Fault Tree Analysis

Chapter 15

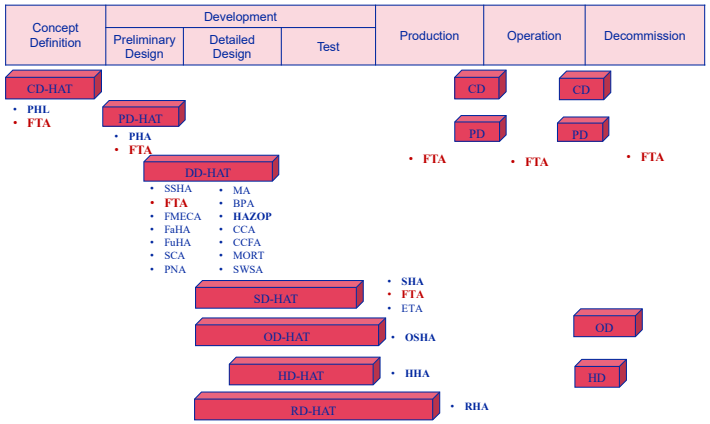
1

What is FTA?

- A method of calculating the expected frequency (or probability) of an unwanted event.
- Use for cases when several different kinds of causes exist.

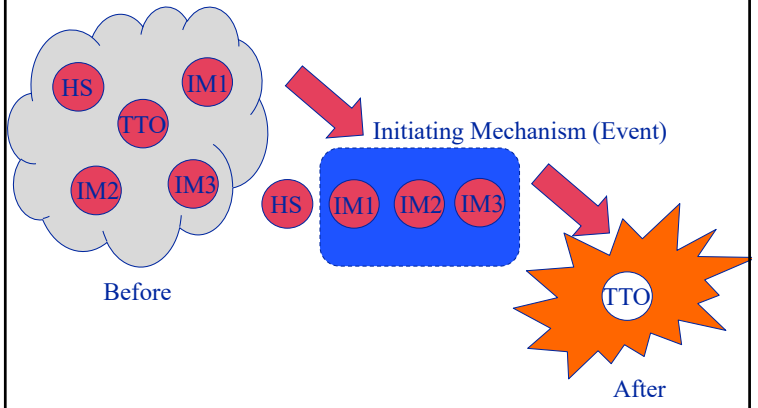
2

Life Cycle Phase



3

Fault Tree Analysis Root Causes



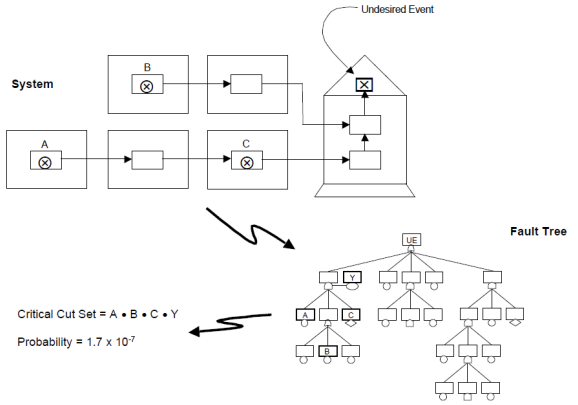
4

Application of FTA

- Calculating failure rate of a sub-assembly with multiple components
  - ⇨ Such as pressure sensor system, or shutdown valve assembly
- Calculating frequency of an unwanted event with a complex set of causes
  - ⇨ e.g. Air Traffic Control Failure
- Finding a single point of failure that could shut down a whole system.

5

FTA Summary



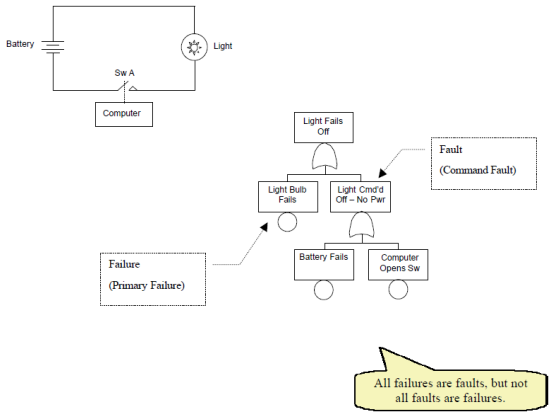
6

Definitions

- **Failure**
  - ⇨Occurrence of a basic component failure
  - ⇨*No further breakdown*
- **Fault**
  - ⇨Occurrence of an undesired state for a component, subsystem or system
  - ⇨Can be *further broken down*

7

Failure and Fault Example



8

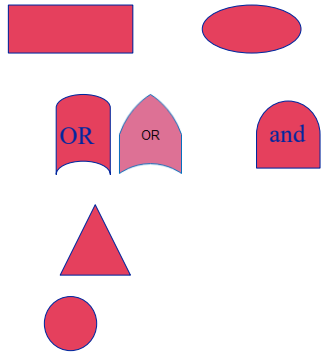
Methodology

9

FTA Building Blocks

Node Types:

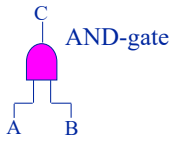
- Gate Event
- Conditional Events
- Transfer Events
- Basic Events



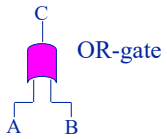
10

Logical Connection Between Events

- AND: The resulting output event requires the ***simultaneous occurrence*** of all input event.
  e.g. Event C will occur only if both events A and B occur simultaneously, which is represented (for independent events, A, B) by
  A • B = C

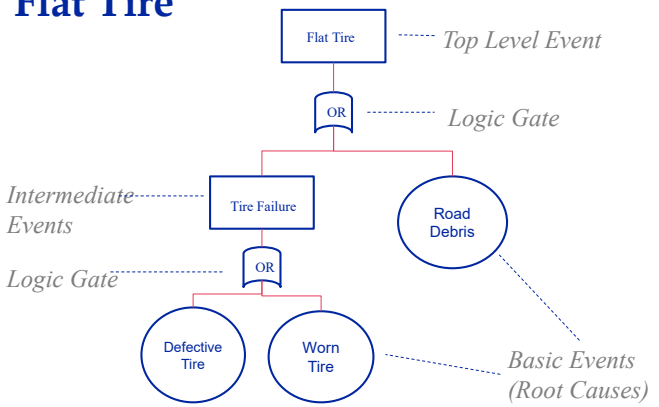


- OR: The resulting output event requires the occurrence of ***any individual*** input event
  e.g. C will occur if either A or B occurs, which is represented (when A, B each has low probability of occurring) by
  A + B = C



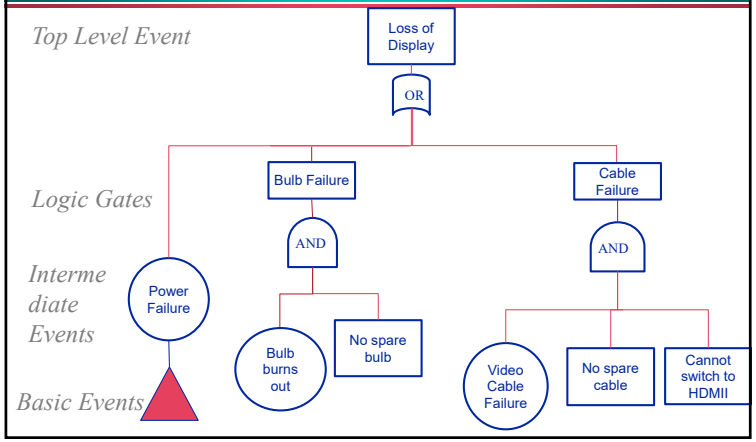
11

Flat Tire

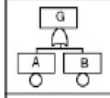
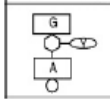


12

Example: Loss of display of presentation



13

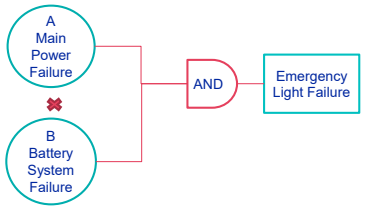
Symbol	Gate Type	Description
	AND Gate	The output occurs only if all of the inputs occur together. $P = P_A \cdot P_B = P_A P_B$ (2 input gate) $P = P_A \cdot P_B \cdot P_C = P_A P_B P_C$ (3 input gate)
	OR Gate	The output occurs only if at least one of the inputs occurs. $P = P_A + P_B - P_A P_B$ (2 input gate) $P = (P_A + P_B + P_C) - (P_{AB} + P_{AC} + P_{BC}) + (P_{ABC})$ (3 input gate)
	Priority AND Gate	The output occurs only if all of the inputs occur together, and A must occur before B. The priority statement is contained in the Condition symbol. $P = (P_A P_B) / N!$ Given $\lambda_A \approx \lambda_B$ and N = number of inputs to gate
	Exclusive OR Gate	The output occurs if either of the inputs occurs, but not both. The exclusivity statement is contained in the condition symbol. $P = P_A + P_B - 2(P_A P_B)$
	Inhibit Gate	The output occurs only if the input event occurs and the attached condition is satisfied. $P = P_A \cdot P_Y = P_A P_Y$

Ch 15 page 246 Figure 15.5

14

Calculation: AND gates

- Multiply the frequency or the probability values
- Ensure input events are independent
  - ⇨ if not, treat as common cause
- No more than one frequency value among the inputs
  - ⇨ Others must be probabilities



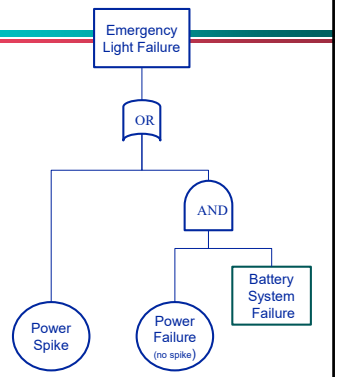
$$P_{AB} = PA \; x \; PB$$

15

What if power failure can cause battery system failure?

Split Power Failure causes into two:

- *Causes leading to battery system failure*
- *Causes that don't affect battery system*



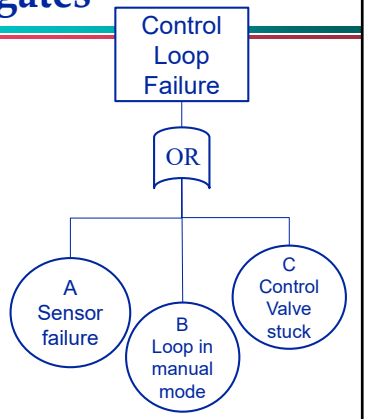
Common Cause Failure Events

Multiple (usually identical) components fail due to shared causes

16

Calculation: OR gates

- Add the frequency or probability values
  - ⇨Events must be mutually exclusive
  - ⇨Cant mix frequency and probability
- If events are not mutually exclusive, probabilities are combined.

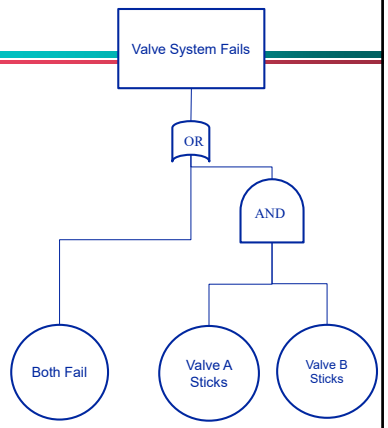


$$P_{ABC} = PA + PB + PC \_ (P_{AB} + PAC + P_{BC}) + PAB_C$$

17

Common Cause

- Common cause events should be added at the top level using an OR gate

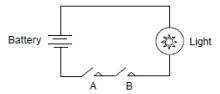


18

FTA Example 1

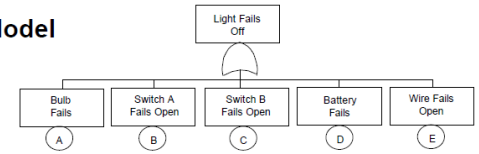
19

System



System Undesired Event: *Light Fails Off*

FT Model

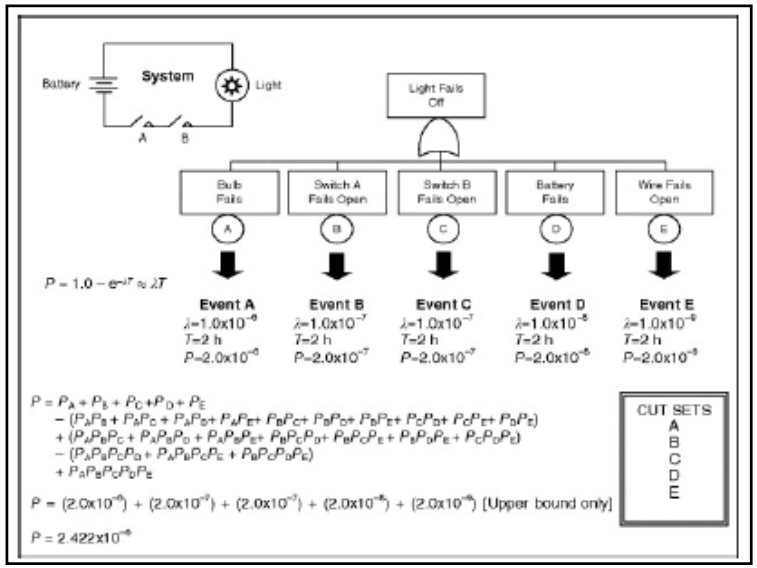


Cut Sets

Event combinations that can cause Top Undesired Event to occur

CS	Probability
A	P_A=1.0x10^{-6}
B	P_B=1.0x10^{-7}
C	P_C=1.0x10^{-7}
D	P_D=1.0x10^{-6}
E	P_E=1.0x10^{-9}

20



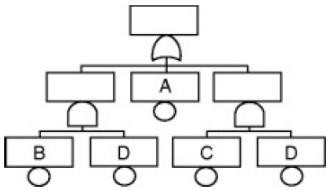
21

Cut Sets

- A set of events that together cause the tress Top Undesired Event (UE) to occur.
- Minimal Cut Set: the minimum number of events that can still cause the top event to occur.
- CS Order: number of items in a CS
  - ⇨One-order CS is a single-point failure (SPF)
- Critical Path: highest probability CS
- MOE: multiple occurring event

22

Cut Sets



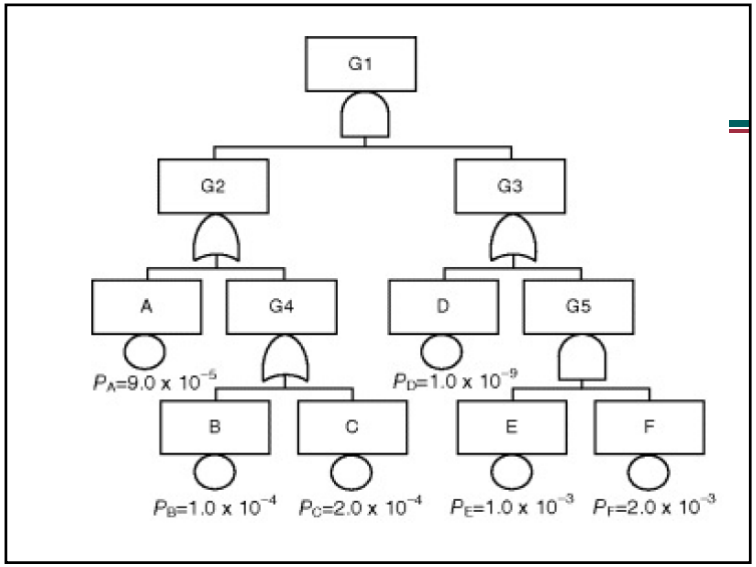
Cut Sets

A	← Order 1	[A]
B, D	← Order 2	[B and D]
C, D	← Order 2	[C and D]

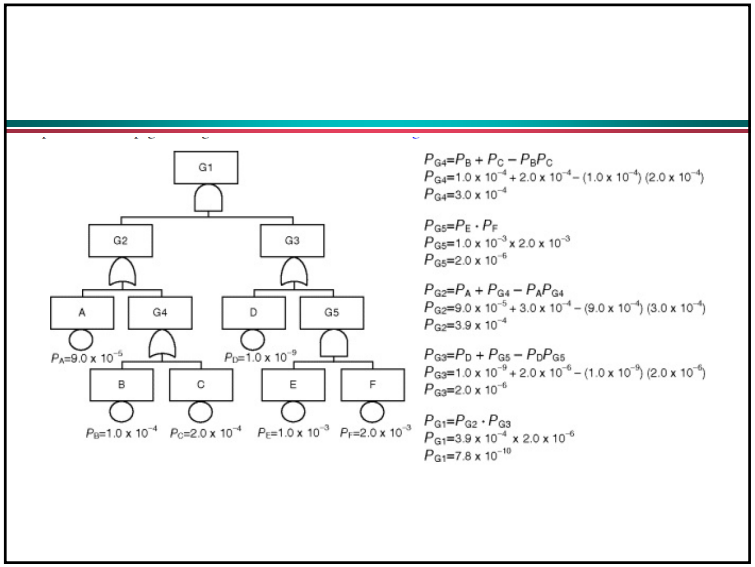
23

FTA Example 2

24



25

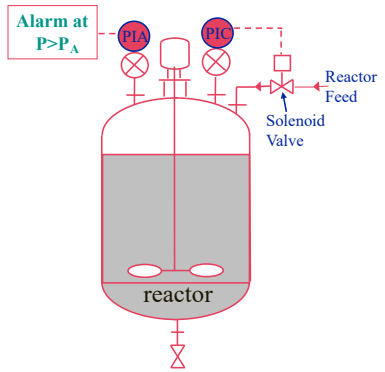


26

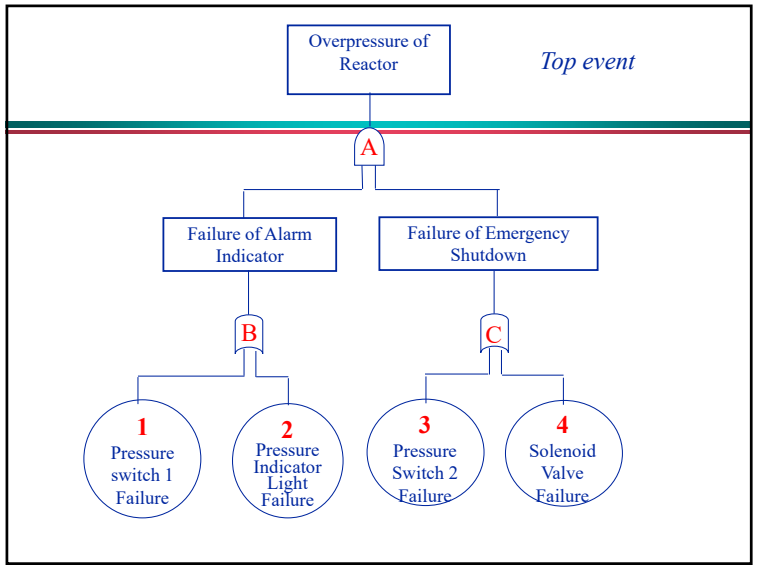
FTA Example 3

27

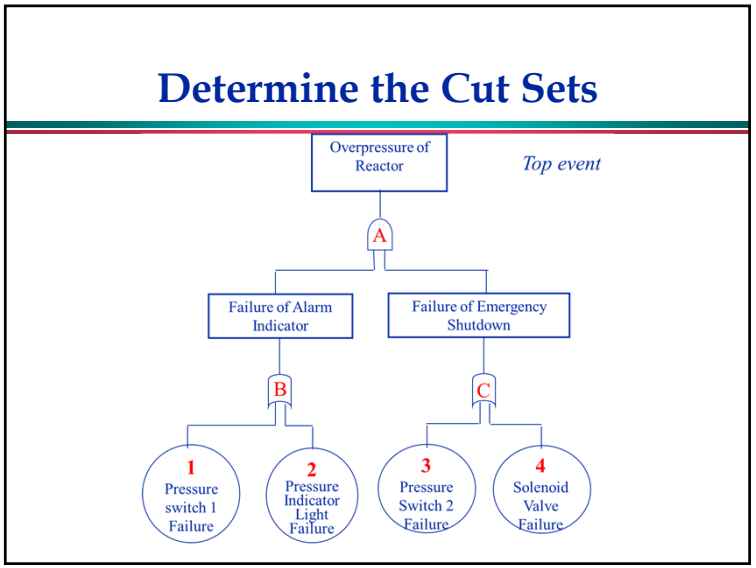
A chemical reactor with an alarm and an inlet feed solenoid. The alarm and feed shutdown systems are linked in parallel.



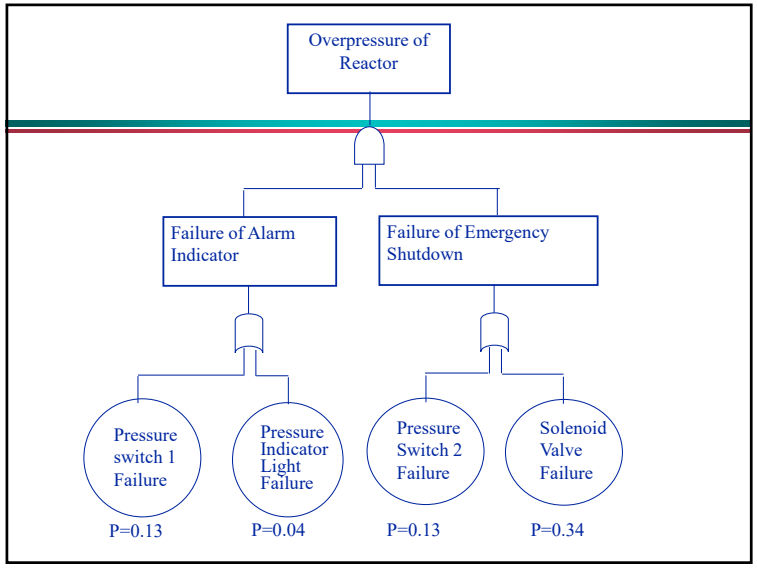
28


Overpressure of Reactor
Top event
A
Failure of Alarm Indicator
Failure of Emergency Shutdown
B
C
1
Pressure switch 1 Failure
2
Pressure Indicator Light Failure
3
Pressure Switch 2 Failure
4
Solenoid Valve Failure

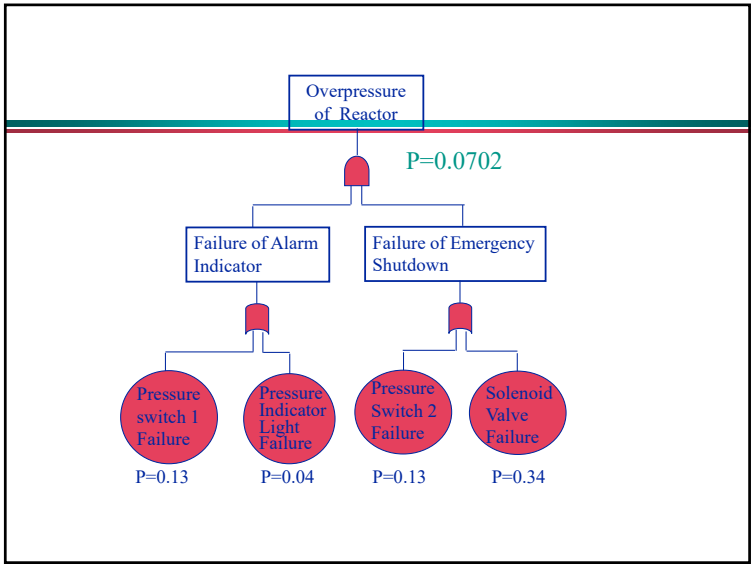
29


Determine the Cut Sets
Overpressure of Reactor
Top event
A
Failure of Alarm Indicator
Failure of Emergency Shutdown
B
C
1
Pressure switch 1 Failure
2
Pressure Indicator Light Failure
3
Pressure Switch 2 Failure
4
Solenoid Valve Failure

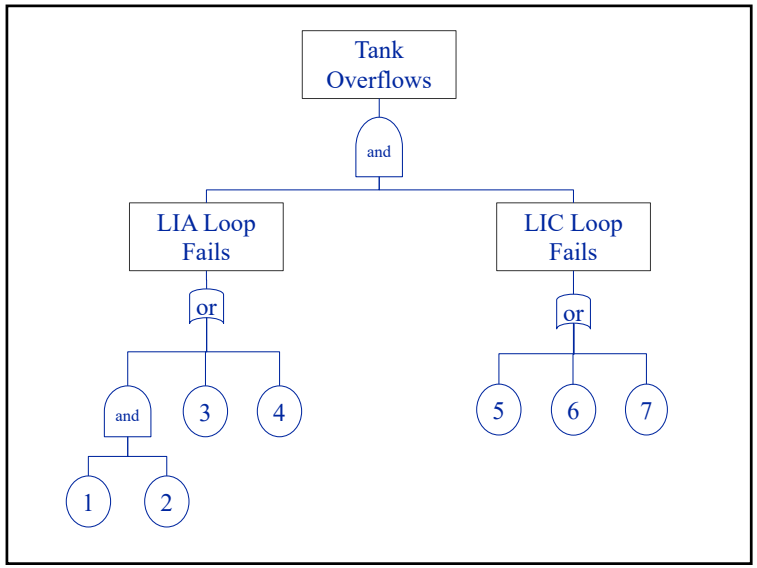
30


Overpressure of Reactor
Failure of Alarm Indicator
Failure of Emergency Shutdown
Pressure switch 1 Failure
Pressure Indicator Light Failure
Pressure Switch 2 Failure
Solenoid Valve Failure
P=0.13
P=0.04
P=0.13
P=0.34

31


Overpressure of Reactor
P=0.0702
Failure of Alarm Indicator
Failure of Emergency Shutdown
Pressure switch 1 Failure
Pressure Indicator Light Failure
Pressure Switch 2 Failure
Solenoid Valve Failure
P=0.13
P=0.04
P=0.13
P=0.34

32


Tank Overflows
and
LIA Loop Fails
LIC Loop Fails
or
or
and
3
4
5
6
7
1
2

33