An Introduction to Fault Tree Analysis

University of Nottingham
UK | CHINA | MALAYSIA

John Andrews

Sally Lunt

Content

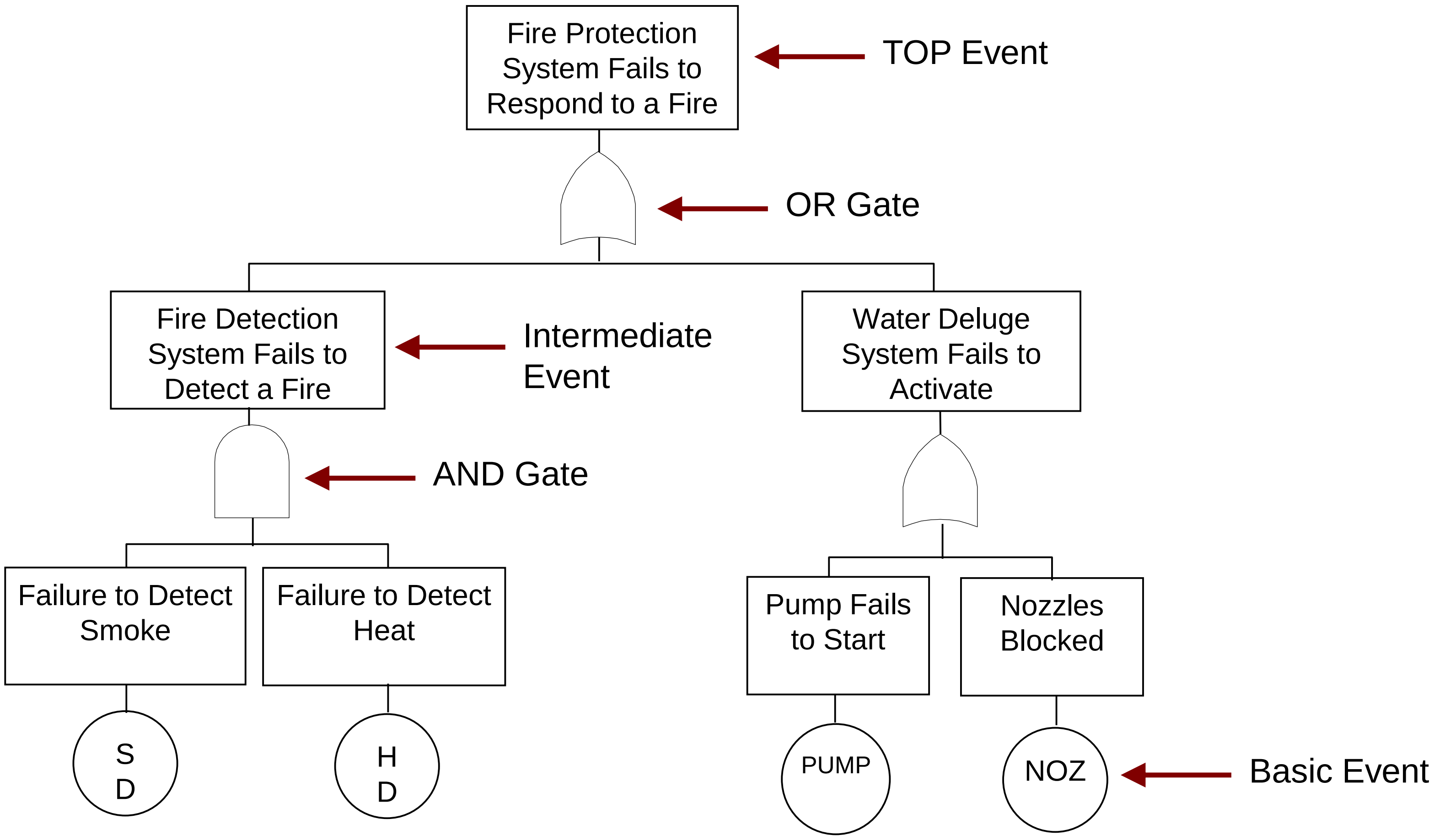
- Fault Tree Analysis Overview
- Symbols
- Fault Tree Construction
- Fault Tree Analysis I
  - Qualitative Analysis
    - Minimal Cut Sets
- Fault Tree Analysis II
  - Top Event Probability

Content

- Fault Tree Analysis III
  - Importance Measures
  - Component Measures
    - Birnbaum’s measure
    - Fussell-Vesely measure
  - Minimal Cut Set Measures
  - Top Event Intensity
- Case Study
- Fault Tree Features Summary

Fault Tree Analysis Overview

Fault Tree Structure



Fault Tree Analysis

- Qualitative
  - Minimal Cut Sets:- minimal (necessary and sufficient) combinations of component failure events which cause the system failure mode.
- Quantitative
  - Unavailability ($Q_{sys}(t)$):- the probability that the system failure mode exists at time t.
  - Unreliability ($F_{sys}(t)$):- the probability that the system failure mode occurs at least once from 0 to time t.
  - Failure rate:- the rate at which the system failure mode occurs
- Component contributions to the system failure

Typical Top Events

- Total Loss of Production.
- Safety System fails to respond.
- Standby System fails to start.

UNAVAILABILITY

- Explosion.
- Loss of space mission.
- Release of radiation.

UNRELIABILITY

Typical Basic Events

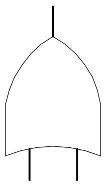
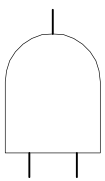
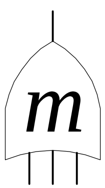
- Pump fails to start.
- Valve fails closed.
- Flow sensor fails to indicate high flow.
- Operator fails to respond.

Symbols

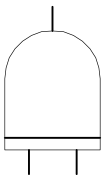
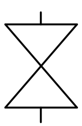
Events

Gates

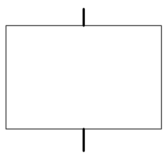
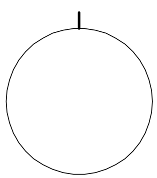
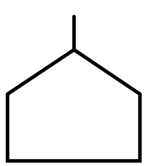
Fault Tree Symbols - Gates

Symbol	Name	Causal Relation
	OR	Output event occurs if at least one of the input events occur.
	AND	Output event occurs if all input events occur.
	Vote	Output event occurs if at least *m* of the input events occur.

Fault Tree Symbols - Gates

Symbol	Name	Causal Relation
	Priority AND	Output event occurs if all input events occur in sequential order from left to right.
	Not	Output event occurs if the input event does not occur.

Fault Tree Symbols - Events

Symbol	Name	Meaning
	Intermediate	System or component event description.
	Basic	Basic event for which failure and repair data is available. Usually represents a component failure.
	House	Represents definitely occurring or definitely not occurring events.

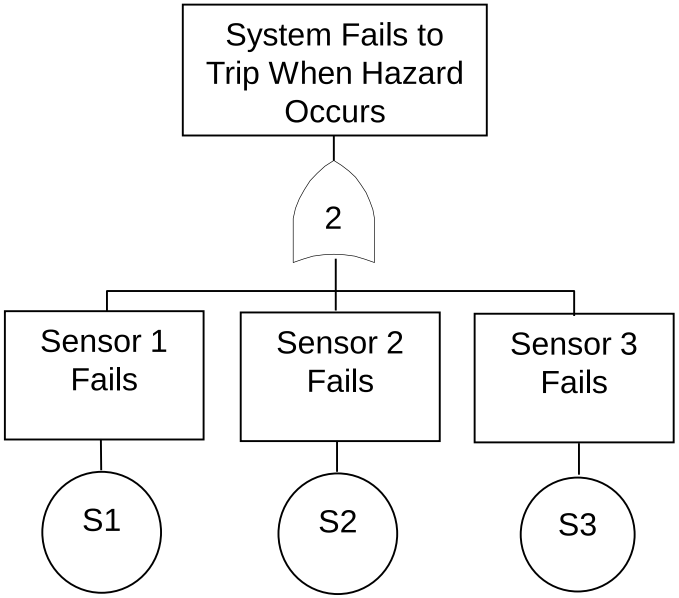
Gate Examples: Vote Gate

Example: System has 3 sensors to detect hazard

2 sensors required to detect hazard to cause trip

2-out-of-3:W

Fault Trees represent system failure causes (2-out-of-3:F)



Minimal Cut Sets

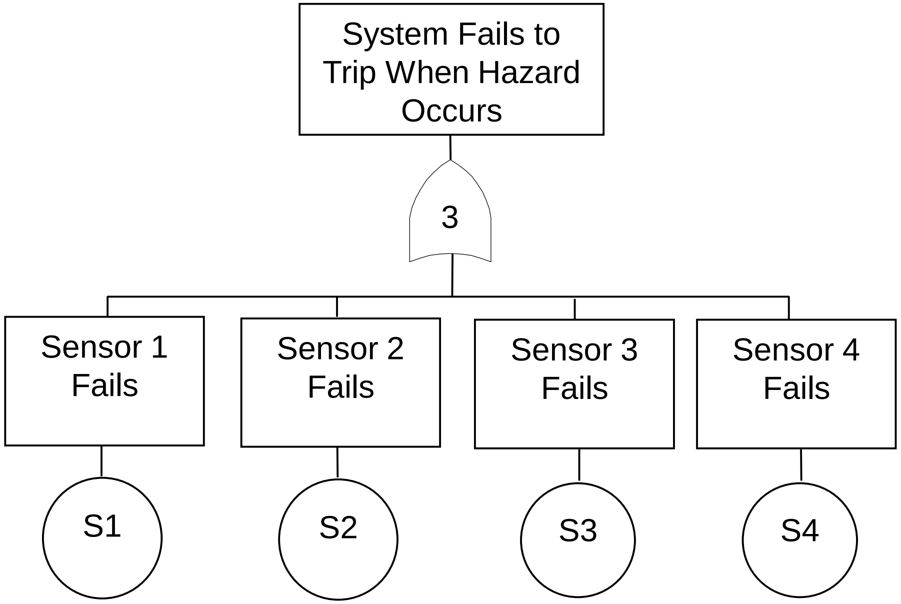
1. S1.S2
2. S2.S3
3. S3.S1

Gate Examples: Vote Gate

Example: System has 4 sensors to detect hazard

2 sensors required to detect hazard to cause trip

2-out-of-4:W $\Rightarrow$ 3-out-of-4:F

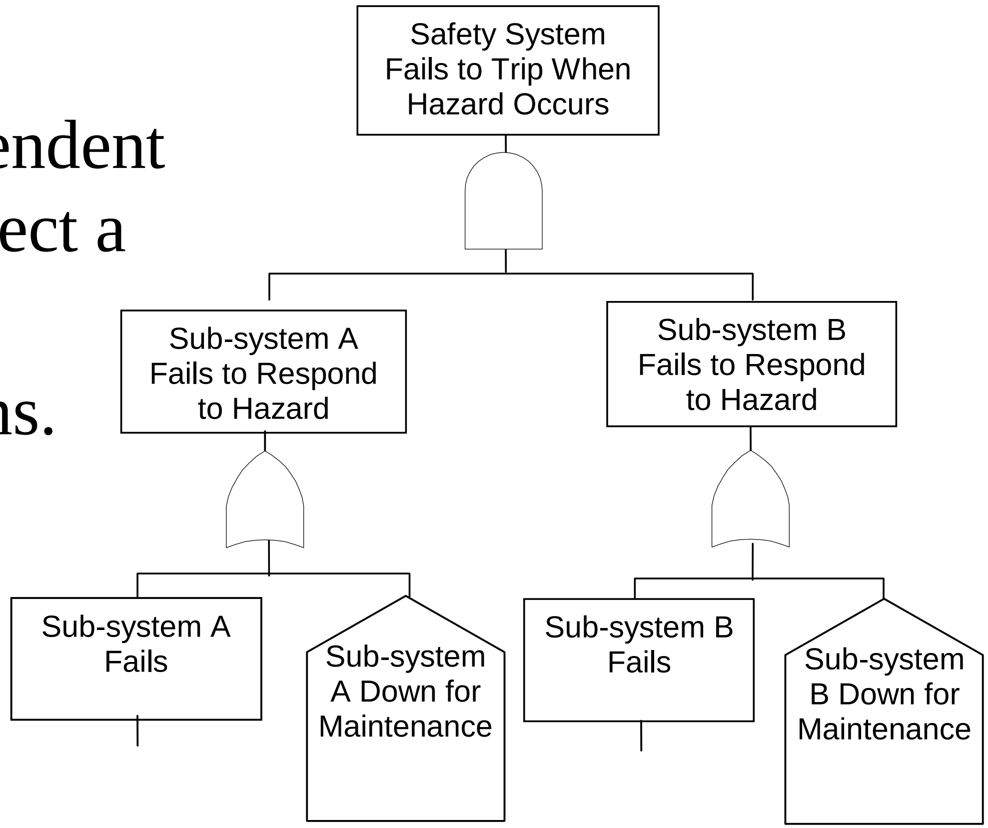


Event Examples: House Event (System Operating Modes)

Safety system has two independent sub-systems (A and B) to detect a hazard and trip system.

Operates under two conditions.

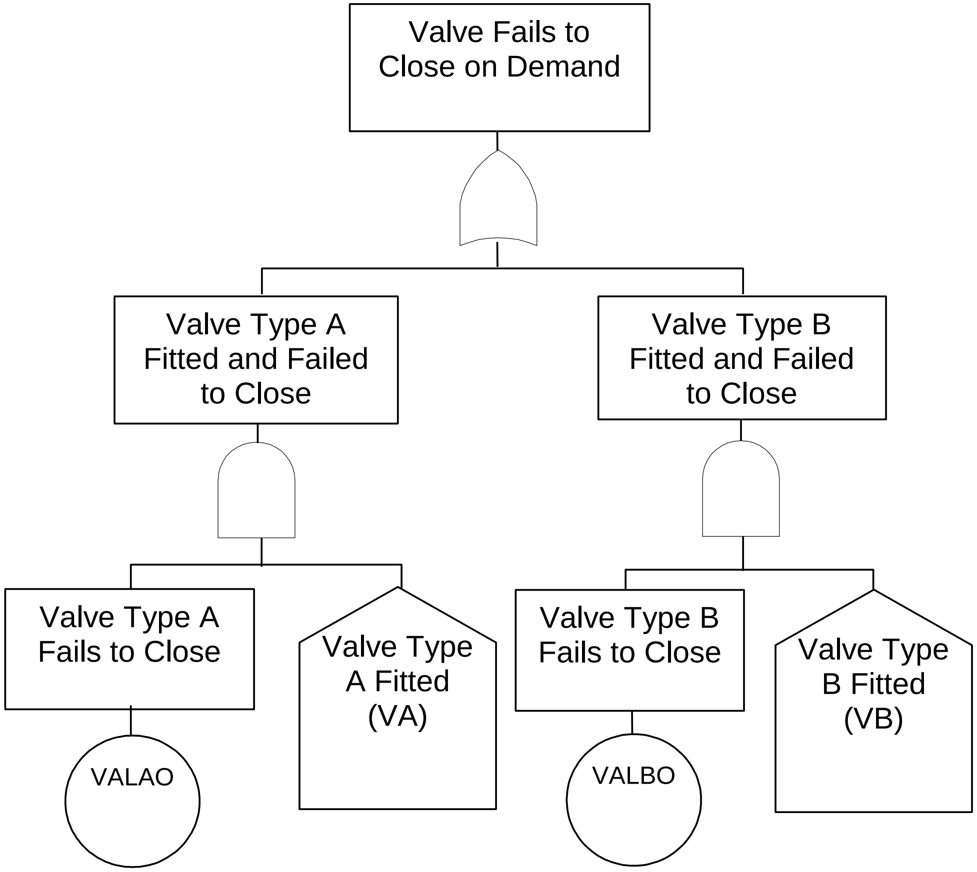
1. No maintenance.
2. One sub-system (say A) out for maintenance.



House events = TRUE (T) or FALSE (F)

Event Example: House Events (System Design Options)

Example: a valve of type A or B can be fitted.



Note:

VA OR VB = TRUE

VA AND VB = FALSE

Fault Tree Construction

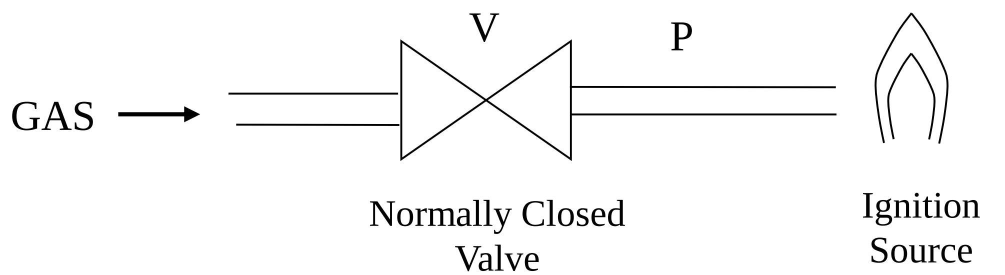
Guidelines for Fault Tree Construction

No set of rules can be given to guarantee construction of the correct fault tree.

Guidelines can be given.

- No Miracles:

  If the normal functioning of a component propagates a fault sequence then it is assumed that the component functions normally.



Fire if gas passes to ignition source (V fails open).
But what about failures of Pipe (P) - Blocked
So failure mode is $V.\overline{P}$ – miracle! (introduces not logic)

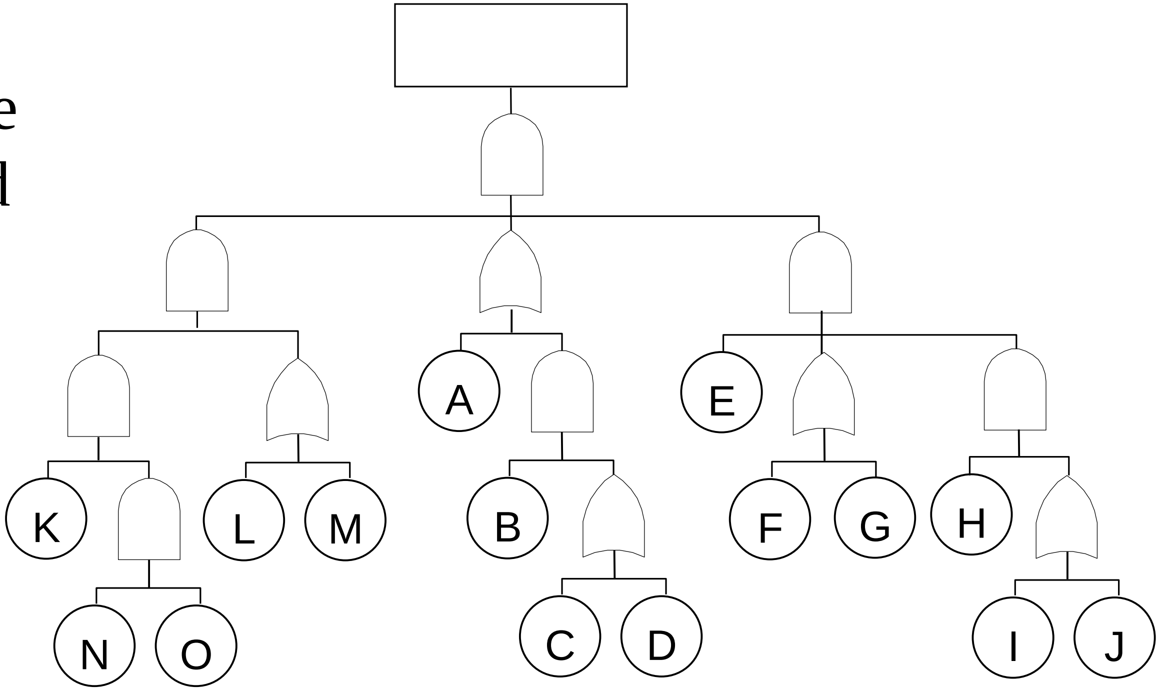
Guidelines for Fault Tree Construction

- Complete-the-gate:

  Define all inputs to a gate before the further development of any one is undertaken.

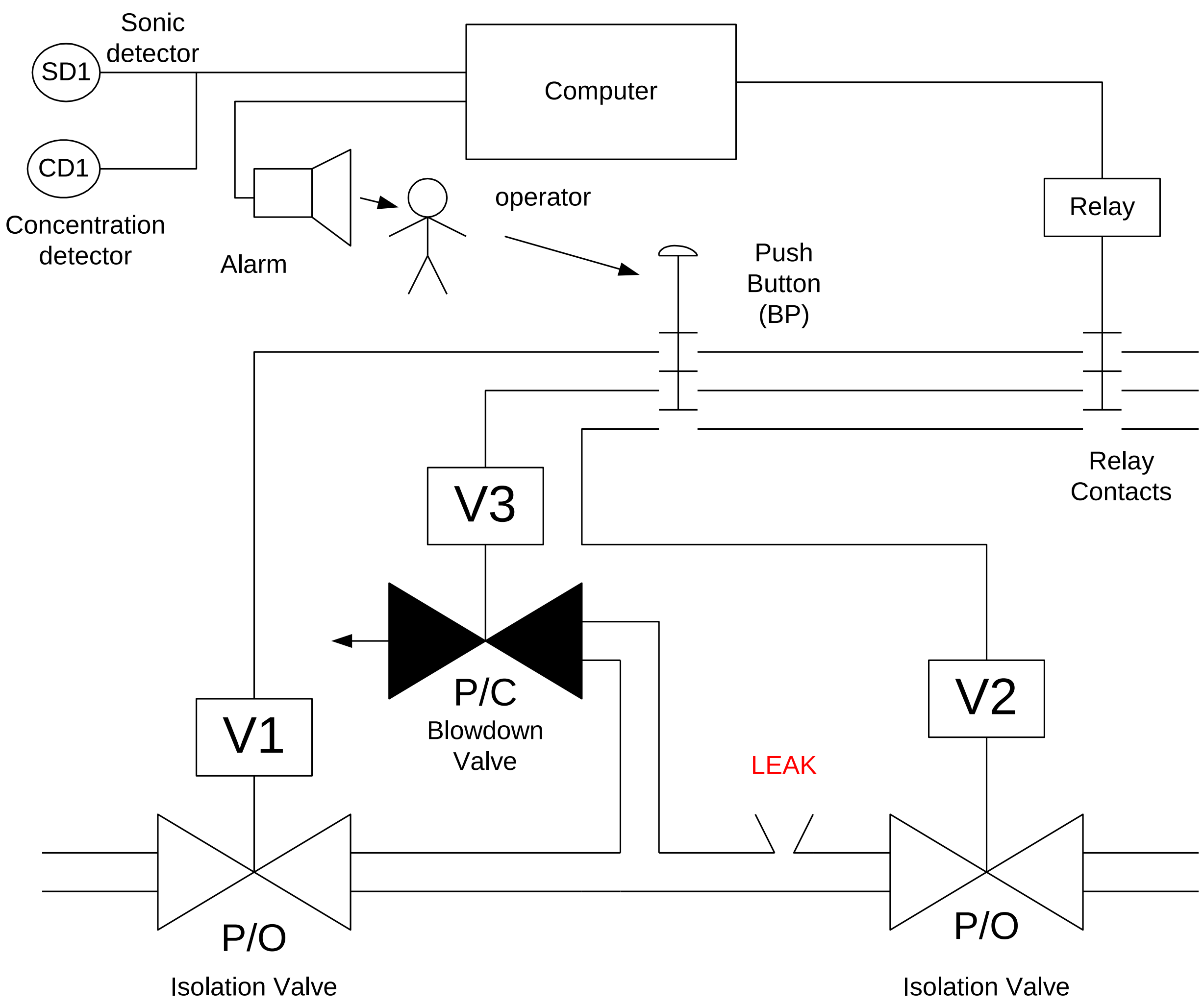
- No gate-to-gate:

  Gate inputs should be properly defined and gates should not be directly connected to other gates.



Gas Leak Detection System

Gas Leak Detection System



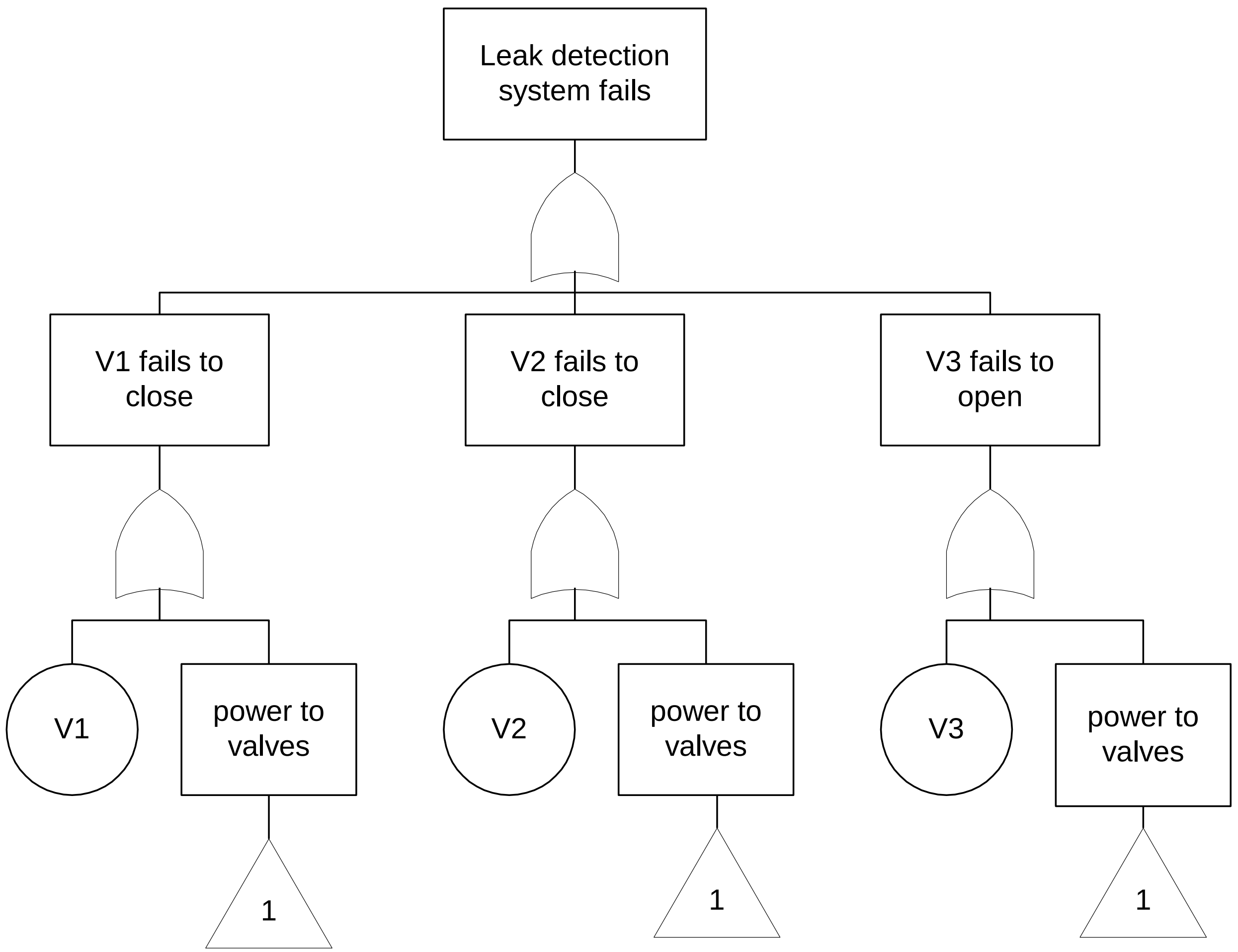
Gas Leak Detection System - Component Failure Modes

Component failure mode	code
Isolation valve 1 fails to close	V1
Isolation valve 2 fails to close	V2
Blowdown valve 3 fails to open	V3
Operator unavailable	OP
Computer fails to process trip condition	COMP
Alarm fails to sound	AL
Relay contacts stuck closed	CONT
Concentration detector fails to register leak	CD1
Sonic detector fails to register leak	SD1
Push Button contacts stuck closed	PB

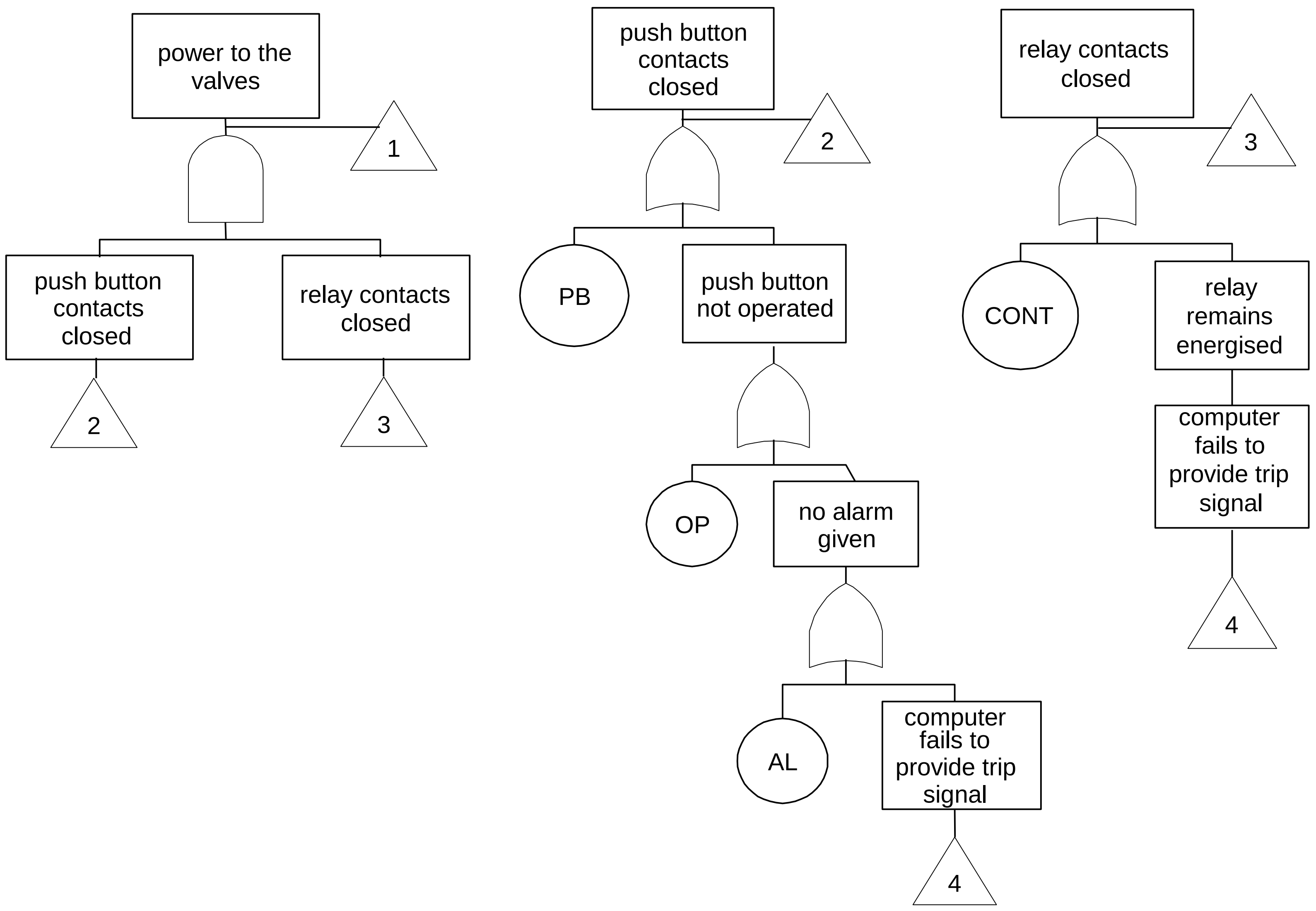
Gas Leak Detection System

- Given a gas leak the system should perform three tasks:
  - close isolation valve V1
  - close isolation valve V2
  - open blowdown valve V3
- Fault tree Top Event ‘leak detection system fails’

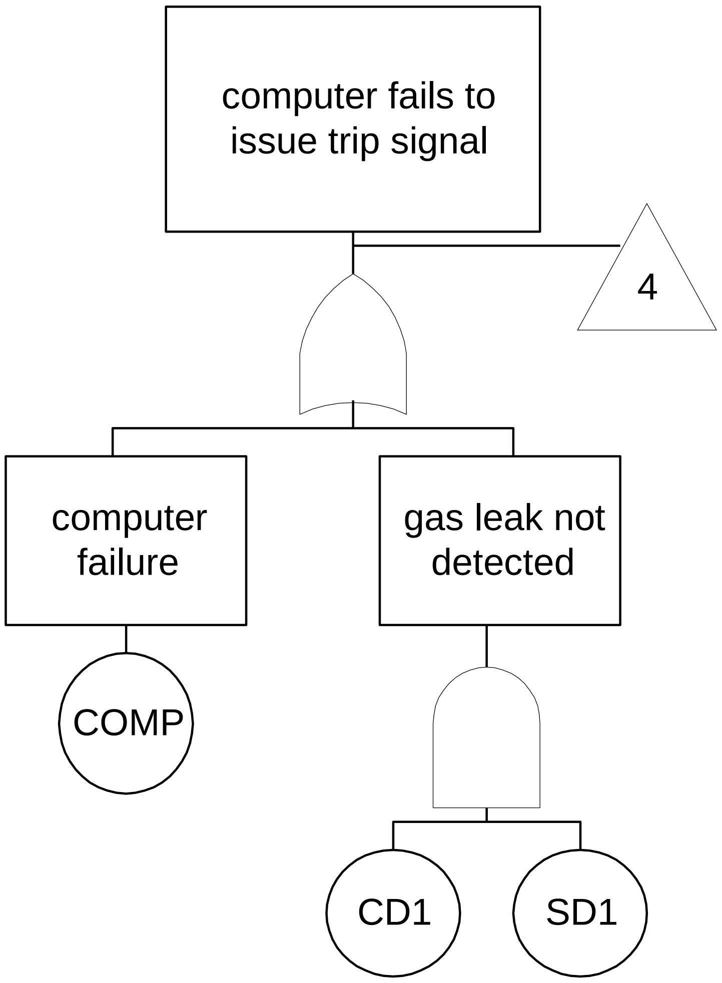
Gas Leak Detection System



Gas Leak Detection System



Gas Leak Detection System - Solution



Fault Tree Analysis I

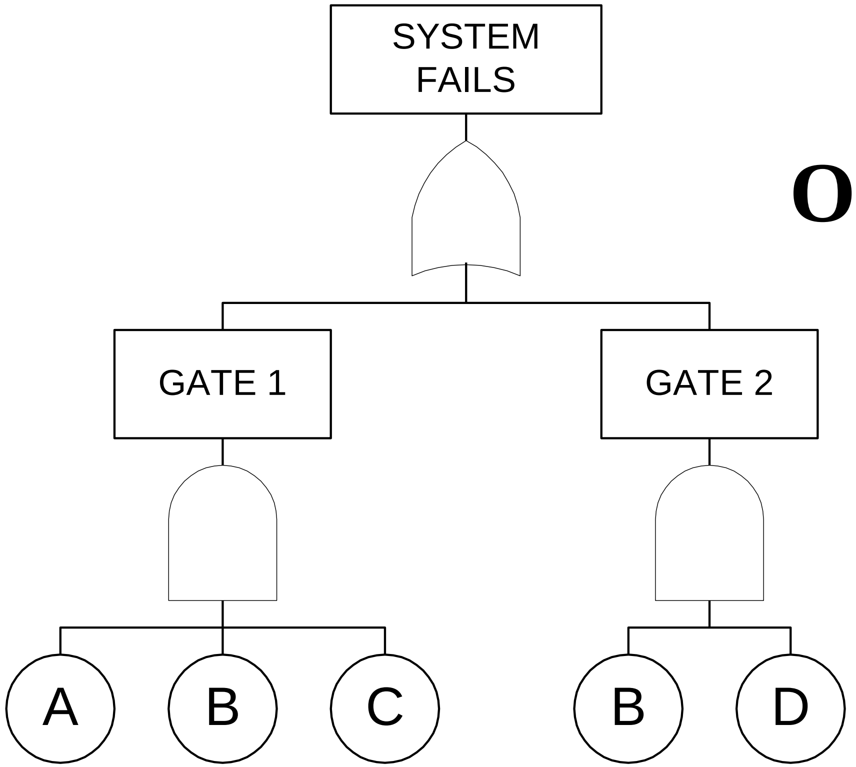
Qualitative Analysis
Minimal Cut Sets

Minimal Cut Sets

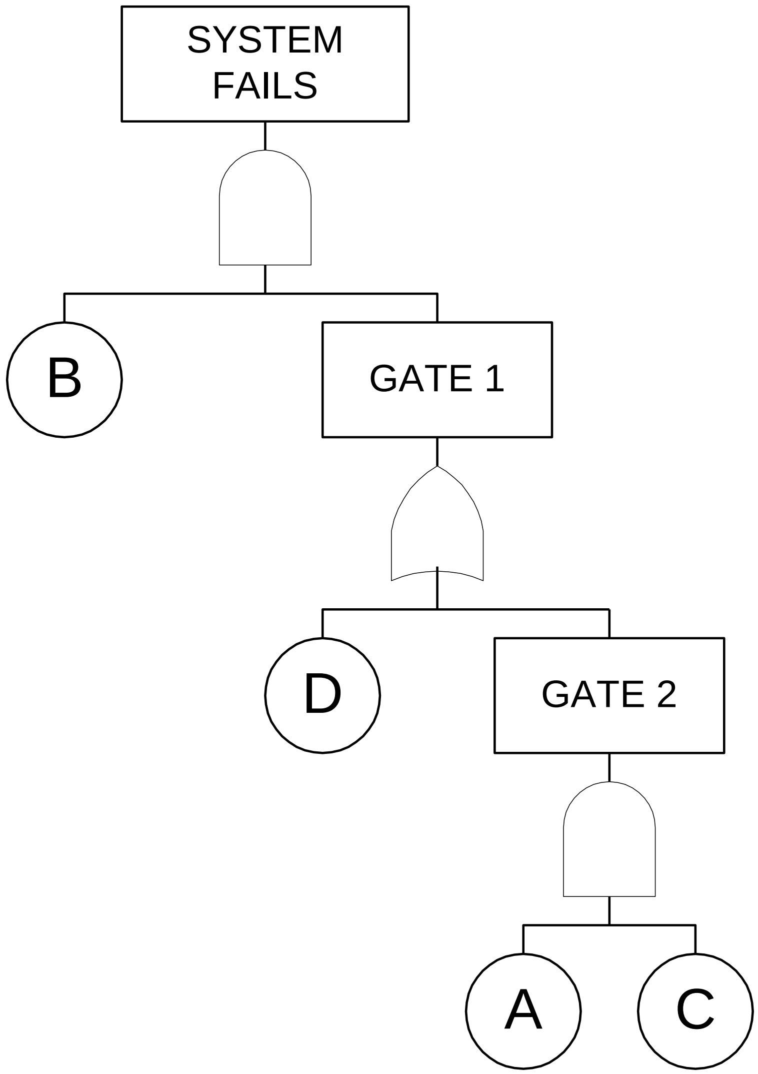
- **Cut Set**
  - A list of component failed states which cause the system failure mode.

- **Minimal Cut Set**
  - A minimal (necessary and sufficient) list of component failed states which cause the system failure mode.

Fault Tree Structures



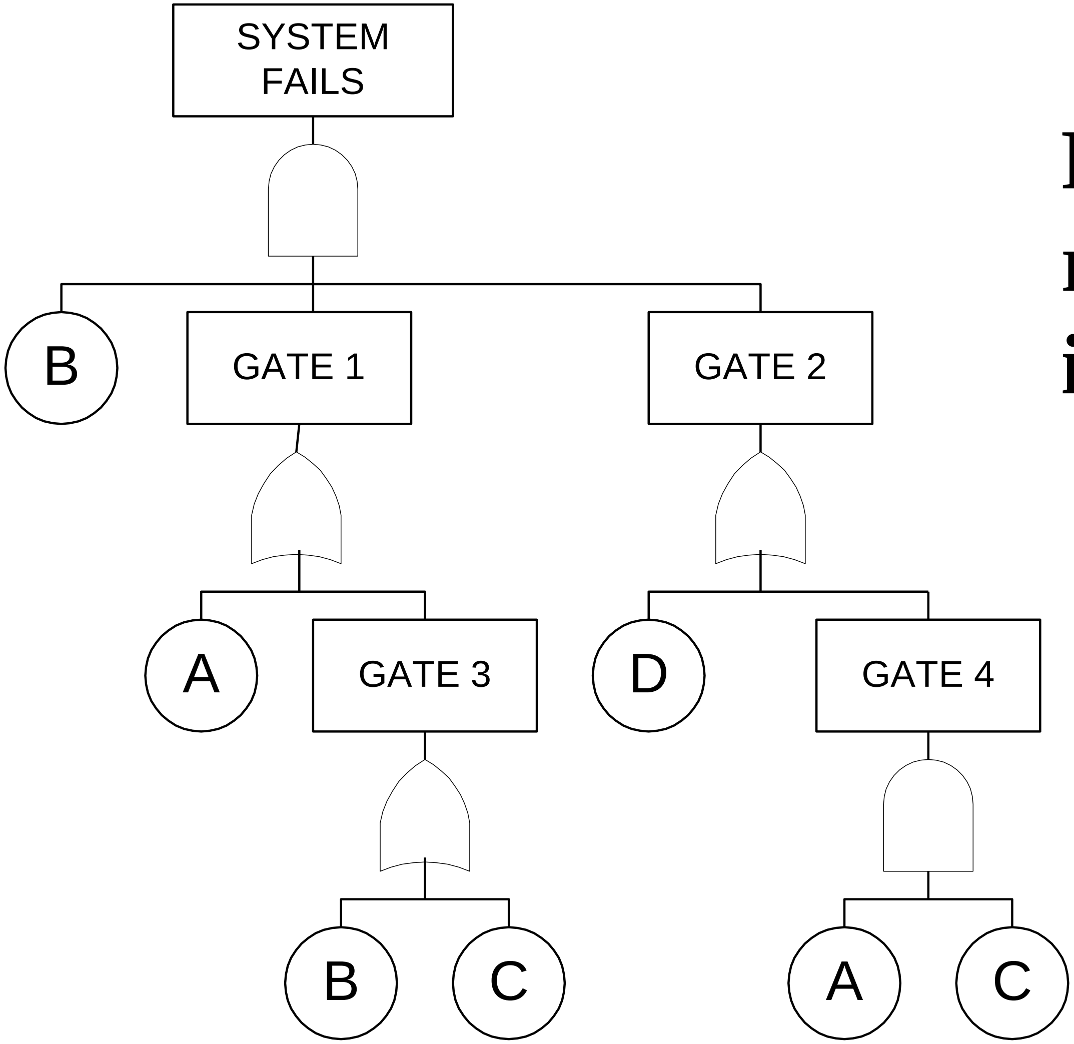
OR



Minimal Cut Sets:

1. **BD**
2. **ABC**

Fault Tree Structures



Fault tree representation is not unique

Boolean Algebra

Variables

$$\text{Let } A = \begin{cases} \text{TRUE}(1) & \text{Component A fails} \\ \text{FALSE}(0) & \text{Component A works} \end{cases}$$

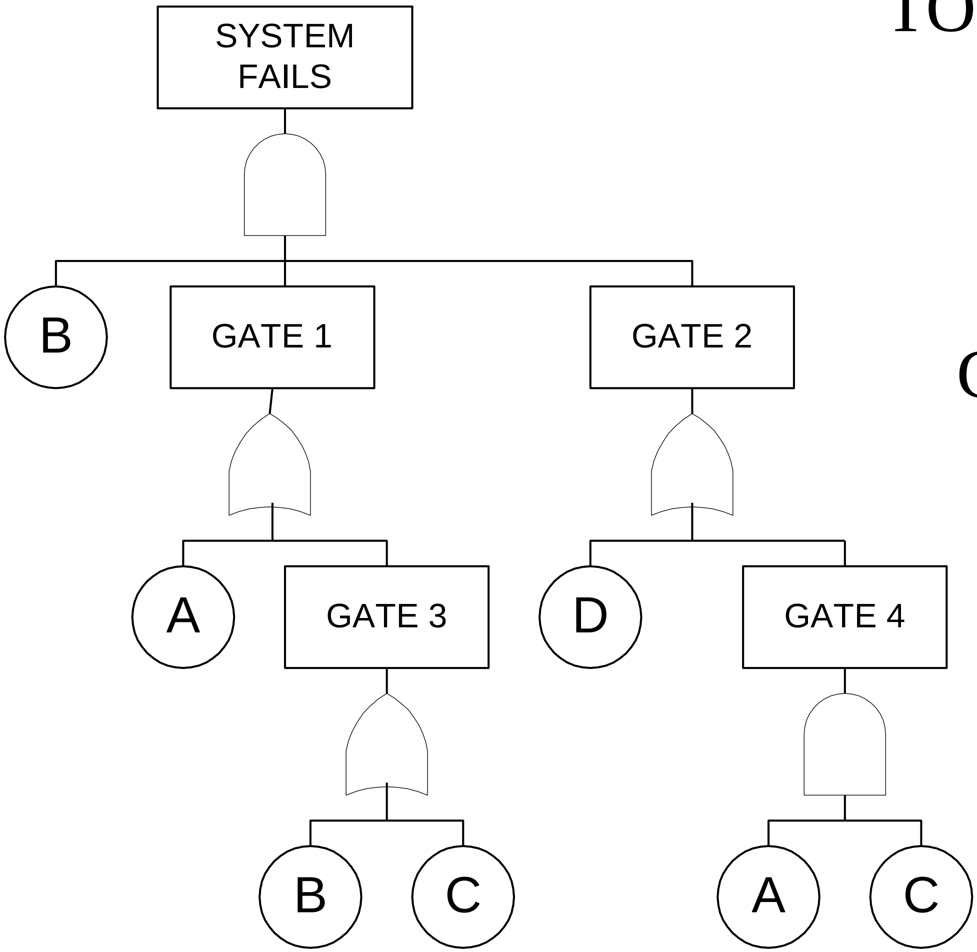
$$\text{TOP} = \begin{cases} \text{TRUE}(1) & \text{System failure mode exists} \\ \text{FALSE}(0) & \text{System works} \end{cases}$$

+ - OR . - AND

Laws

Distributive	A.(B+C) = A.B+A.C
Idempotent	A+A = A
	A.A = A
Absorption	A+A.B = A

Minimal Cut Sets



TOP=B.GATE1.GATE2

=B.(A+GATE3).
(D+GATE4)

=B.(A.D+A.GATE4+
GATE3.D+GATE3.GATE4)

=B.[A.D+A.A.C+
(B+C).D+(B+C).A.C]

=B.[A.D+A.A.C+B.D+
+C.D+B.A.C+C.A.C]

Minimal Cut Sets

$$TOP = B.(A.D + \boxed{A.A.C} + B.D + C.D + \boxed{B.A.C} + \boxed{C.A.C})$$

Reduction Laws:

Idempotent: $\boxed{\mathbf{X.X = X}}$ $\boxed{\mathbf{X + X = X}}$

Absorption: $\boxed{\mathbf{X + X.Y = X}}$

$$TOP = B.(A.D + A.C + B.D + C.D)$$

$$TOP = \boxed{B.A.D} + B.A.C + \boxed{B.B.D} + \boxed{B.C.D}$$

$$TOP = B.A.C + B.D$$

Fault Tree Analysis II

Top Event Probability

Component Failure Probability

$\Downarrow$

Minimal Cut Set Failure Probability

$\Downarrow$

System Failure Probability

Component Failure Probabilities

- Unavailability of components is calculated differently depending on maintenance policy used.

- Three Maintenance Policies:

  - No Repair.
  - Repair when failure is revealed.
    (Unscheduled Maintenance)
  - Repair when failure is discovered.
    (Scheduled Maintenance)

Maintenance Policy - No Repair

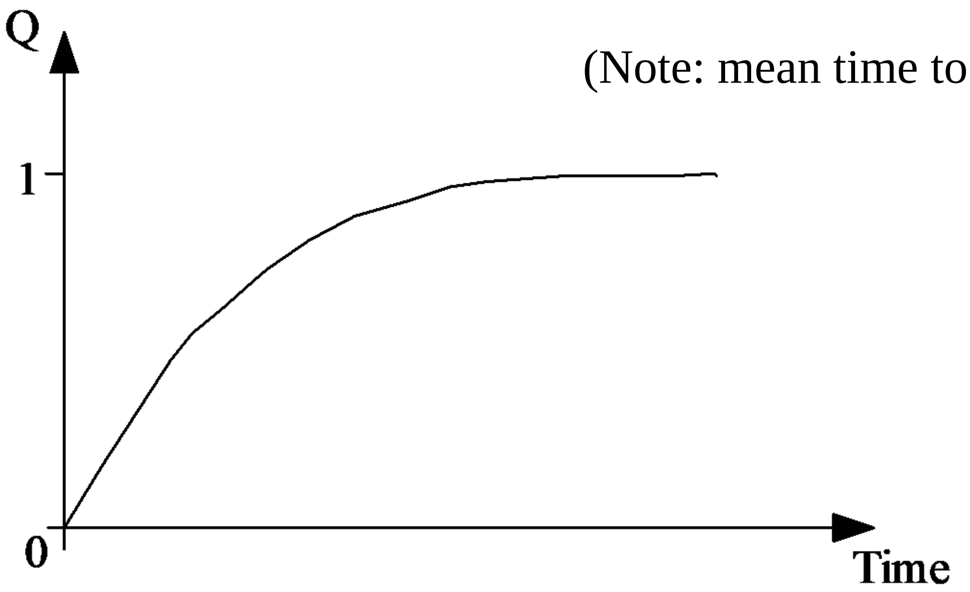
- Typical of remotely controlled systems
- $$Q(t) = F(t) = 1 - e^{-\lambda t}$$

Q – unavailability

F – unreliability

λ – failure rate

(Note: mean time to failure $\mu = \dfrac{1}{\lambda}$)

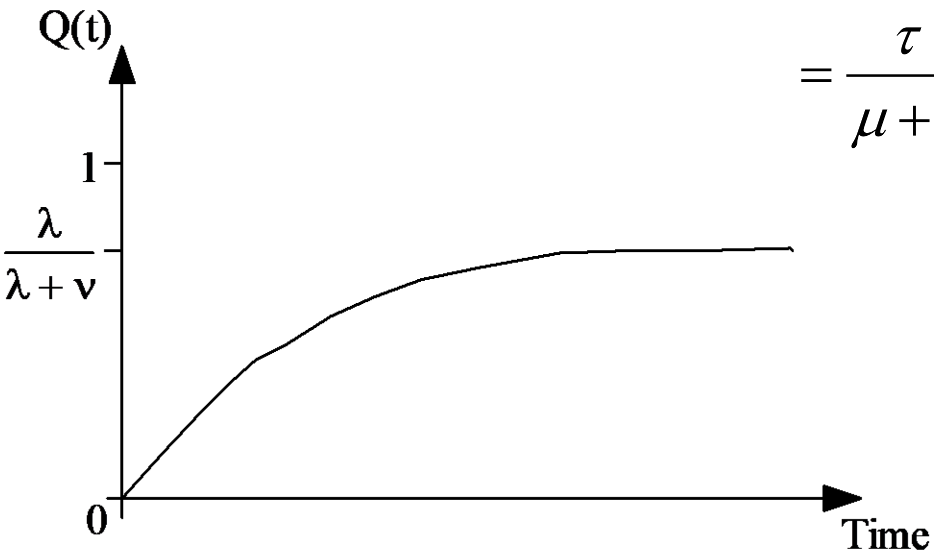


Maintenance Policy - Unscheduled Maintenance

- $$Q(t) = \frac{\lambda}{\lambda + \nu}\left(1 - e^{-(\lambda+\nu)t}\right)$$

STEADY-STATE

- As $t \to \infty$ $$Q_\infty \to \frac{\lambda}{\lambda+\nu} = \frac{\tau}{\mu+\tau}$$



λ – failure rate $= \frac{1}{\mu}$

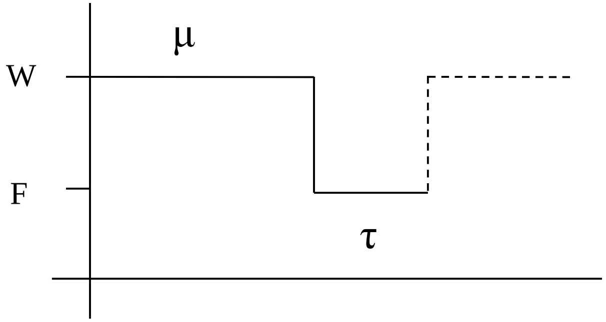
μ – mean time to failure

υ – repair rate $= \frac{1}{\tau}$

τ – mean time to repair

Maintenance Policy – Unscheduled Maintenance

Average Cycle



μ – mean time to failure

τ – mean time to repair

Note: $\mu >> \tau$

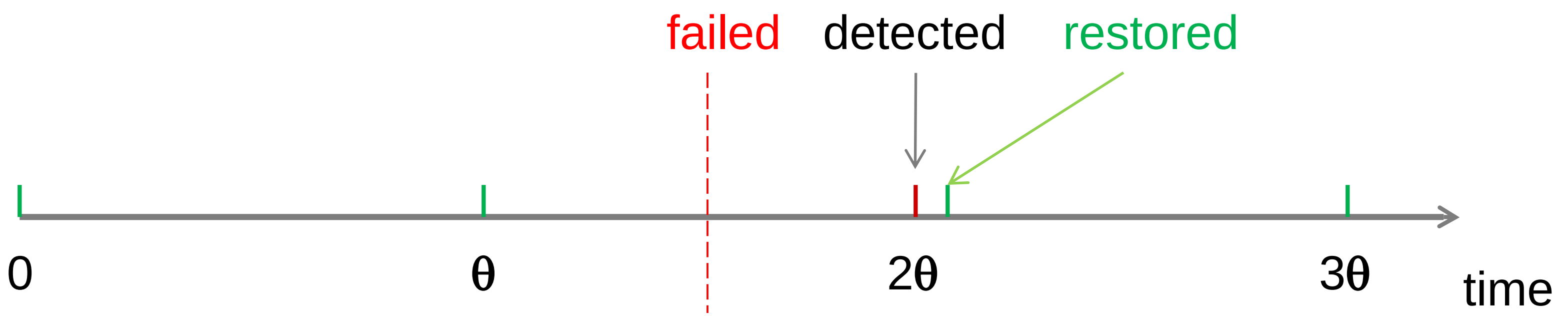
$\therefore \mu + \tau \approx \mu$

$$Q_{\infty} = \frac{\tau}{\mu + \tau} \approx \frac{\tau}{\mu} \approx \lambda\tau$$

i.e. (failure rate) x (mean time to repair/restore)

Maintenance Policies - Scheduled Maintenance

- If: θ - time between inspections



- Time to restore = detection time + repair time
- R_{AV} - average restoration time.

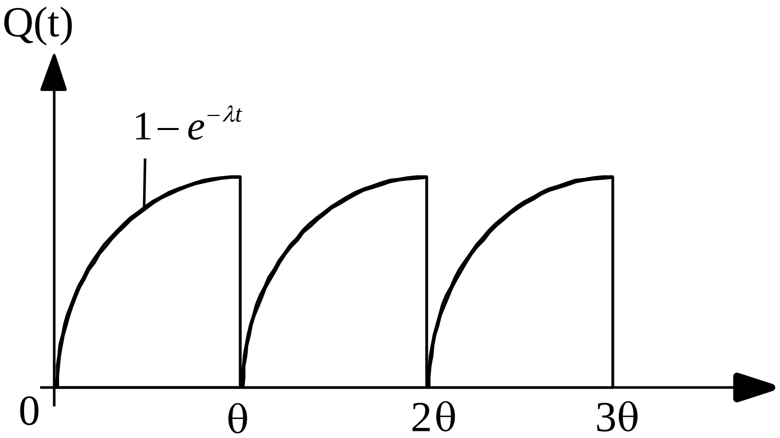
$$R_{AV} = \frac{\theta}{2} + \tau$$

$$Q_{AV} = \lambda R_{AV} = \lambda\left(\frac{\theta}{2} + \tau\right)$$

$$\theta >> \tau \qquad Q_{AV} \approx \frac{\lambda\theta}{2}$$

Maintenance Policies - Scheduled Maintenance

- More accurately:



- $$Q_{AV} = \frac{1}{\theta}\int_0^{\theta}(1-e^{-\lambda t})dt$$

$$= \frac{1}{\theta}\left[t + \frac{e^{-\lambda t}}{\lambda}\right]_0^{\theta}$$

$$= 1 - \frac{\left(1-e^{-\lambda\theta}\right)}{\lambda\theta}$$

Minimal Cut Set Failure Probabilities

If $C_i = X_1.X_2. \ldots X_n$

then $P(C_i) = P(X_1).P(X_2). \ldots .P(X_n)$

assuming all X_i independent.

i.e. $$P(C_i) = \prod_{j=1}^{n} P(X_j)$$

Example If C_i = A.B.C

P(A) = 0.1, P(B) = 0.05, P(C) = 0.001

$P(C_1) = 0.1 \times 0.05 \times 0.001 = 5 \times 10^{-5}$

Inclusion- Exclusion Principle

- From Minimal Cut Sets:

$$TOP = C_1 + C_2 + \cdots + C_{N_C}$$

$$Q_{SYS} = P(TOP) = P(C_1 + C_2 + \cdots + C_{N_C})$$

C_i – ith Minimal Cut Set

N_C – Number of Minimal Cut Sets

- Top Event Probability

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

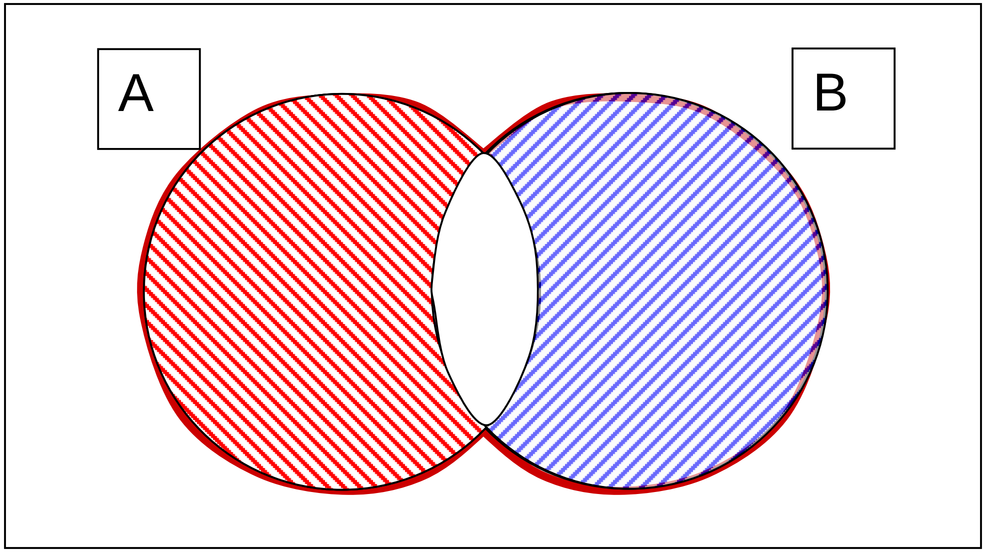
$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

Inclusion- Exclusion Principle

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

TWO EVENTS



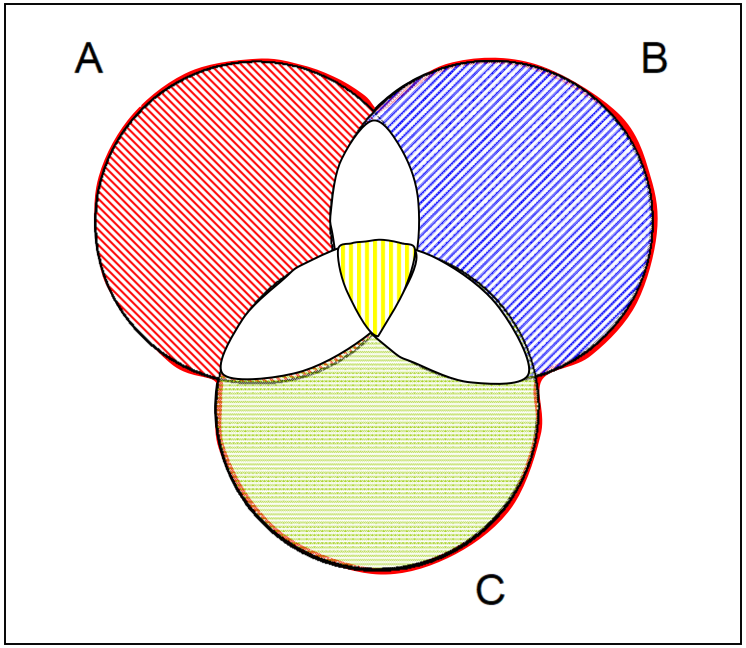
P(A+B) = P(A) + P(B) – P(A.B)

Inclusion- Exclusion Principle

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

THREE EVENTS



P(A+B+C) = P(A) + P(B) + P(C)– P(AB)– P(BC)– P(CA) + P(ABC)

Example

If $C_1 = A$ $C_2 = B.C$ $C_3 = B.D$ $C_4 = D.E.F$

assume all failure probabilities = 0.1

$$
\begin{aligned}
P[TOP] &= [P(C_1) + P(C_2) + P(C_3) + P(C_4)] - [P(C_1.C_2) + P(C_1.C_3) + P(C_1.C_4) + \\
&\quad P(C_2.C_3) + P(C_2.C_4) + P(C_3.C_4)] + [P(C_1.C_2.C_3) + P(C_1.C_2.C_4) + \\
&\quad P(C_1.C_3.C_4) + P(C_2.C_3.C_4)] - [P(C_1.C_2.C_3.C_4)] \\
&= [P(A) + P(B.C) + P(B.D) + P(D.E.F)] - [P(A.B.C) + P(A.B.D) + \\
&\quad P(A.D.E.F) + P(B.C.D) + P(B.C.D.E.F) + P(B.D.E.F)] + [P(A.B.C.D) + \\
&\quad P(A.B.C.D.E.F) + P(A.B.D.E.F) + P(B.C.D.E.F)] - [P(A.B.C.D.E.F)] \\
&= [0.1 + 0.01 + 0.01 + 0.001] - [0.001 + 0.001 + 0.0001 + 0.001 + 0.00001 \\
&\quad + 0.0001] + [0.0001 + 0.000001 + 0.00001 + 0.00001] - [0.000001] \\
&= [0.121] - [0.00321] + [0.000112] - [0.000001] \\
&= 0.117901
\end{aligned}
$$

1 term	0.121	(U)
2 terms	0.11779	(L)
3 terms	0.117902	(U)
4 terms	0.117901	(Exact)

Top Event Probability

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

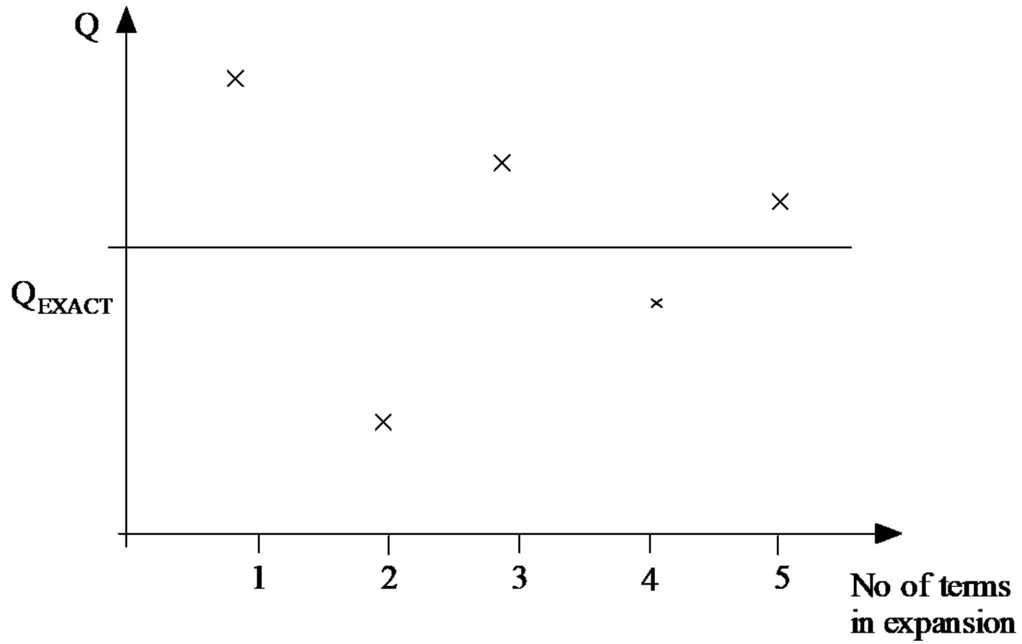
- If large number of minimal cut sets eg. 100,000 (10^5)
  - Number of terms in full expansion : 10^5
    - No. of elements in first term = 10^5
    - No. of elements in second term ≈ 5 x 10^9
    - No. of elements in third term ≈ 1.7 x 10^{14}
    - - etc…...
- Even for fast modern digital computers this calculation can be too CPU intensive!

Approximations

$$Q_{SYS} = \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{N_C} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \cdots$$

$$\cdots + (-1)^{N_C+1} P(C_1 \cap C_2 \cdots \cap C_{N_C})$$

Inclusion-exclusion principle



Approximations

- Rare Event

$$Q_{SYS} \leq \sum_{i=1}^{N_C} P(C_i)$$

- Lower Bound

$$Q_{SYS} \geq \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j)$$

- Minimal Cut Set Upper Bound

$$Q_{SYS} \leq 1 - \prod_{i=1}^{N_C} (1 - P(C_i))$$

Example

If $C_1 = A$ $C_2 = B.C$ $C_3 = B.D$ $C_4 = D.E.F$
assume all failure probabilities = 0.1

P[TOP] = $[P(C_1) + P(C_2) + P(C_3) + P(C_4)] – [P(C_1.C_2) + P(C_1.C_3) + P(C_1.C_4) + P(C_2.C_3) + P(C_2.C_4) + P(C_3.C_4)] + [P(C_1.C_2.C_3) + P(C_1.C_2.C_4) + P(C_1.C_3.C_4) + P(C_2.C_3.C_4)] – [P(C_1.C_2.C_3.C_4)]$

= [0.121] – [0.00321] + [0.000112] – [0.000001]

= 0.117901

Rare Event: $$Q_{SYS} \leq \sum_{i=1}^{N_C} P(C_i) = 0.121$$

Lower Bound: $$Q_{SYS} \geq \sum_{i=1}^{N_C} P(C_i) - \sum_{i=2}^{N_C} \sum_{j=1}^{i-1} P(C_i \cap C_j) = 0.121 - 0.00321 = 0.11779$$

Approximation – Example

Minimal Cut Set Upper Bound

$$Q_{SYS} \leq 1 - \prod_{i=1}^{N_C} \left(1 - P(C_i)\right)$$

If $C_1 = A$ $C_2 = B.C$ $C_3 = B.D$ $C_4 = D.E.F$

all failure probabilities = 0.1

$= 1 - (1 - 0.1)(1-(0.1)^2)^2(1-(0.1)^3)$

$= 0.118792$

$$Q_{LOWER} \leq Q_{SYS} \leq Q_{MCSU} \leq Q_{RE}$$

$$0.11779 \leq 0.117901 \leq 0.118792 \leq 0.121$$

Fault Tree Analysis III

Importance Measures

Importance Measures

- Indicate, in some sense, the contribution each component of the system makes to the system failure event.

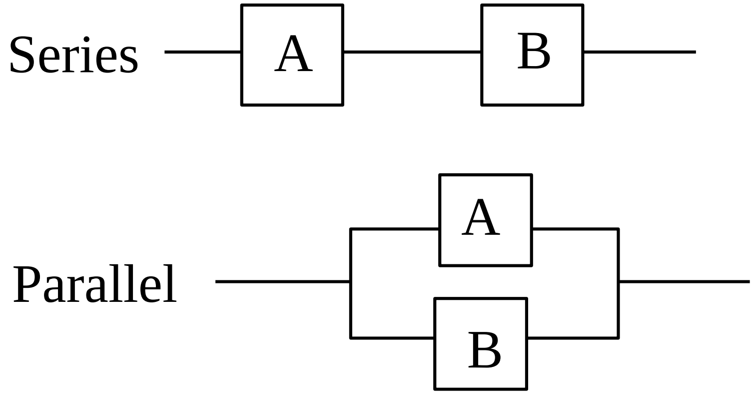
- Contribution is dependent upon:
  - Susceptibility of system to fail when component fails.
    - Vulnerability:- redundancy, diversity
    - Chance of a component being in a failed state.
      - frequency of a component failure.
      - time to repair component.

Types of Importance Measures

- Two distinct types:
  - Deterministic → Consider only the structure of the system
  - Probabilistic → Availability
    → Reliability

Critical System States

A critical system state for component i is a state for the remaining n-1 components such that failure of component i causes the system to go from a working to a failed state.



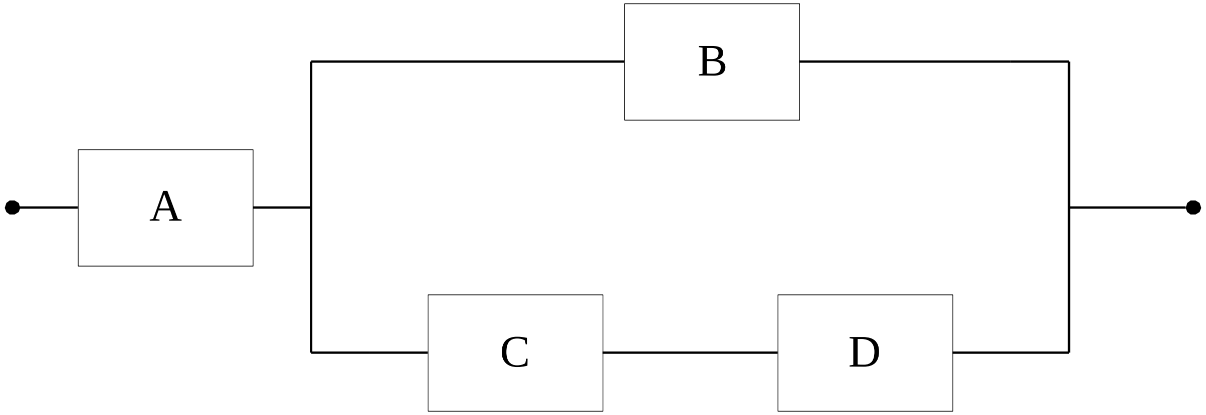
SYSTEM	STATE	PROBABILITY	CRITICAL FOR A ?
Series	$(\cdot, B)$	q_B	No
	$(\cdot, \overline{B})$	$1 - q_B$	Yes
Parallel	$(\cdot, B)$	q_B	Yes
	$(\cdot, \overline{B})$	$1 - q_B$	No

Deterministic Importance Measures

Structural Importance Measure

$$I = \frac{\text{number of critical states for component i}}{\text{total number of states for the (n-1) remaining components}}$$

Example Structural Importance Measure

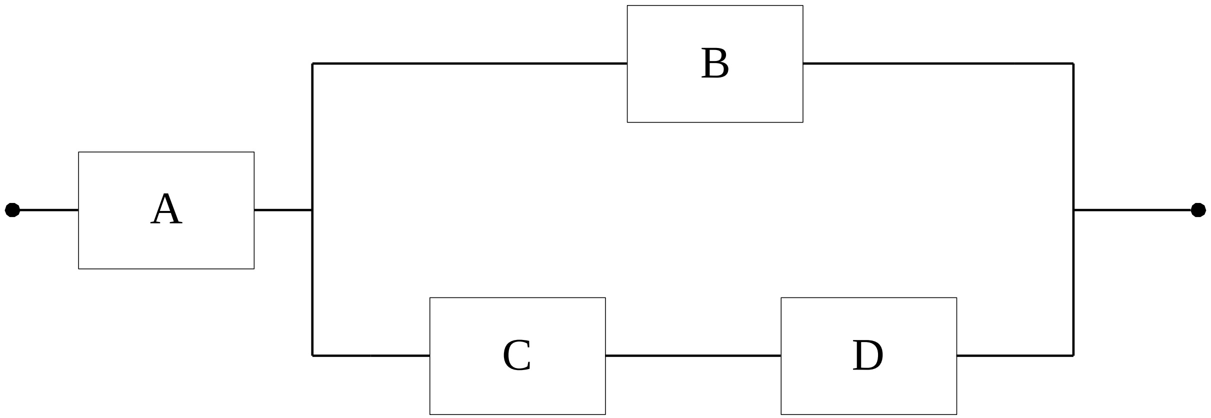


- For A:

	States			
	B	C	D	Critical for A?
1	W	W	W	Y
2	W	W	F	Y
3	W	F	W	Y
4	W	F	F	Y
5	F	W	W	Y
6	F	W	F	N
7	F	F	W	N
8	F	F	F	N

- $I_A = 5/8$

Example Structural Measure of Importance



- $I_A = 5/8$
- $I_B = 3/8$
- $I_C = I_D = 1/8$

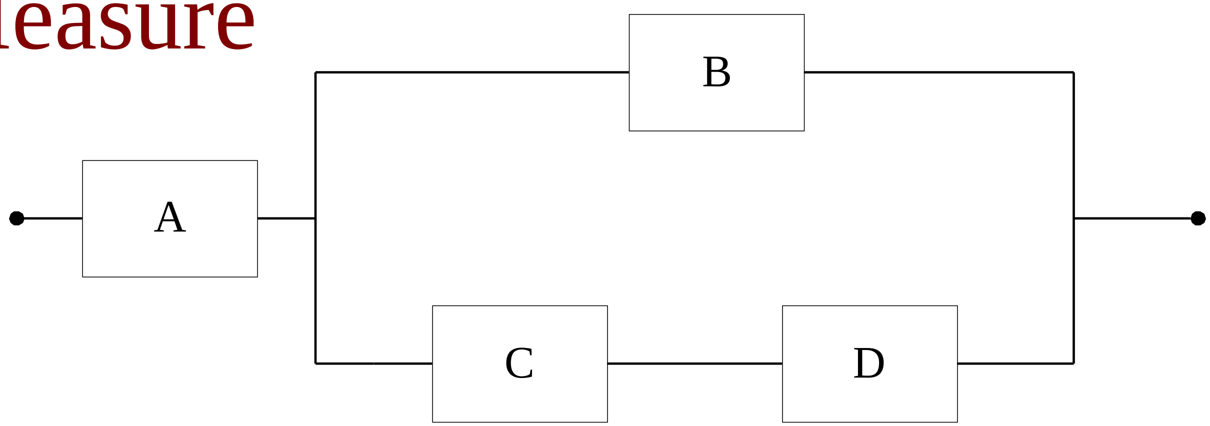
Probabilistic Component Importance Measures (Availability)

- Birnbaum's measure of importance or Criticality Function.
- Fussell - Vesely measure of importance.

Birnbaum's Measure of Importance or Criticality Function

The Criticality Function for a component i, $G_i(q)$ is the probability that the system is in a critical state for component i.

Example – Birnbaum's Importance Measure



$q_A = q_C = 0.1$

$q_B = q_D = 0.2$

$$
\begin{aligned}
G_A &= (1 - q_B)(1 - q_C)(1 - q_D) \\
&+ (1 - q_B)(1 - q_C)q_D \\
&+ (1 - q_B)(q_C)(1 - q_D) \\
&+ (1 - q_B)q_C q_D + q_B(1 - q_C)(1 - q_D) \\
&= (1 - q_B)+q_B(1 - q_C)(1 - q_D)
\end{aligned}
$$

$G_A = 0.944$

	States			
	B	C	D	Critical for A?
1	W	W	W	Y
2	W	W	F	Y
3	W	F	W	Y
4	W	F	F	Y
5	F	W	W	Y
6	F	W	F	N
7	F	F	W	N
8	F	F	F	N

Birnbaum's Measure - Criticality Function

- Not a function of the components own availability.
- Many other Importance measures are based on this measure.
- Tabular approaches are not a practical means to produce this measure. For an 11 component system there would be 11 tables of $2^{10} = 1024$ entries.

Alternative Expressions for Birnbaum's Measure

$G_i(\mathbf{q})$ is the probability that the system fails only if component i fails.

i.e. $G_i(\mathbf{q})$ is the probability the system fails with component i failed minus the probability the system fails with component i working.

i.e. $G_i(q) = Q_{SYS}(1_i, q) - Q_{SYS}(0_i, q)$

$Q_{SYS}(1_i, q) = Q_{SYS}(q_1, q_2, \ldots, q_{i-1}, 1, q_{i+1}, \ldots, q_n)$

$Q_{SYS}(0_i, q) = Q_{SYS}(q_1, q_2, \ldots, q_{i-1}, 0, q_{i+1}, \ldots, q_n)$

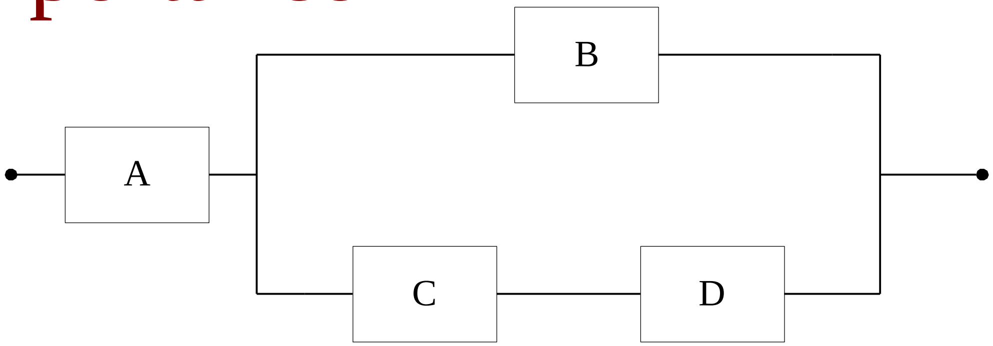
or $$G_i(q) = \frac{\partial Q_{SYS}}{\partial q_i}$$

Fussell - Vesely Measure of Importance

- Probability of the union of all minimal cut sets containing i given that the system has failed.

$$I_{FV_i} = \frac{P\left(\bigcup_{i \in C_j} C_j\right)}{Q_{SYS}}$$

Example Fussell-Vesely Measure of Importance



Min Cut Sets

A

B.C

B.D

$$I_{FV_A} = \frac{q_A}{Q_{SYS}} = \frac{0.1}{0.1504} = 0.6649$$

$$I_{FV_B} = \frac{q_B(q_C + q_D - q_C q_D)}{Q_{SYS}} = \frac{0.2(0.1 + 0.2 - 0.02)}{0.1504} = 0.3723$$

$$I_{FV_C} = \frac{q_C q_B}{Q_{SYS}} = \frac{0.02}{0.1504} = 0.1330$$

$$I_{FV_D} = \frac{q_D q_B}{Q_{SYS}} = \frac{0.04}{0.1504} = 0.2660$$

Importance Measures Summary

Component	**Structural**	**Birnbaum**	**Fussell-Vesely**
A	0.625	0.944	0.6649
B	0.375	0.252	0.3723
C	0.125	0.144	0.1330
D	0.125	0.162	0.2660

System Failure Intensity

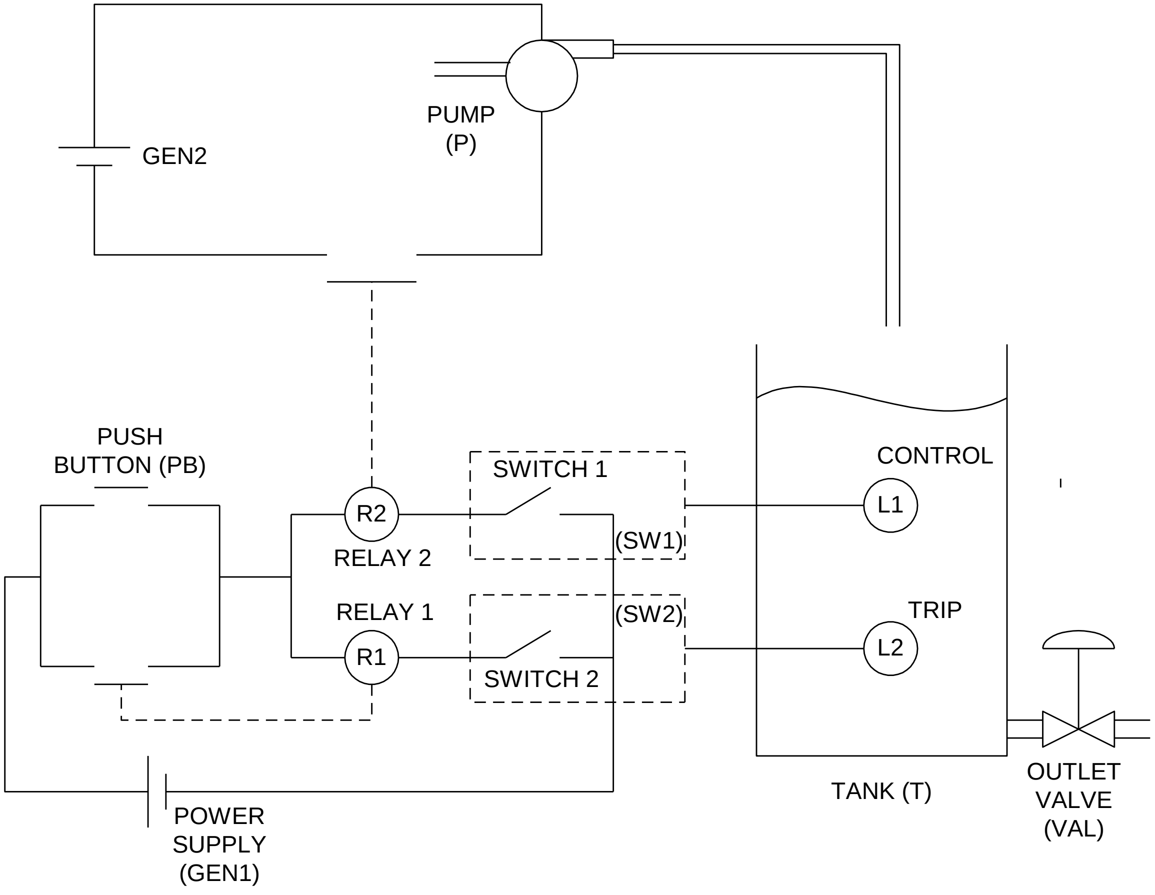
- $w_{SYS}(t)$ is the system failure intensity at time t.
- This can be determined from:

$$w_{SYS}(t) = \sum_{i=1}^{n} G_i(\underline{q}).w_i(t)$$

  - where w_i is the component failure intensity and
  - $G_i(q)$ is the Criticality Function

Case Study

Tank Level Control System



System Failure Mode: Tanks Overfills

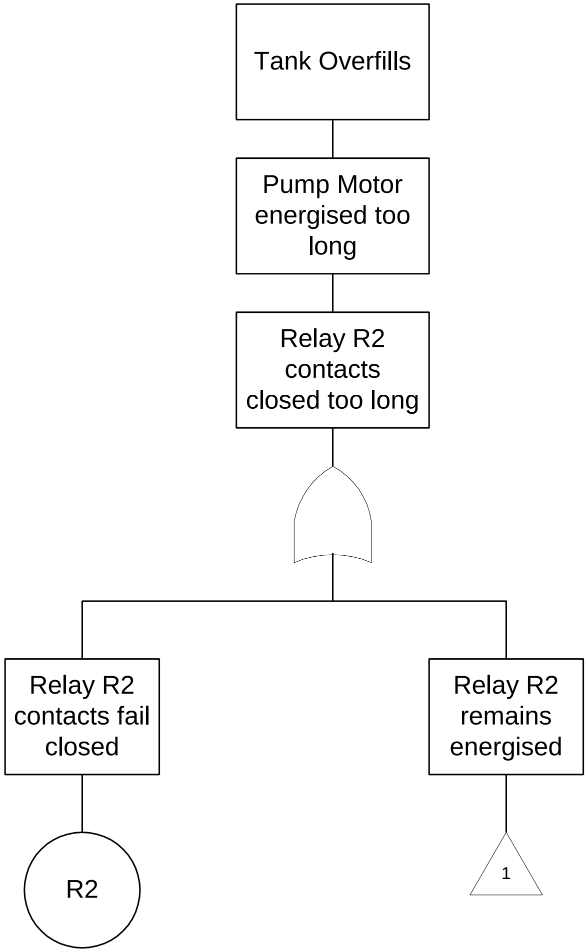
Tank Level Control System Component Failure Modes

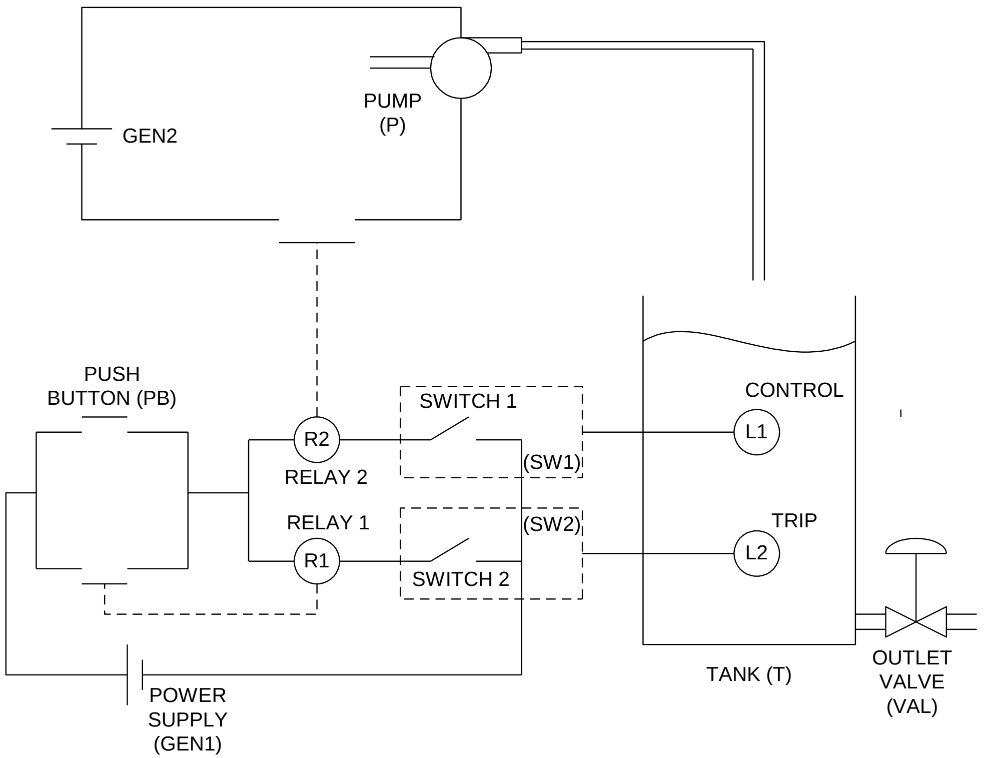
Component	Failure Mode	Code	Failure Rate (per hour)	Mean Time to Repair (hours)
Push Button	Stuck closed	PB	$5. \times 10^{-5}$	2.
Relay Contacts	Stuck closed	R1/R2	$6. \times 10^{-5}$	10.
Switch	Stuck closed	SW1/SW2	$5. \times 10^{-5}$	10.
Level Sensors	Fail to indicate high level	L1/L2	$2. \times 10^{-6}$	5.

Unrevealed failures R1/PB/SW2/L2 –

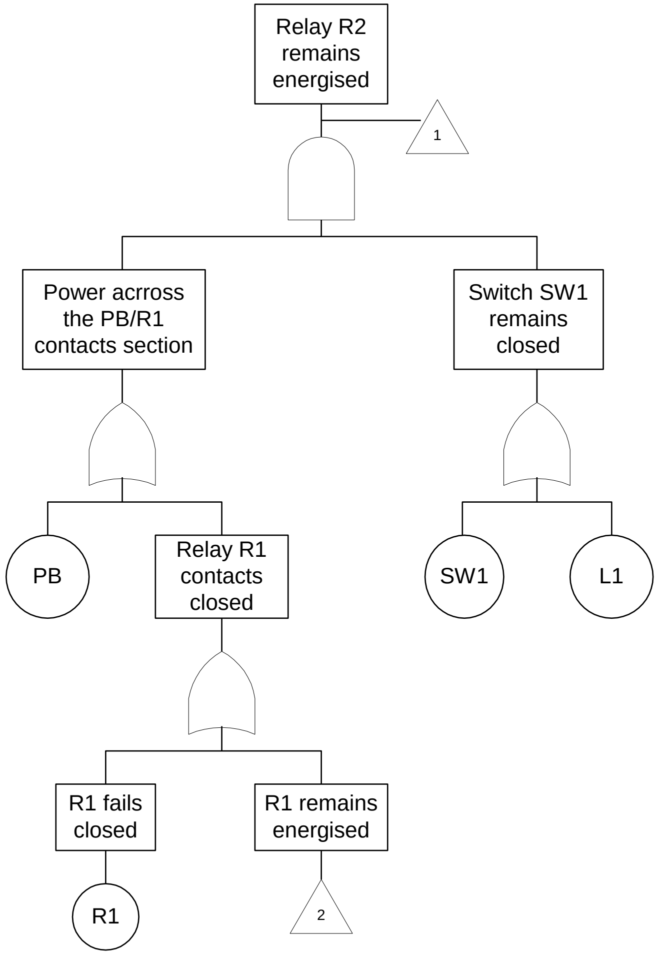
inspection interval = 4380 hours

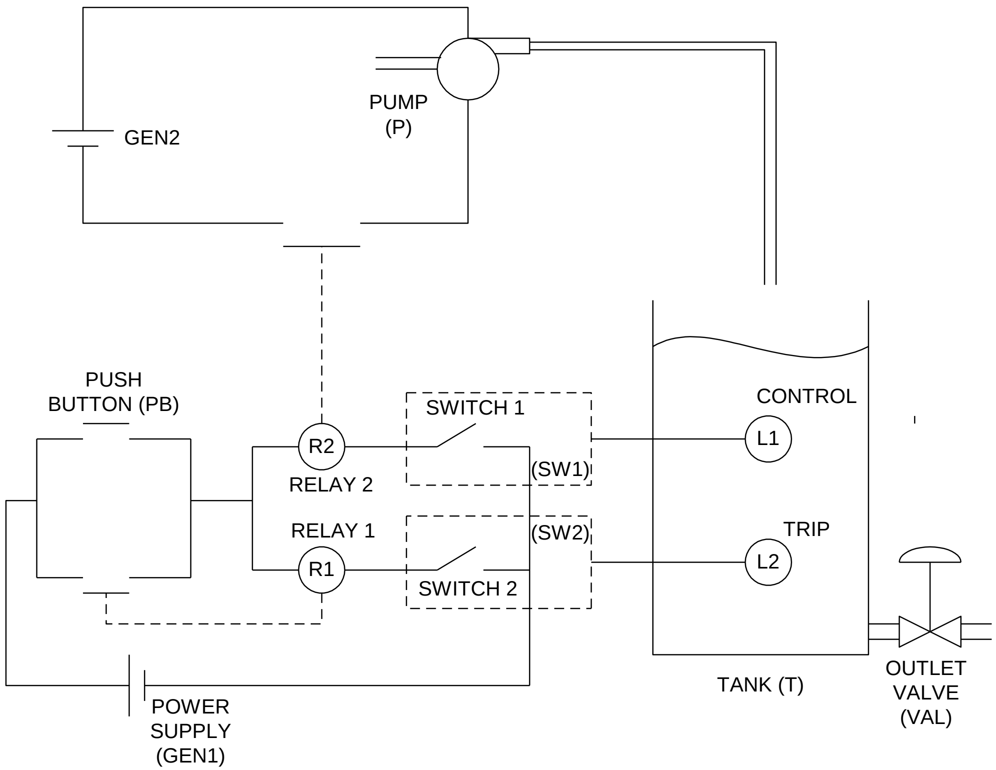
Tank Level Control System – FT(1)



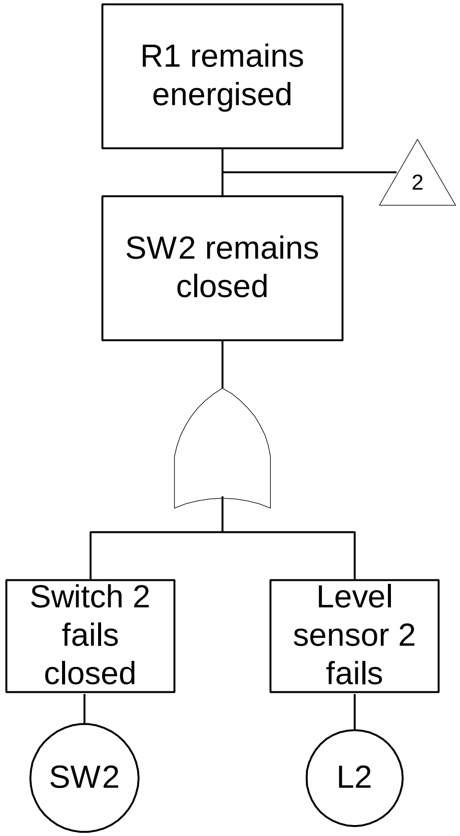


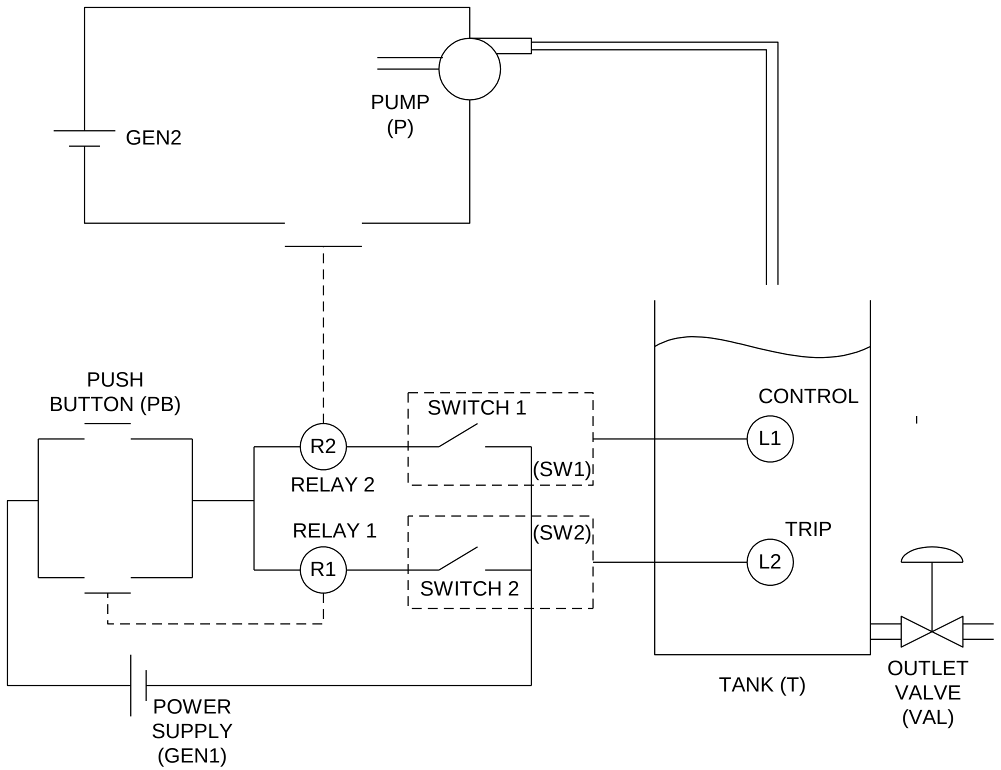
Tank Level Control System – FT(2)



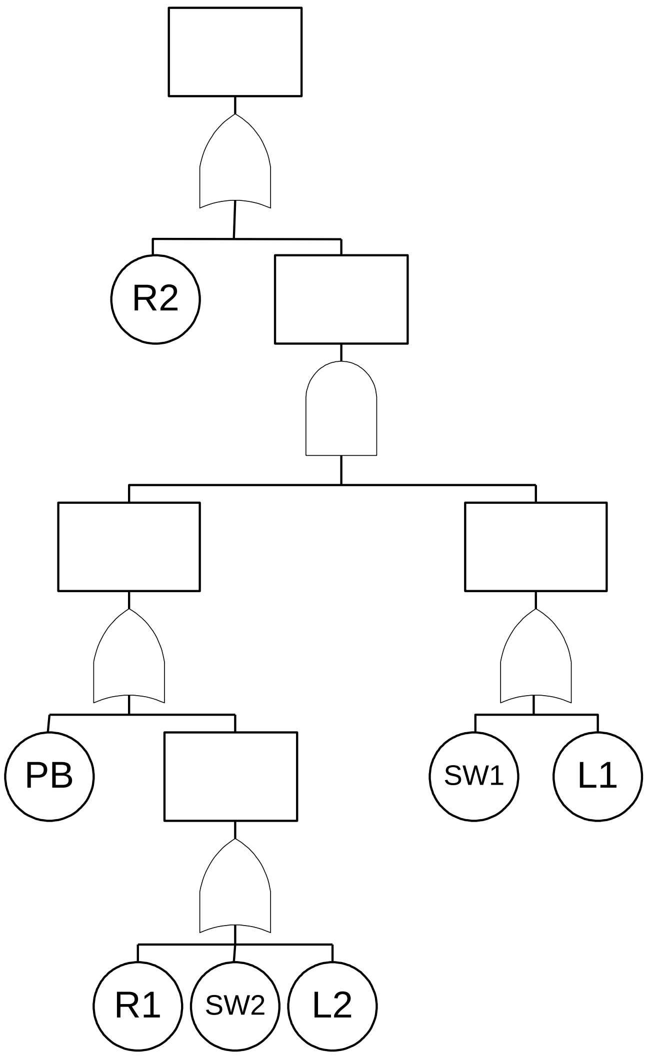


Tank Level Control System – FT(2)





Tank Level Control System - MCS



Minimal Cut Sets

1	R2	
2	SW1	PB
3	SW1	R1
4	SW1	SW2
5	SW1	L2
6	L1	PB
7	L1	R1
8	L1	SW2
9	L1	R1

Tank Level Control System

Top Event Probability = 7.5 x 10^{-4}

Top Event Frequency = 7.72 x 10^{-5} per hour

Rank	***Component***	***Fussell Vesely***
1	R2	0.781
2	SW1	0.215
3	R1	0.080
4	SW2	0.068
5	PB	0.067
6	L1	0.004
7	L2	0.003

Summary – Fault Tree Analysis Features

Fault Tree Analysis

- Provides a well structured development of the system failure logic.
- Forms a documented record of analysis which can be used to communicate fault development with regulators etc.
- Directly developed from the engineering system structure.
- Easily interpreted from the engineering viewpoint.
- Analysis gives all minimal cut sets.
- Quantification gives the top system failure mode probability or frequency.
- Vulnerability to system failure can be identified using importance measures.

The End

Any Questions?

Professor John Andrews
Faculty of Engineering
University of Nottingham
Nottingham, NG7 2RD
England

Email: john.andrews@nottingham.ac.uk

Dr Sally Lunt
Faculty of Engineering
University of Nottingham
Nottingham, NG7 2RD
England

Email: sally.lunt@nottingham.ac.uk