPS3-H	CONTAINMENT PRESSURE SENSOR 3 FAILS HIGH
		CPS4-H	CONTAINMENT PRESSURE SENSOR 4 FAILS HIGH
7		CPS2-H	CONTAINMENT PRESSURE SENSOR 2 FAILS HIGH
		CPS3-H	CONTAINMENT PRESSURE SENSOR 3 FAILS HIGH
		CPS4-H	CONTAINMENT PRESSURE SENSOR 4 FAILS HIGH



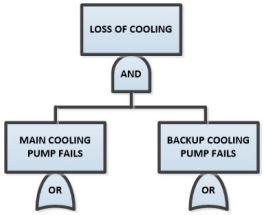
Min Cut Sets for LOCA and Safety Injection Signal Not Generated



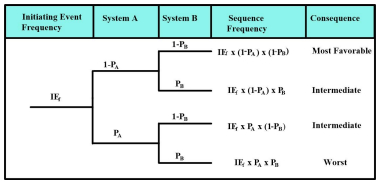
REFERENCE TABLE FOR MIN CUT SETS (TOTAL 48)

ORDER	1	2	3	4	5	6
NO. OF MIN CUT SETS	0	0	0	0	0	48

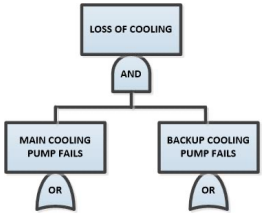
MIN CUT SET NO	ORDER	8-DIGIT NAME	FULL BASIC EVENT DESCRIPTION
1	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS1-H	PRESSURIZER LEVEL SENSOR 1 FAILS HIGH
		PLS2-H	PRESSURIZER LEVEL SENSOR 2 FAILS HIGH
		PPS3-H	PRESSURIZER PRESSURE SENSOR 3 FAILS HIGH
2	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS2-H	PRESSURIZER LEVEL SENSOR 2 FAILS HIGH
		PPS1-H	PRESSURIZER PRESSURE SENSOR 1 FAILS HIGH
		PPS3-H	PRESSURIZER PRESSURE SENSOR 3 FAILS HIGH
3	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS1-H	PRESSURIZER LEVEL SENSOR 1 FAILS HIGH
		PLS3-H	PRESSURIZER LEVEL SENSOR 3 FAILS HIGH
		PPS2-H	PRESSURIZER PRESSURE SENSOR 2 FAILS HIGH
4	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS3-H	PRESSURIZER LEVEL SENSOR 3 FAILS HIGH
		PPS1-H	PRESSURIZER PRESSURE SENSOR 1 FAILS HIGH
		PPS2-H	PRESSURIZER PRESSURE SENSOR 2 FAILS HIGH
5	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS1-H	PRESSURIZER LEVEL SENSOR 1 FAILS HIGH
		PPS2-H	PRESSURIZER PRESSURE SENSOR 2 FAILS HIGH
		PPS3-H	PRESSURIZER PRESSURE SENSOR 3 FAILS HIGH
6	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PPS1-H	PRESSURIZER PRESSURE SENSOR 1 FAILS HIGH
		PPS2-H	PRESSURIZER PRESSURE SENSOR 2 FAILS HIGH
		PPS3-H	PRESSURIZER PRESSURE SENSOR 3 FAILS HIGH
7	6	CPS2-L	CONTAINMENT PRESSURE SENSOR 2 FAILS LOW
		CPS3-L	CONTAINMENT PRESSURE SENSOR 3 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS1-H	PRESSURIZER LEVEL SENSOR 1 FAILS HIGH
		PLS2-H	PRESSURIZER LEVEL SENSOR 2 FAILS HIGH
		PLS3-H	PRESSURIZER LEVEL SENSOR 3 FAILS HIGH
8	6	CPS1-L	CONTAINMENT PRESSURE SENSOR 1 FAILS LOW
		CPS4-L	CONTAINMENT PRESSURE SENSOR 4 FAILS LOW
		LOCA	LOSS OF COOLANT ACCIDENT -- INITIATING EVENT
		PLS2-H	PRESSURIZER LEVEL SENSOR 2 FAILS HIGH
		PLS3-H	PRESSURIZER LEVEL SENSOR 3 FAILS HIGH
		PPS1-H	PRESSURIZER PRESSURE SENSOR 1 FAILS HIGH



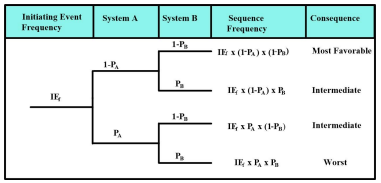
Insights regarding initiating, enabling events and critical system states



- Min cut sets can contain more than one initiating event
- Number of initiating events in a min cut set define the number of sequences – examples
  - Fire or explosion scenarios
  - K-out-of-N systems
  - Type 2 fault events
    - Inadvertent safety injection
    - Inadvertent reactor trip
- Critical system states define the set of enabling events conditional on the occurrence of the initiating event
- Two types of enabling events
  - Predecessor events (e.g., demand failures)
    - Failure of safety devices
    - Preexisting conditions involving fire or explosion
  - Successor Events
    - Failure to recover in time
    - Time delays before phenomena can occur



Basic Event Naming Convention



SY-CC-XXX-FM

SY is the system ID:

SI – Safety Injection
CS – Containment Spray
EP – Electric Power
SW – Service Water
AF – Auxiliary Feedwater
AC – Safety Injection Accumulators
CF – Containment Fan Coolers
CW – Cooling Water
CI – Containment Isolation
IA – Instrument Air

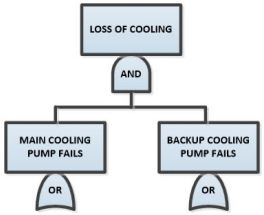
CC is the component type:

AV – Air Operated Valve
CV – Check Valve
FN – Fan
MP – Motor-driven Pump
PO - PORV
RY – Safety Valve
TK – Tank
AC – Air Compressor
TR - Train
CB - Circuit Breaker
DG – Emergency Diesel Generator
HX – Heat Exchanger
MV – Motor Operated Valve
RV – Relief Valve
TP – Turbine-driven Pump
XV – Manual Valve
HV – Hydraulic Valve

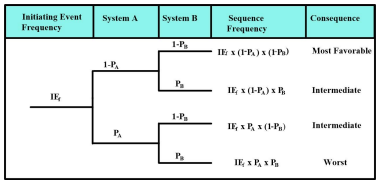
XXX is the component number (e.g., 01A, 13B, etc.)

FM is the failure mode being modeled for the component:

S – Fails to start
O – Fails to open
T – Spuriously transfers
L – Leaks
H – Human action
F – Loss of Function
R – Fails to run
C – Fails to close
P – Plugs
M – Maintenance or Test
U – Undeveloped
CC – Common Cause

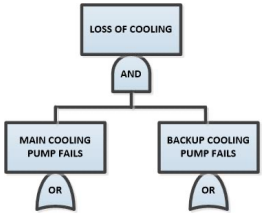


Generic Component/Failure Mode Data

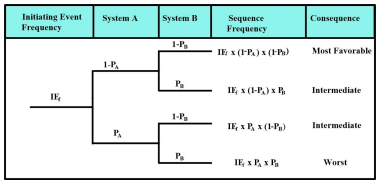


Component Type	Component Failure Mode	Type	Code	Failure Rate	Error Factor
Air-Operated Valve (AOV)	Air-Operated Valve Fails to Control	H	AVC	3.00E-06	18.8
	Air-Operated Valve Spuriously Operates	H	AVT	2.00E-07	18.8
Bus	AC Power Bus Fails to Operate	H	BSF	1.00E-08	5
Circuit Breaker	Circuit Breaker Fails to Close	D	CBC	2.50E-03	5.8
	Circuit Breaker Fails to Open	D	CBO	2.50E-03	5.8
	Circuit Breaker Spuriously Operates	H	CBT	1.50E-07	2.8
Check Valve	Check Valve Fails to Close	D	CVC	1.00E-04	8.4
	Check Valve Fails to Open	D	CVO	1.20E-05	8.4
Emergency Diesel Generator (EDG)	Emergency Diesel Generator in Test or Maintenance	D	DG M	1.20E-02	2.1
	Emergency Diesel Generator Fails to Run	H	DGR	8.00E-04	2.8
	Emergency Diesel Generator Fails to Start & Load*	D	DGS	8.00E-03	4.3
Fan	Fan Fails to Run	H	FN R	1.20E-04	1.7
	Fan Fails to Start	D	FNS	5.00E-03	18.6
Heat Exchanger	Heat Exchanger in Test or Maintenance	D	HXM	7.00E-03	4.3
	Heat Exchanger Plug/Foul	H	HXP	6.00E-07	3.3
Motor-Driven Pump (MDP)	Motor-Driven Pump Test or Maintenance	D	MPM	8.00E-03	4.3
	Motor-Driven Pump Fails to Run	H	MPR	6.00E-06	8.4
	Motor-Driven Pump Fails to Start*	D	MPS	1.90E-03	4.7

Ref. Data Derived from NUREG/CR-6928 * Combined FTS w/FTR within 1st Hour

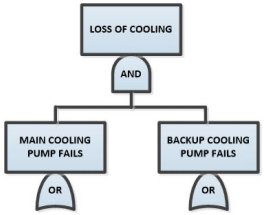


Generic Component /Failure Mode Data Cont'd

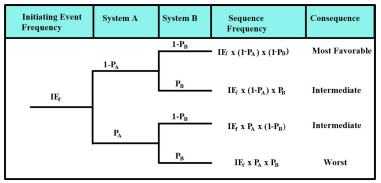


Component Type	Unavailability Mode	Demand / Hourly	Code	Mean Value	Error Factor
Emergency Diesel Generator	Emergency Diesel Generator Test or Maintenance	**d**	**M**	1.2E-02	**2.1**
Heat Exchanger	Heat Exchanger Test or Maintenance (CCW)	**d**	**M**	7.0E-03	**4.3**
	Heat Exchanger Test or Maintenance (RHR-PWR) "	**d**	**M**	5.0E-03	**2.5**
Motor-driven Pump	Motor-Driven Pump Test or Maintenance (AFWS)	**d**	**M**	4.0E-03	**2.5**
	Motor-Driven Pump Test or Maintenance (CCW)	**d**	**M**	6.0E-03	**3.8**
	Motor-Driven Pump Test or Maintenance (ESW)	**d**	**M**	1.2E-02	**4.3**
	Motor-Driven Pump Test or Maintenance (Other)	**d**	**M**	8.0E-03	**4.3**
Turbine-driven Pump	Turbine-Driven Pump Test or Maintenance (AFWS)	**d**	**M**	5.0E-03	**2.8**

Ref. Data Derived from NUREG/CR-6928 * Combined FTS w/FTR within 1st Hour

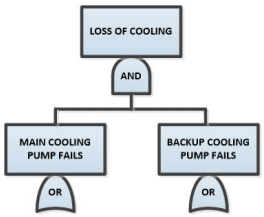


System Analysis: Component Boundaries

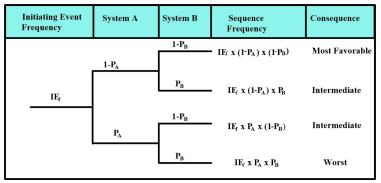


Example Boundary: Diesel Generators do not include:

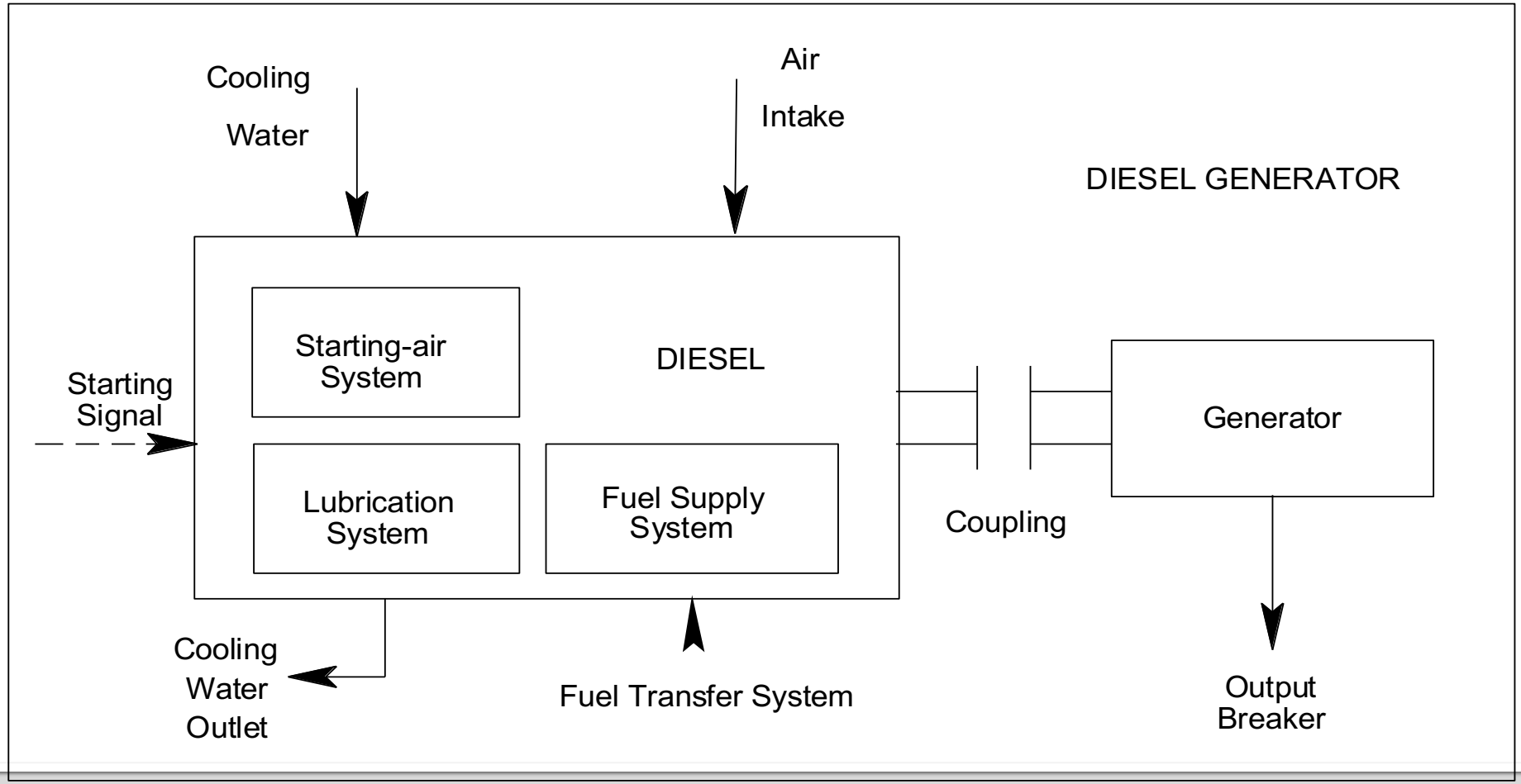
- Diesel generator load sequencers
- Diesel fuel oil transfer system
- Cooling water valves
- Diesel generator output breaker or bus
- Protection system, actuation relays
- Diesel room cooling

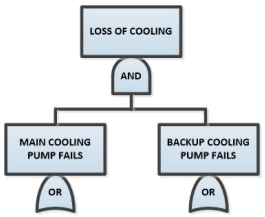


System Analysis: Component Boundaries

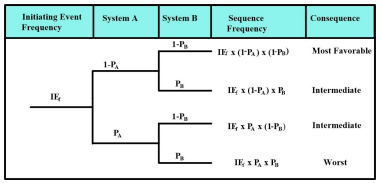


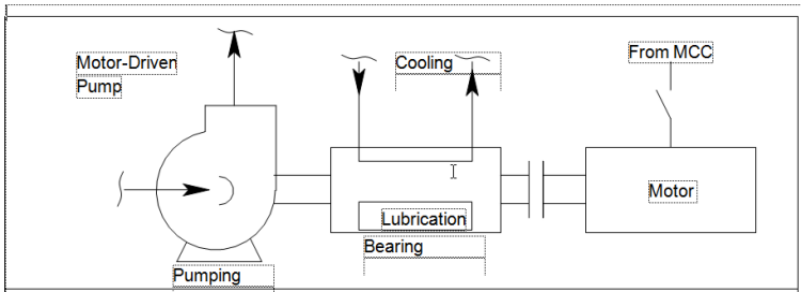
Component Boundary for a Diesel Generator

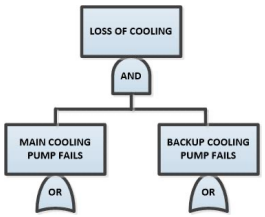




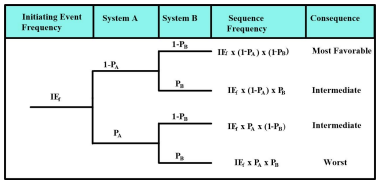
Example Fault Tree for a Motor Driven Pump

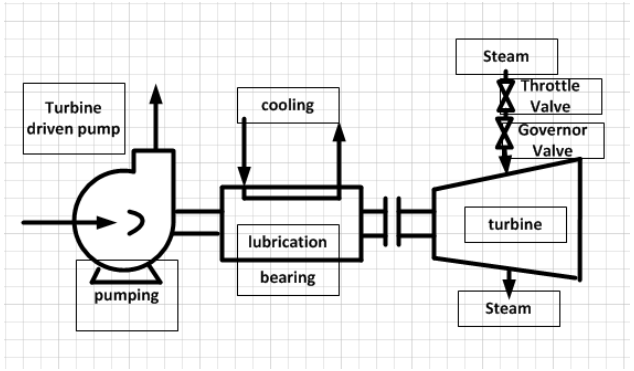


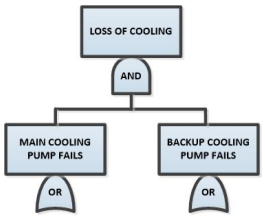




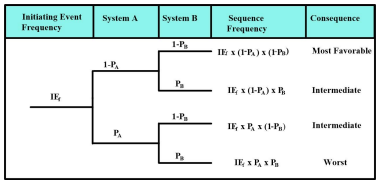
Example Fault Tree for a Turbine Driven Pump

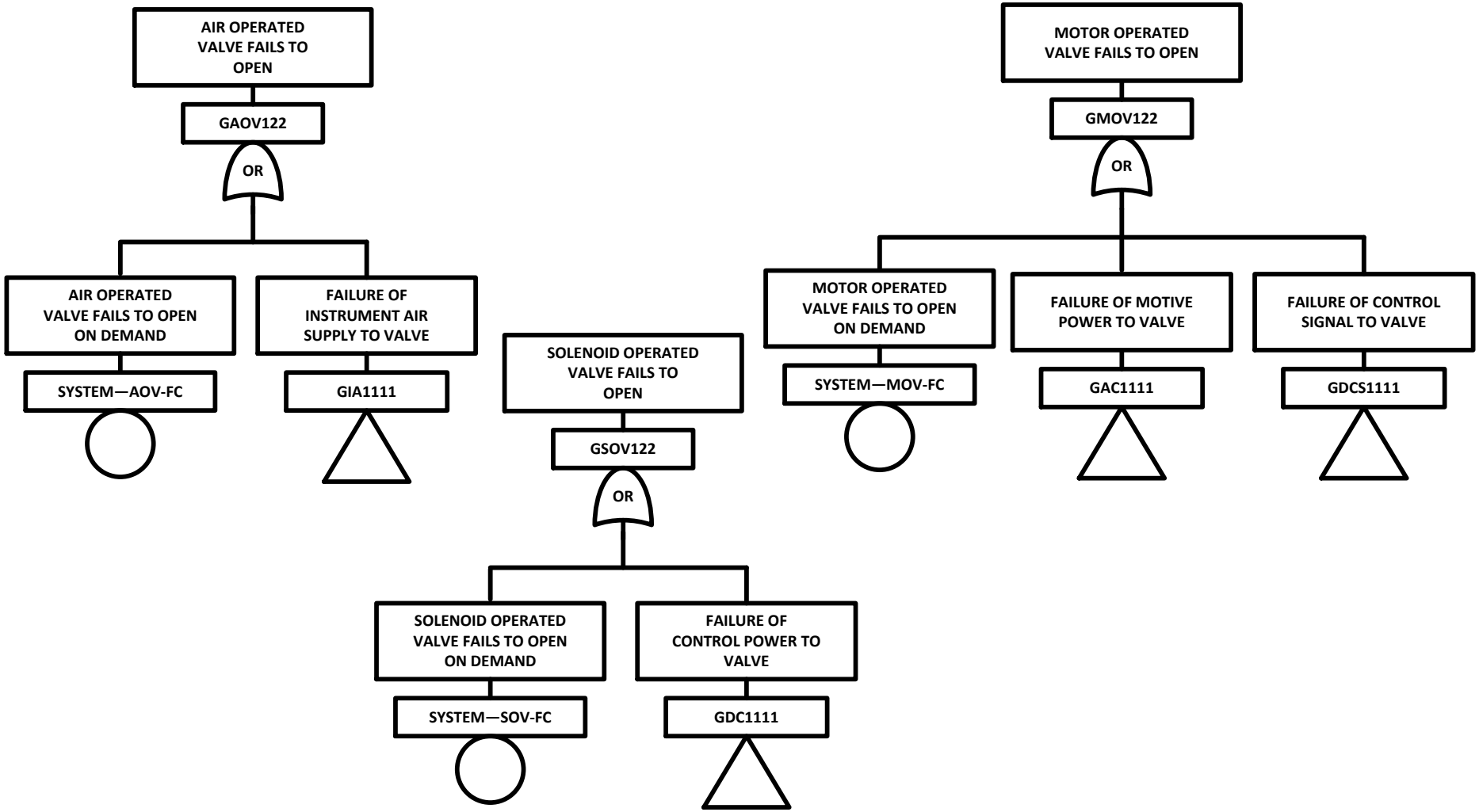


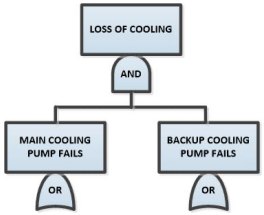




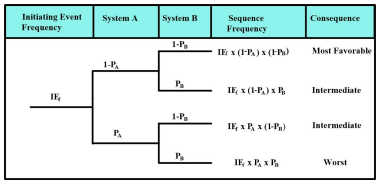
Fault Trees for pneumatic valve, solenoid operated valve and motor operated valve



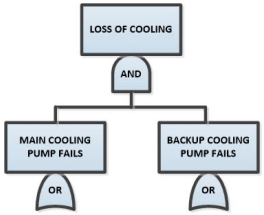




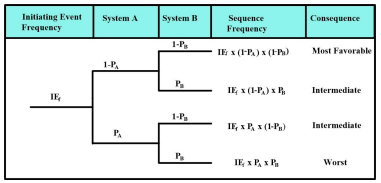
FTA -- Heuristic Guidelines Construction of Fault Trees



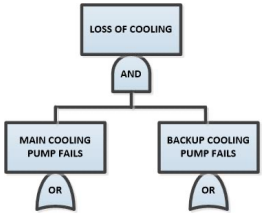
- Replace an abstract event by a less abstract event. Example: “Motor Operates Too Long” versus “Current to Motor Too Long.”
- Classify an event into more elementary events. Example: “Explosion of Tank” versus “Explosion by Overfilling” or “Explosion by Runaway Reaction.”
- Identify distinct causes for an event. Example: “Runaway Reaction” versus “excessive feed” and “Loss of Cooling.”



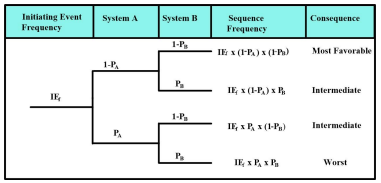
FTA -- Heuristic Guidelines Continued



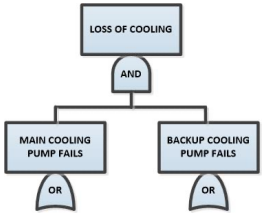
- Specify the **immediate** cause of the event under development
- Couple trigger events with “no protective action.” Example: “overheating” versus “loss of cooling” couple with “no system shutdown.”
- Find cooperative causes for an event. Example: “Fire” versus “leak of flammable fluid” and “relay sparks.”
- Pinpoint a component failure event. Example: “No cooling water” versus “main valve is closed” coupled with “bypass valve is not opened.”



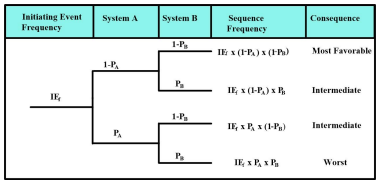
FTA -- Heuristic Guidelines for Fault Tree Construction



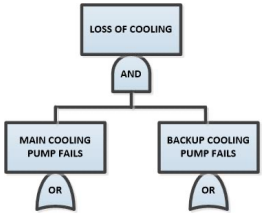
- Expect no miracles; if the “normal” functioning of a component helps to propagate a fault sequence, it must be assumed that the component functions “normally”
- Write complete, detailed fault statements
- Avoid direct gate-to-gate relationships
- Avoid the use of successes or complemented events in FTA
- For example, for inadvertent actuation (type 2 fault event) it is common to assume components work normally – the number of individual components that are assumed to work can be large
- Think locally (little steps)



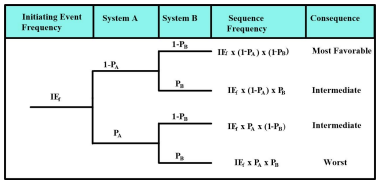
FTA -- Heuristic Guidelines (cont.)



- Always complete the inputs to a gate
- Include notes on the side of the fault tree to explain assumptions not explicit in the fault statements
- Repeat fault statements on both sides of the transfer symbols
- To make FTA of complex systems easier to follow, use zone indices for components on the system schematic and link component indices to gate events and basic events in the fault tree.
- Put OR, AND, K-out-of-N descriptions inside the logic gate (as was done in this presentation) so that the uniformed (e.g, management) can understand the fault tree logic

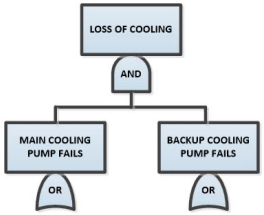


FTA -- Strengths of Fault Tree Analysis

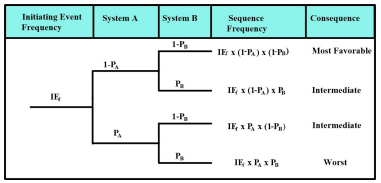


By organizing abnormal behavior in a logical and graphical manner, the engineering-manager is better able to evaluate risk and communicate managerial reasoning to peers, supervisors and subordinates. Decision making is consequently (hopefully) carried out more objectively and accurately. A powerful aid to selling ideas and results.

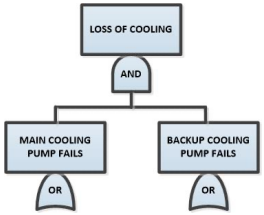
Process of constructing fault trees lead to insights regarding interactions difficult for a single failure analysis



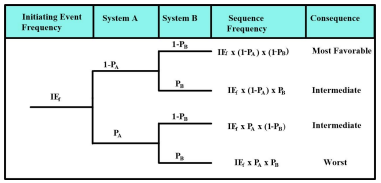
FTA -- Strengths of Fault Tree Analysis (cont.)



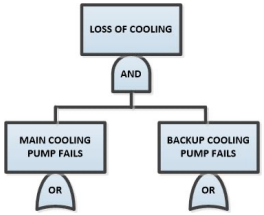
- Qualitative analysis often reveals the most important system features
- Applicable to a wide range of systems
- Human performance may be included
- Software defects can be addressed
- Design errors may be included
- Excellent safety and reliability analysis technique
- Can suggest other analysis if FTA is insufficient



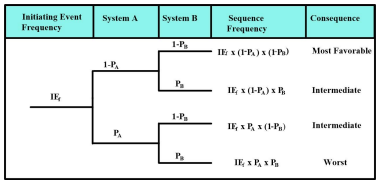
FTA --Limitations of Fault Tree Analysis



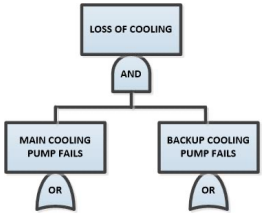
- Time consuming if large, detailed systems are analyzed
- Adequate time and resources must be given to conduct FTA including conducting a peer review
- Binary events (on or off) are assumed
- Completeness issue
- Probability data may be sparse or not applicable
- Difficult to follow if not documented and summarized properly
- The fault tree logic does not necessarily bare relationship on how the system works – for example development of type 2 fault events
- For top events that cause injury or harm, the fault tree logic does not necessarily address system restoration when the top event occurs – i.e., not a repair model.



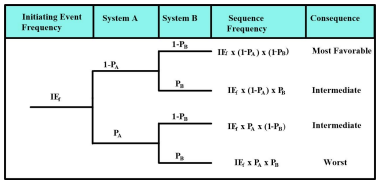
FTA --Limitations of Fault Tree Analysis continued



- If you teach FTA solely as an exercise in Boolean Algebra and generating structure functions, you are teaching math. The generation and analysis of fault trees require a multidisciplinary approach and depends upon the process analyzed – this applies to analysis of complex control systems.
- The identification of normal, type 1 and type 2 fault events and secondary failures in FTA is important and is generally not considered in a reliability analysis and depends upon the Top undesired event or scenario analyzed in the FTA.



FTA --Limitations of Fault Tree Analysis continued



- Use of basic event frequencies in probability expressions such as the min cut set upper bound generate incorrect results –for example multiplying a frequency times a frequency can occur. A basic event frequency is not a probability.
- The calculation must identify initiating events in the fault tree and then define the critical system state for each initiating event. The modeling assumes each initiating event is in series and if the critical system state occurs given the occurrence of the initiating event, the top event occurs. Using this method, initiating event frequencies are not multiplied together.
- A basic event can be both initiating and enabling. The enabling event appears in the critical system state for the initiating event.
- The min cut set upper bound can be used to compute the critical system unavailability since this is a conditional probability.
- If the analyst does not understand the significance of initiating and enabling events– the analyst does not understand FTA
- Arguments -- Lose Friends!