

Tutorial

Fault Tree Analysis



Dr John Andrews

Department of Mathematical Sciences

Loughborough University

Loughborough

LE11 3TU, UK

Tel: +44 (0)1509 222862

Fax: +44 (0)1509 223969

E-mail: J.D.Andrews@lboro.ac.uk

Contents

♋ Session 1: Basic Concepts

- Fault Tree Symbols/Terminology
- Fault Tree Construction
- Minimal Cut Sets
- Component Failure Models
- Top Event Probability
- Top Event Frequency
- Other Top Event Parameters
- Importance Measures

⌘ Session 2: Advanced Features

- Initiator/Enabler Events
- Non-Coherent Fault Trees

⌘ Session 3: Current Research

- Binary Decision Diagrams
- Dependency Modelling
- Optimal System Design

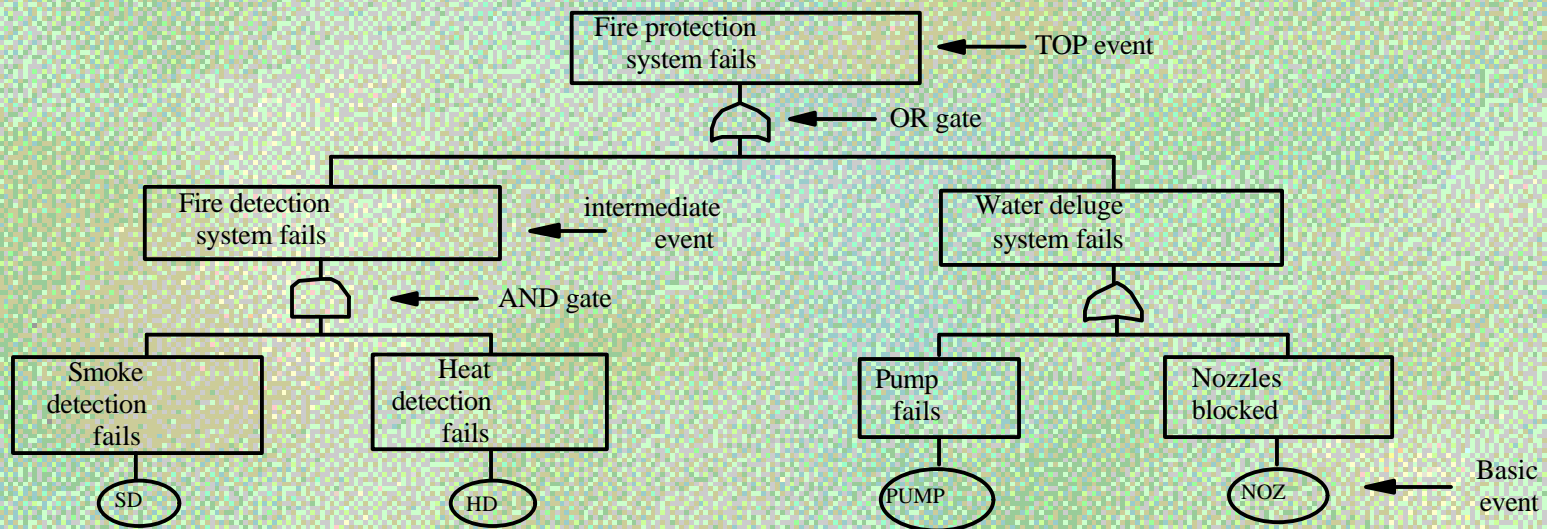
Session 1: Basic Concepts



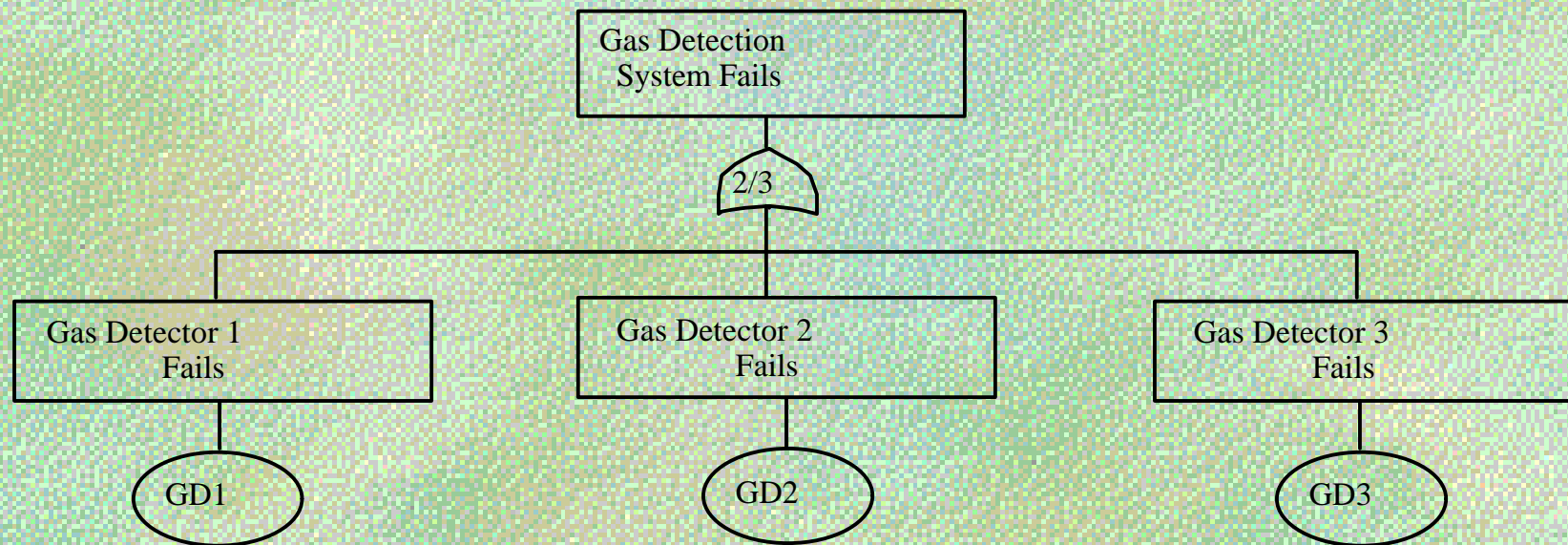
History

- ⌘ 1961 - FTA Concept by H Watson, Bell Telephone Laboratories
- ⌘ 1970 - Vesely - Kinetic Tree Theory
- ⌘ Importance measures - Birnbaum, Esary, Proschan, Fussel, Vesely
- ⌘ Initiator/Enabler Theory - Lambert and Dunglinson
- ⌘ FTA on PCs with GUI's
- ⌘ Automatic Fault Tree Construction
- ⌘ Binary Decision Diagrams

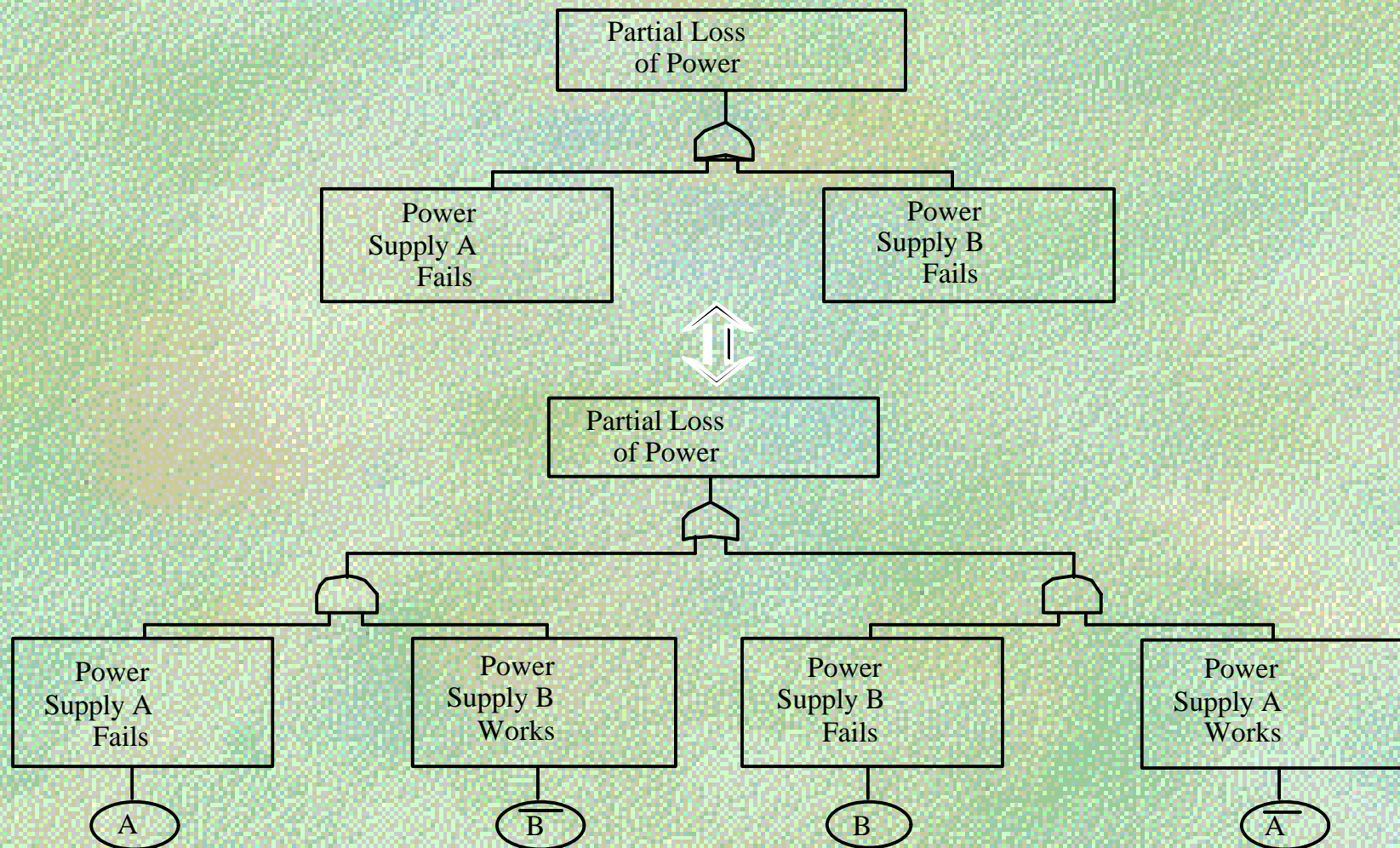
Fault Tree Example



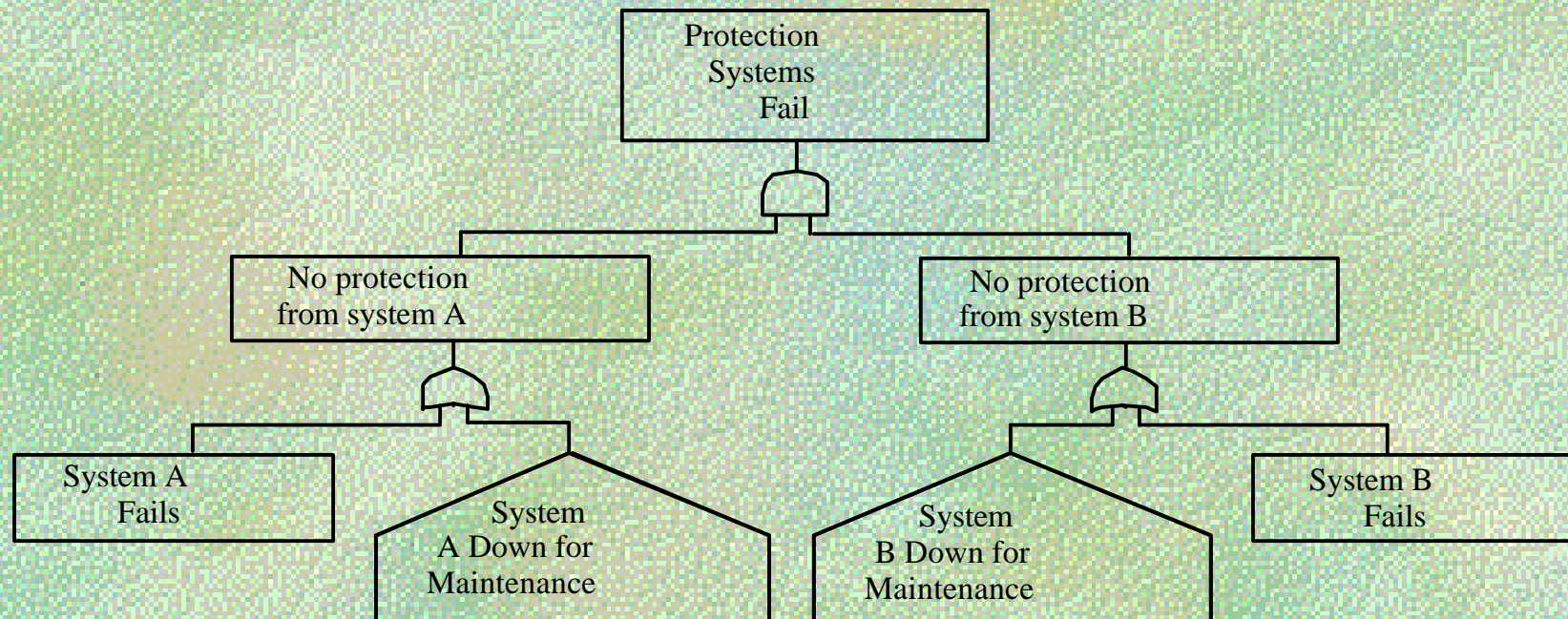
Voting Gates k/n



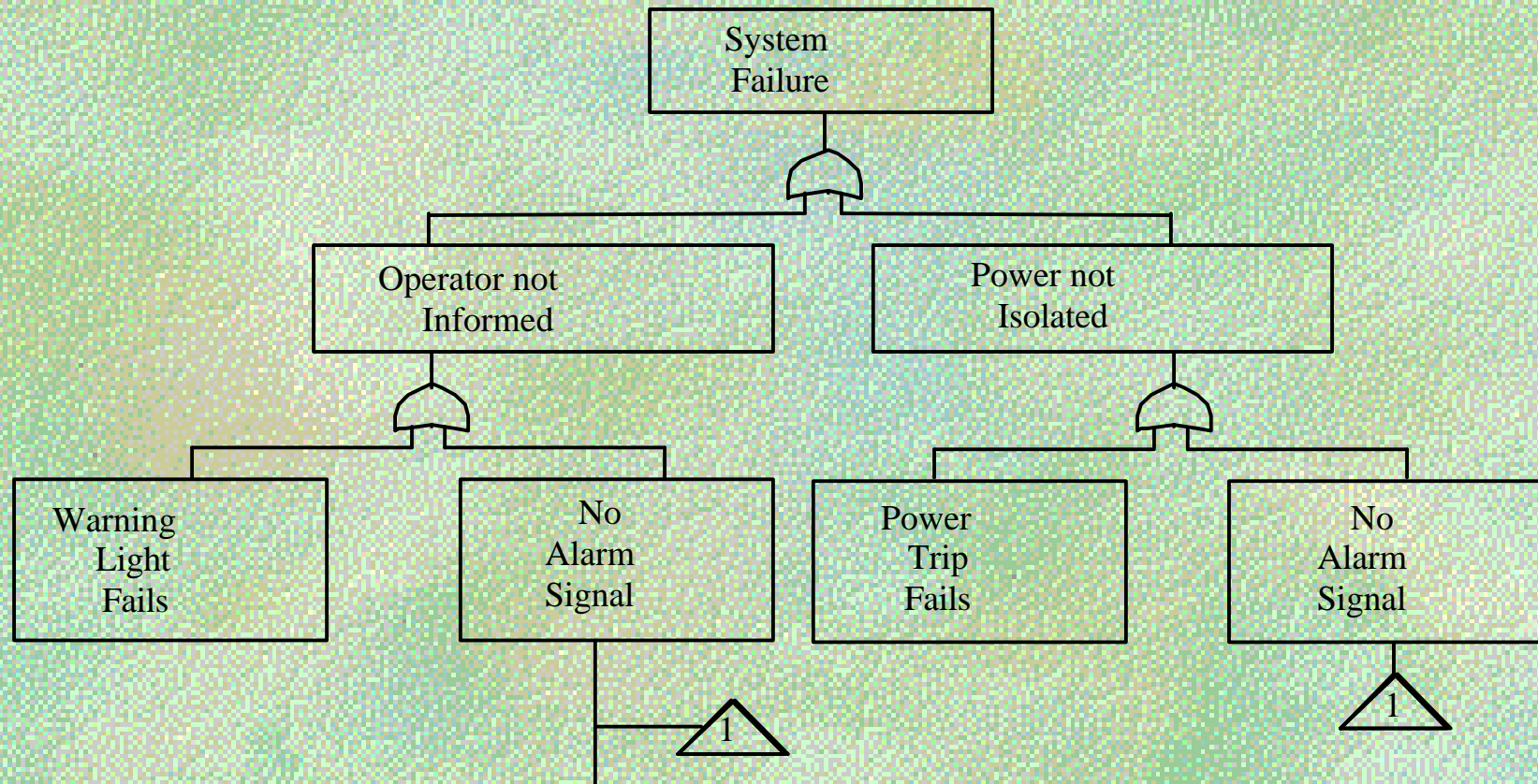
Exclusive OR Gate



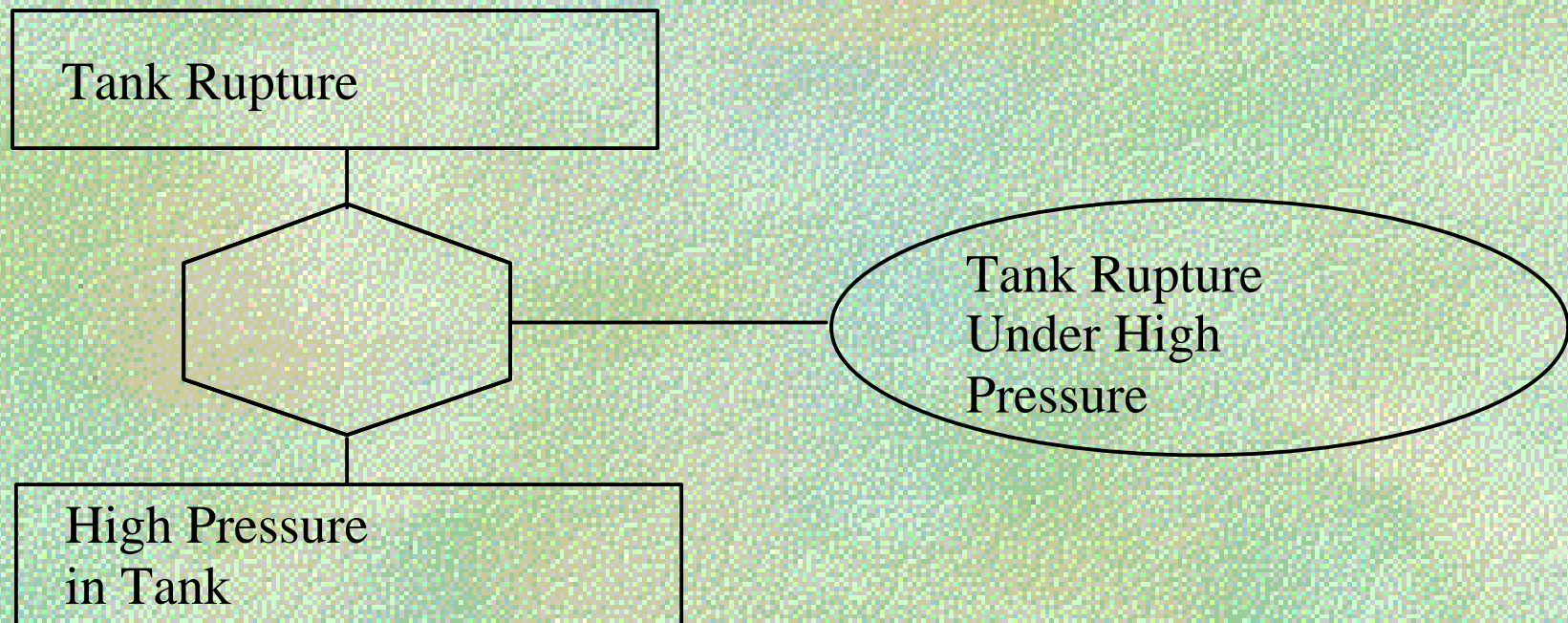
House Events



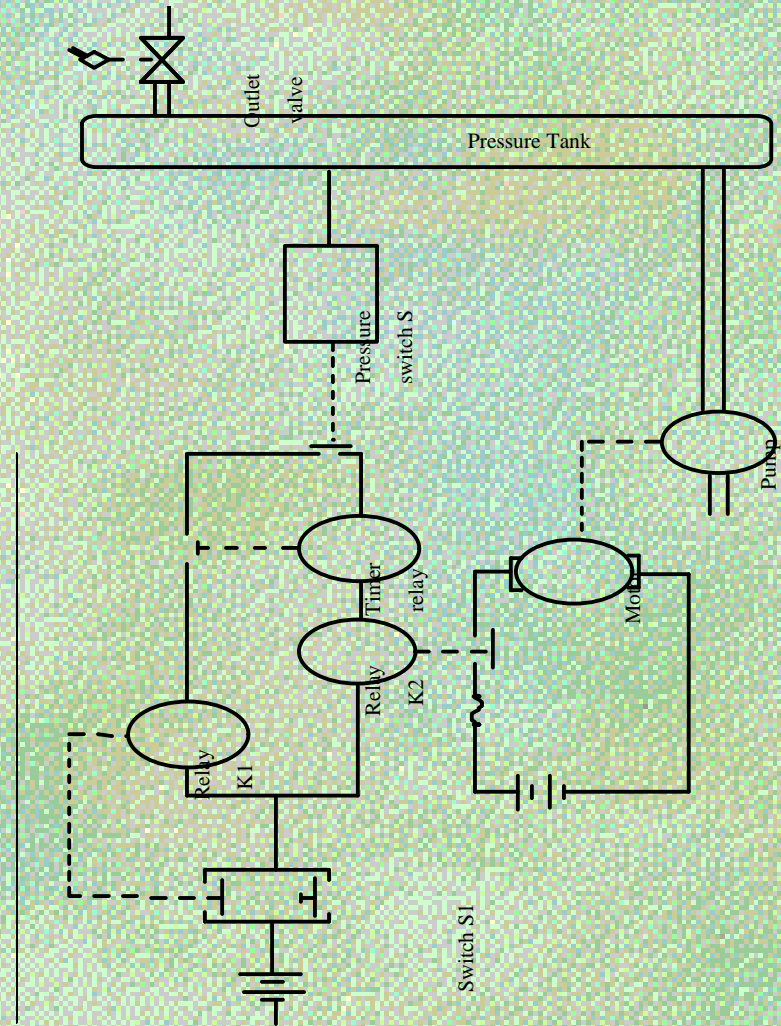
Transfer IN/OUT



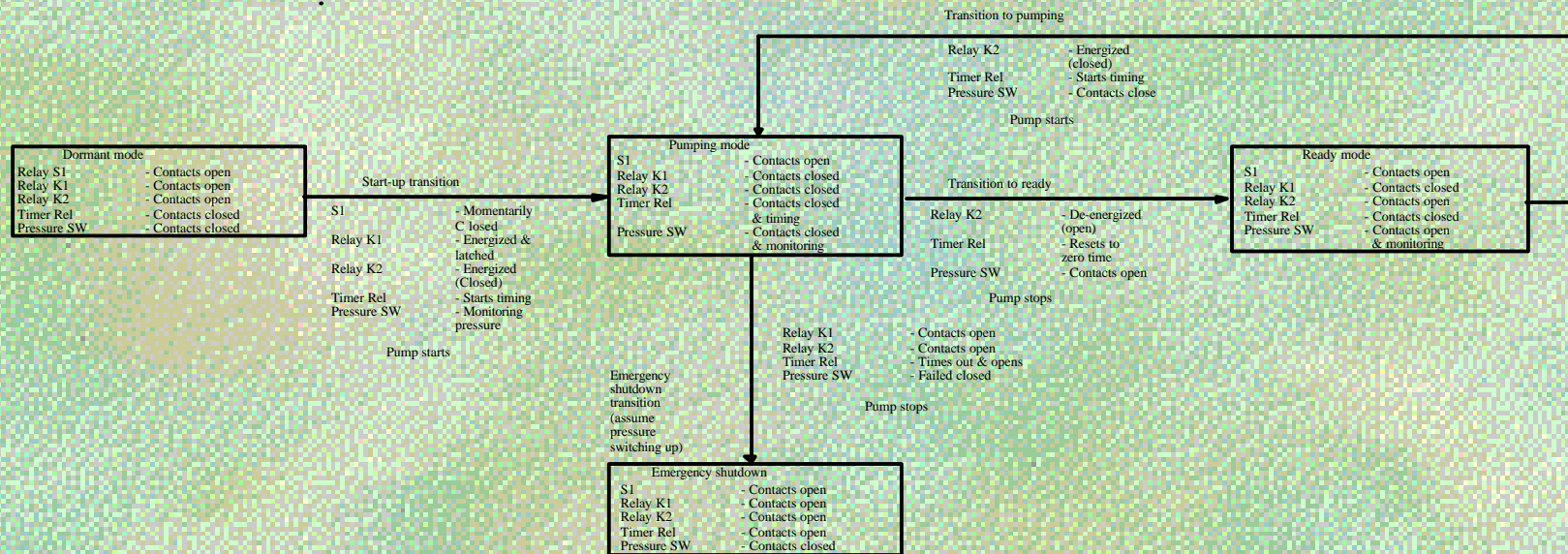
Inhibit Gate

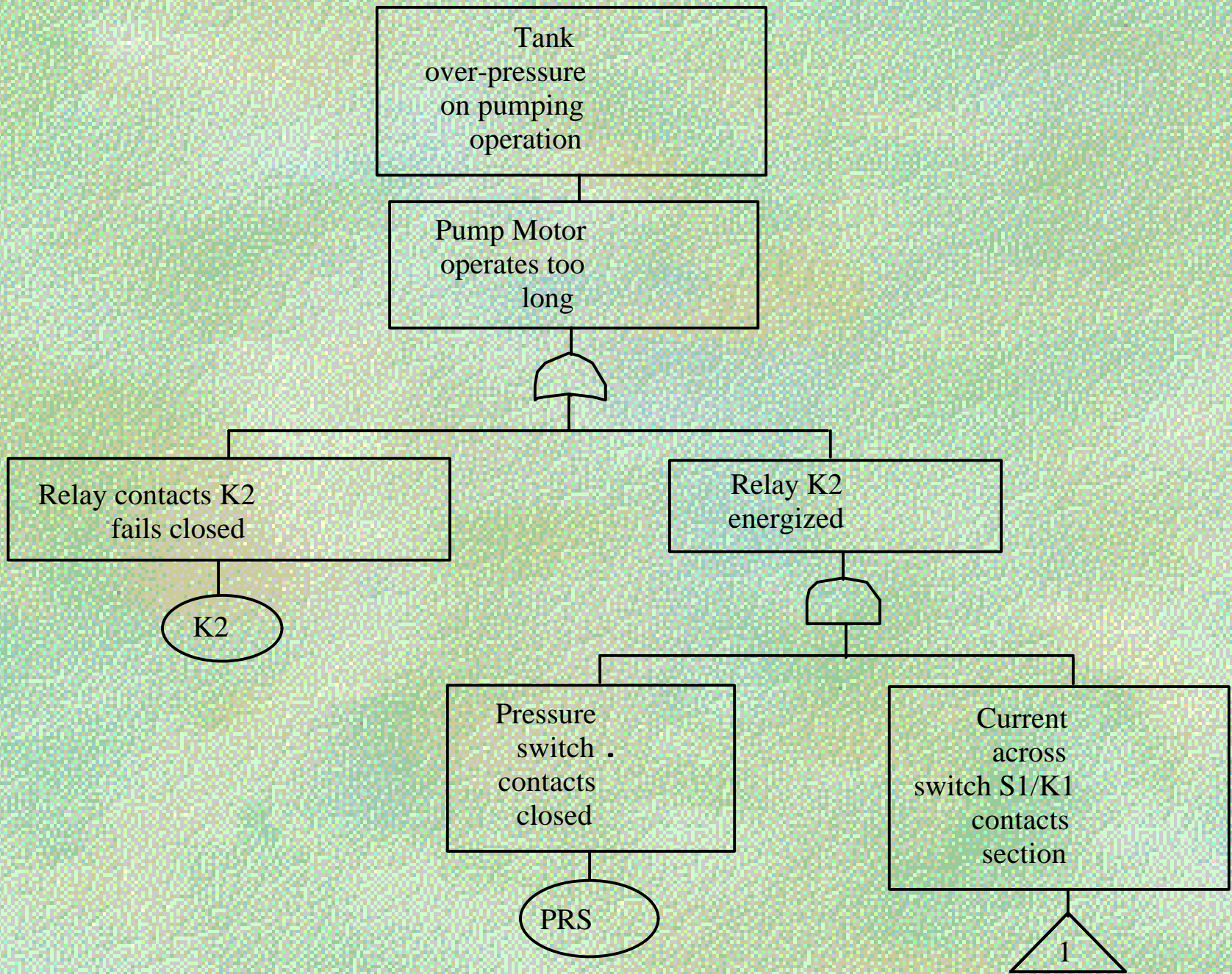


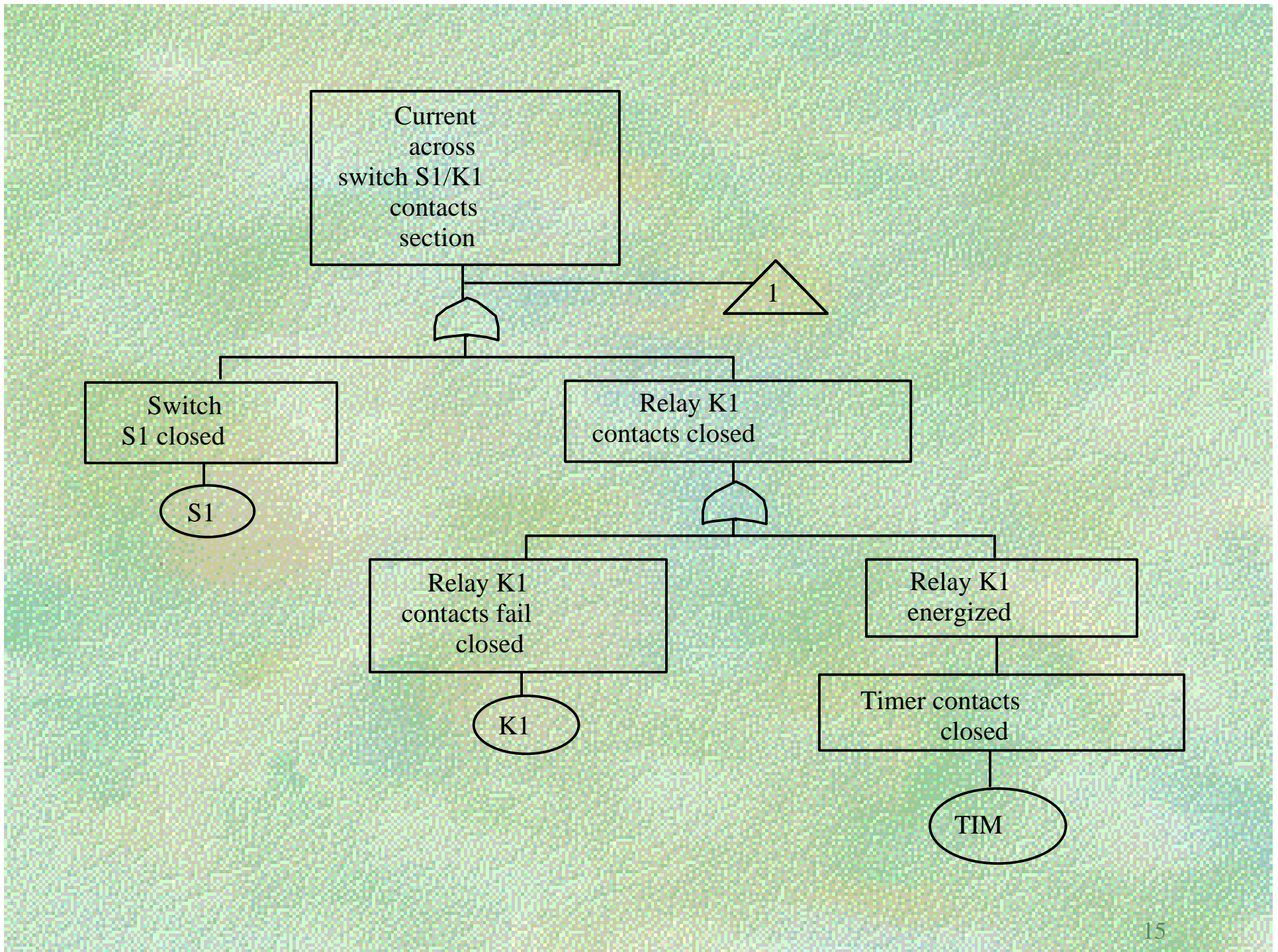
Pressure Tank Example



Circuit Actions







Minimal Cut Sets

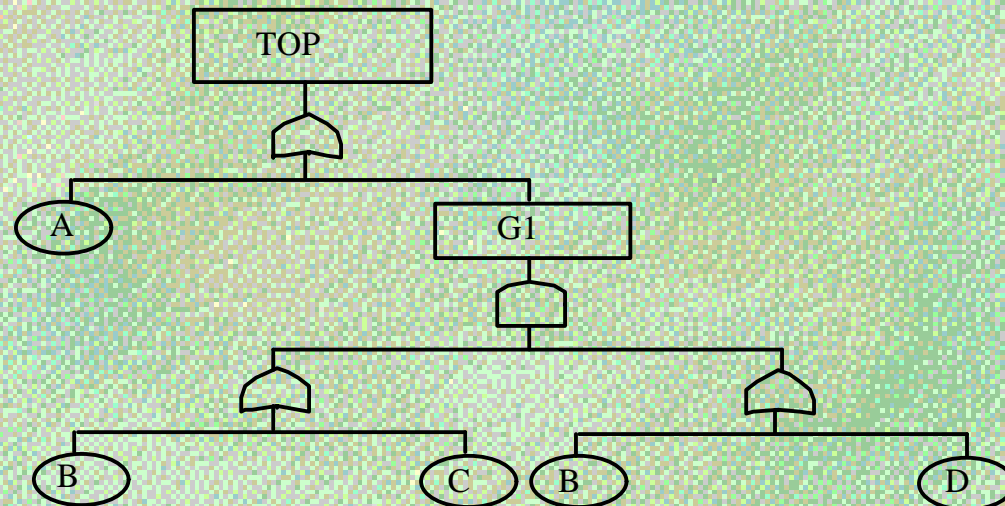
☞ Cut sets

- A list of failure events such that if they occur then so does the top event.

☞ Minimal Cut Sets

- A list of minimal, necessary and sufficient conditions for the occurrence of the top event.

☞ Example



List of possible failure combinations

	System State
A	F
B	F
C	W
D	W
AB	F
AC	F
AD	F
BC	F
BD	F
CD	F
ABC	F
ABD	F
ACD	F
BCD	F
ABCD	F

Minimal Cut Sets

A
B
CD

We want a way to produce the minimal cut sets from the fault tree structure then:

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

Qualitative Fault Tree Analysis

- ⌘ Need to identify the min cut sets whose occurrence is most likely.
- ⌘ Minimal Cut Set expression for the top event.

$$\mathbf{T} = \mathbf{C}_1 + \mathbf{C}_2 + \mathbf{C}_3 + \dots + \mathbf{C}_N$$

$$\mathbf{C}_I, \quad I = 1, \dots, N$$

e.g. $T = A + BC + CD$ are the minimal cut sets

3 minimal Cut Sets

1 first order

2 second order

Laws of Boolean Algebra

- AND
- + OR

Distributive

$$(A + B) \cdot (C + D) = A \cdot C + A \cdot D + B \cdot C + B \cdot D$$

Idempotent

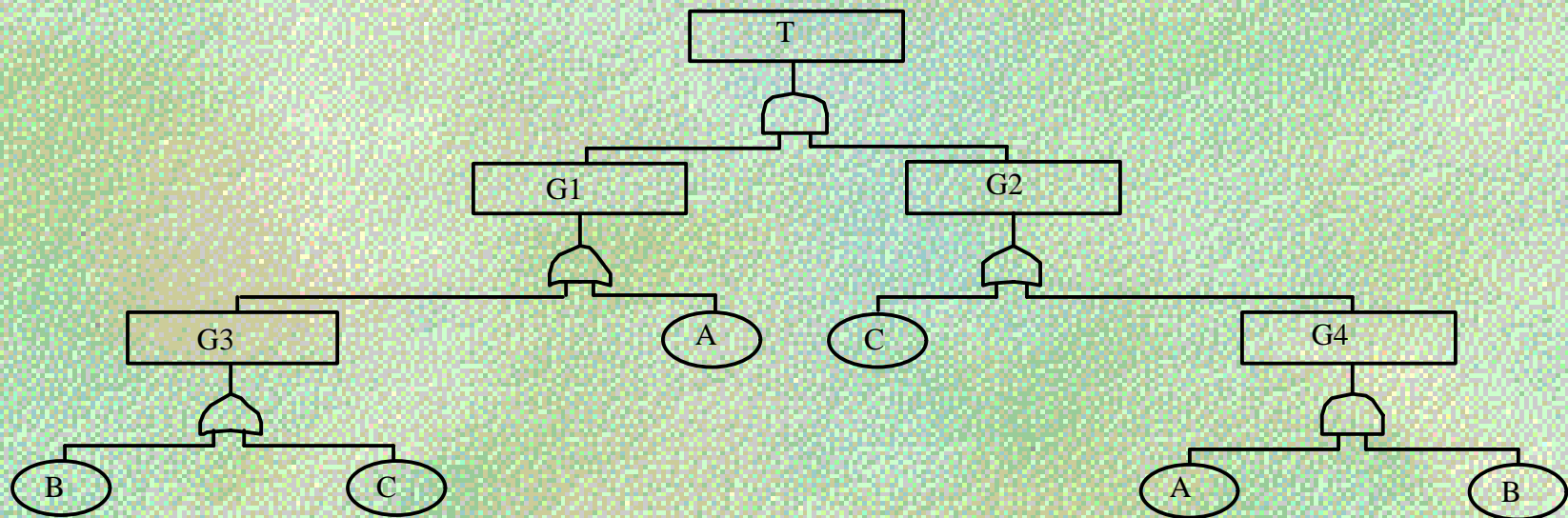
$$A + A = A$$

$$A \cdot A = A$$

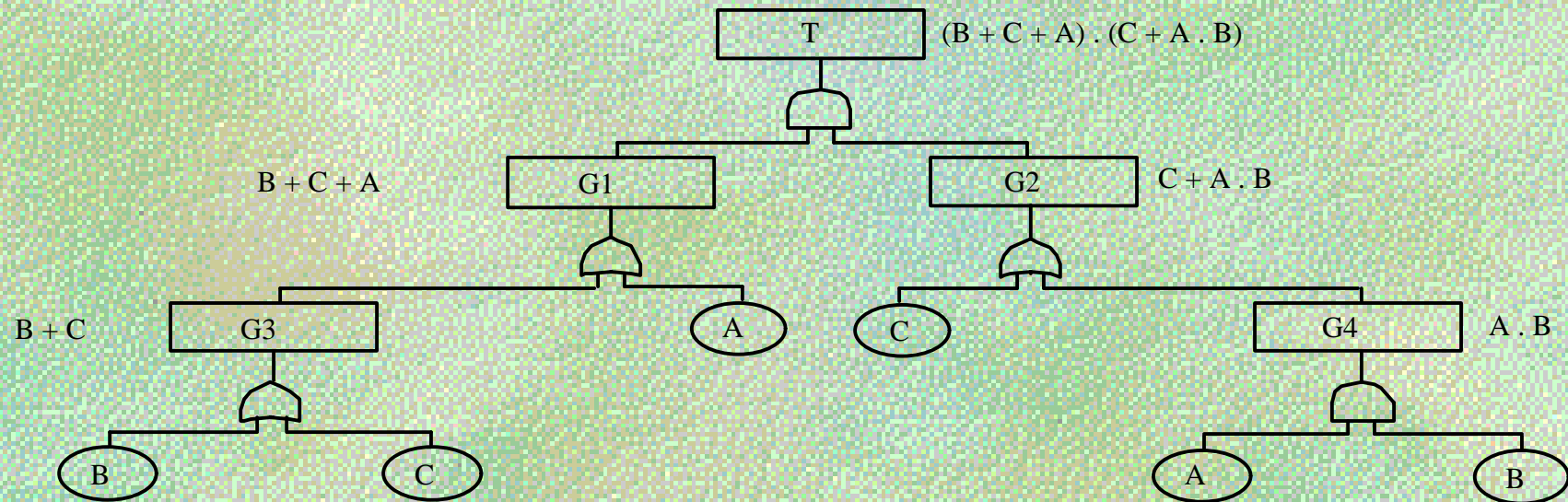
Absorption

$$A + A \cdot B = A$$

Example



Bottom-up method



$$\begin{aligned} \text{TOP} &= (B + C + A) \cdot (C + A \cdot B) \\ &= B \cdot C + B \cdot A \cdot B + C \cdot C + C \cdot A \cdot B \\ &\quad + A \cdot C + A \cdot A \cdot B \end{aligned}$$

$$(A \cdot A = A)$$

$$\begin{aligned} &= B \cdot C + A \cdot B + C + C \cdot A \cdot B \\ &\quad + A \cdot C + A \cdot B \end{aligned}$$

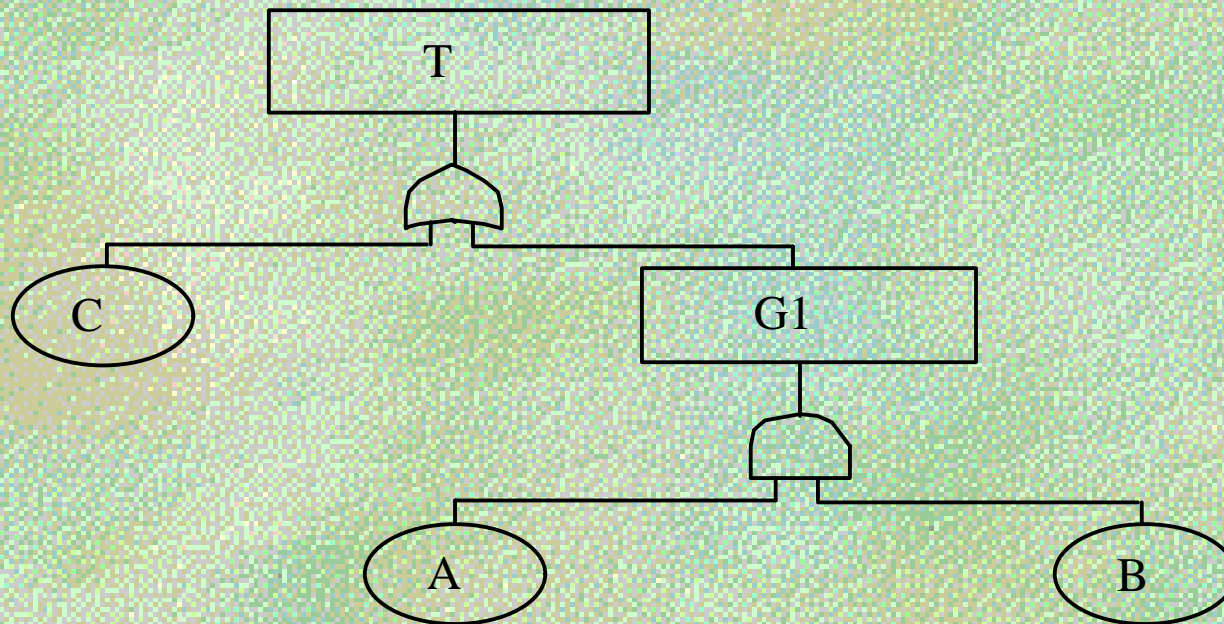
$$(A + A = A)$$

$$\text{TOP} = B \cdot C + A \cdot B + C + C \cdot A \cdot B + A \cdot C$$

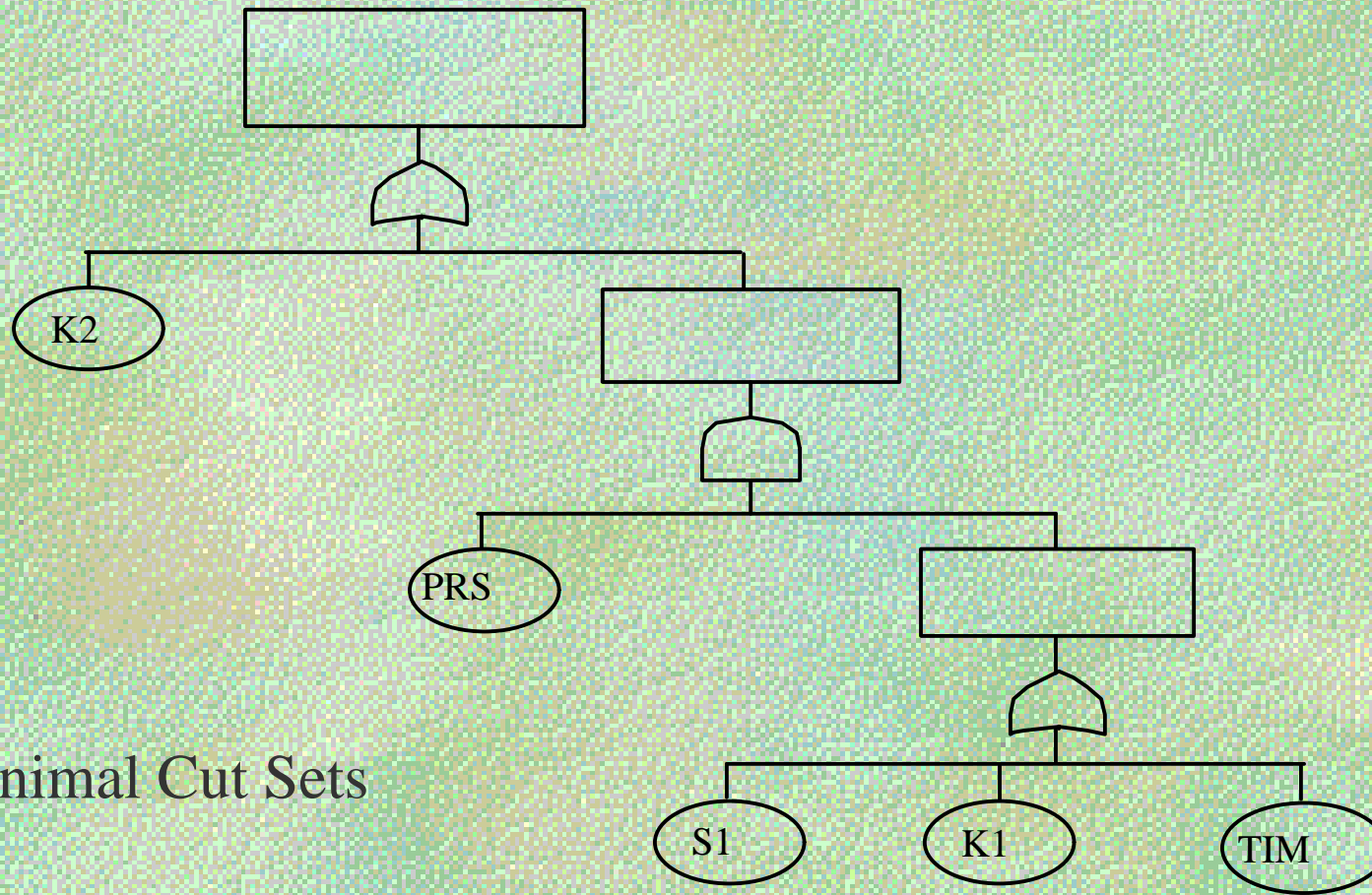
$$(A + A \cdot B = A)$$

$$\text{TOP} = A \cdot B + C$$

The tree could have been drawn:



Pump System Example



Minimal Cut Sets

K2

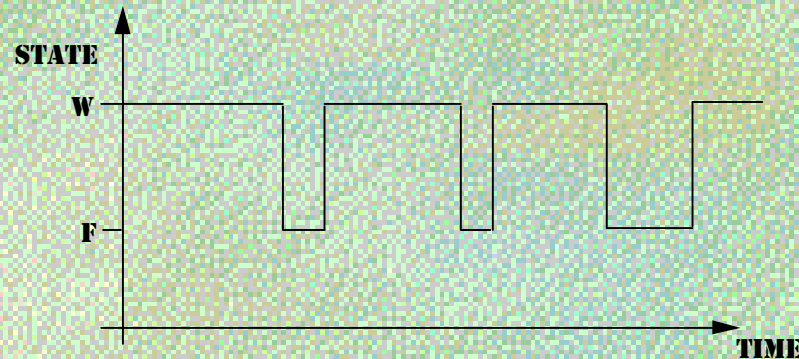
PRS S1

PRS K1

PRS TIM

Component Performance Characteristics

Typical History of a Repairable Component



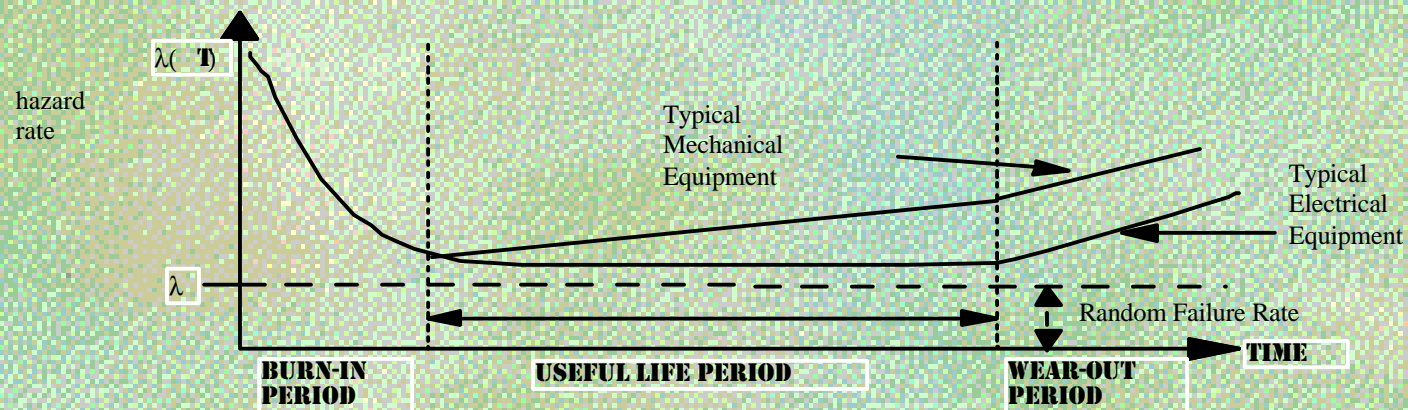
Downtime Depends on

- Failure detection time
- Availability of Maintenance team
- **REPAIR TIME** { **OBTAIN REPLACEMENT**
INSTALLATION
- System Test Time

Performance indicators

- Rate at which failures occur
- Measure of expected up-time

The Failure Process



For useful life period

Unreliability

$$\mathbf{F}(\mathbf{T}) = \mathbf{1} - \mathbf{E}^{-\lambda \mathbf{T}}$$

(Density Function)

$$\mathbf{F}(\mathbf{T}) = \lambda \mathbf{E}^{-\lambda \mathbf{T}}$$

Reliability

$$\begin{aligned} \mathbf{R}(\mathbf{T}) &= \mathbf{1} - \mathbf{F}(\mathbf{T}) \\ &= \mathbf{E}^{-\lambda \mathbf{T}} \\ &= \frac{\mathbf{1}}{\lambda} \end{aligned}$$

Mean Time to Failure

$\lambda(\mathbf{T}) =$ Conditional failure rate (hazard rate)

Probability that a component fails in
(t, t + dt) given that it was working at t

Maintenance Policies

1. No Repair

Q (T) - UNAVAILABILITY

F (T) - UNRELIABILITY

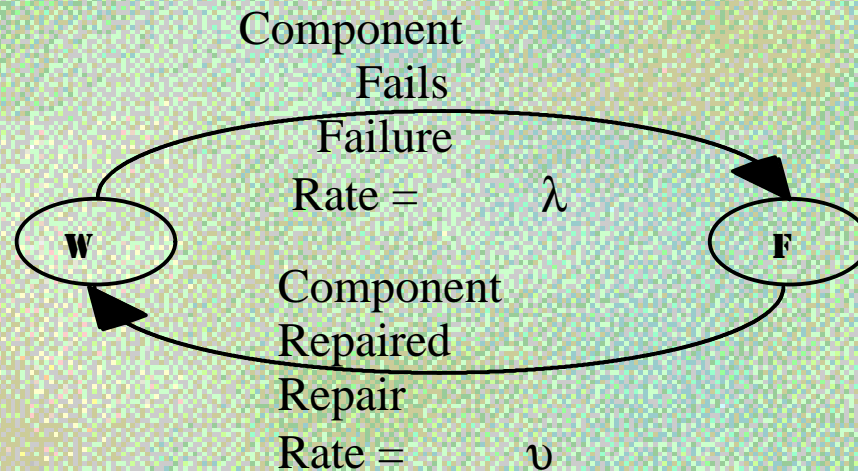
$$\mathbf{F (T) = 1 - E^{-\lambda T}}$$

$$\mathbf{Q (T) = F (T)}$$



Repairable Components

Failure/Repair Process



1. Only one transition can occur in a small period of time Δt .
2. Change between states is instantaneous.
3. Following repair components are as good as new.

2. Revealed Failures - unscheduled maintenance

λ - **FAILURE RATE**

ν - **REPAIR RATE**

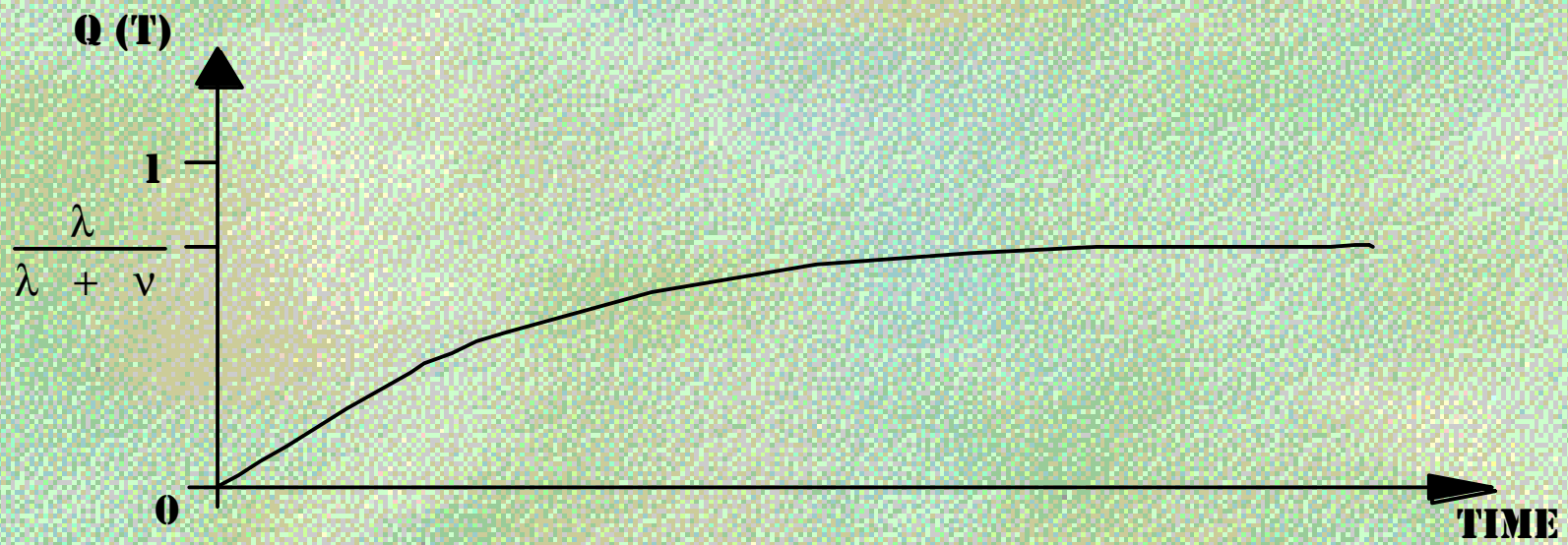
μ - **MEAN TIME TO FA**

τ - **MEAN TIME TO RE**

Q(T) - UNAVAILABILITY

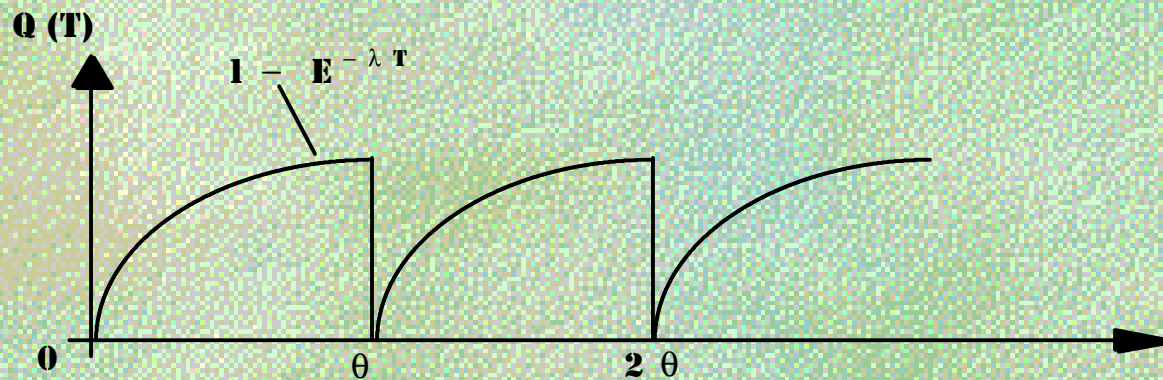
$$Q(T) = \frac{\lambda}{\lambda + \nu} (1 - E^{-(\lambda + \nu)T})$$

AT STEADY STATE $\frac{\lambda}{\lambda + \nu} = \frac{\tau}{\mu + \tau} \approx \lambda\tau$



3. Unrevealed or Dormant Failures - Scheduled Maintenance

θ - **TIME BETWEEN INSPECTIONS**



$$Q \approx \lambda \tau$$

(for revealed failures)

Mean time to restore

$$= \text{MEAN DETECTION TIME} + \text{MEAN TIME TO REPAIR}$$

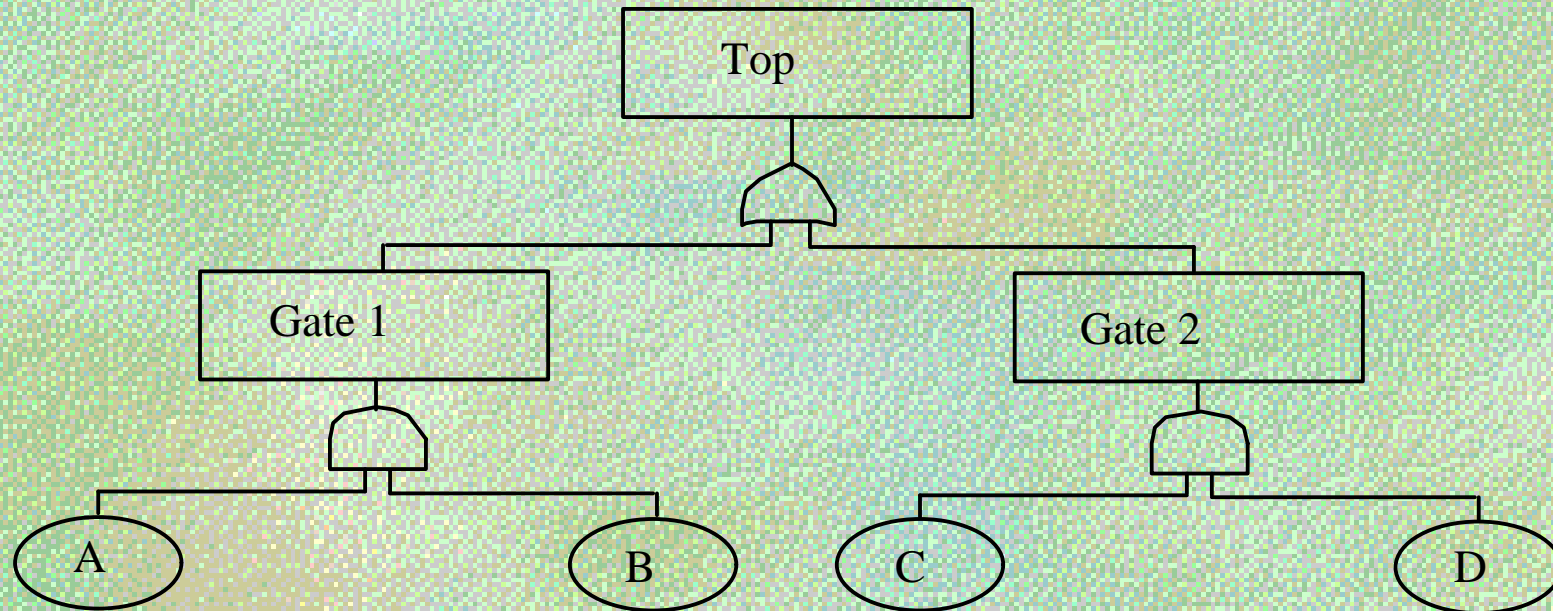
$$= \frac{\theta}{2} + \tau$$

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

IN GENERAL $\tau \gg \frac{\theta}{2}$ $Q_{AV} \approx \lambda \tau$

[MORE ACCURATE ALTERNATIVE] $Q_{AV} = \frac{\lambda \theta (1 - e^{-\lambda \theta})}{2}$

Top Event Probability

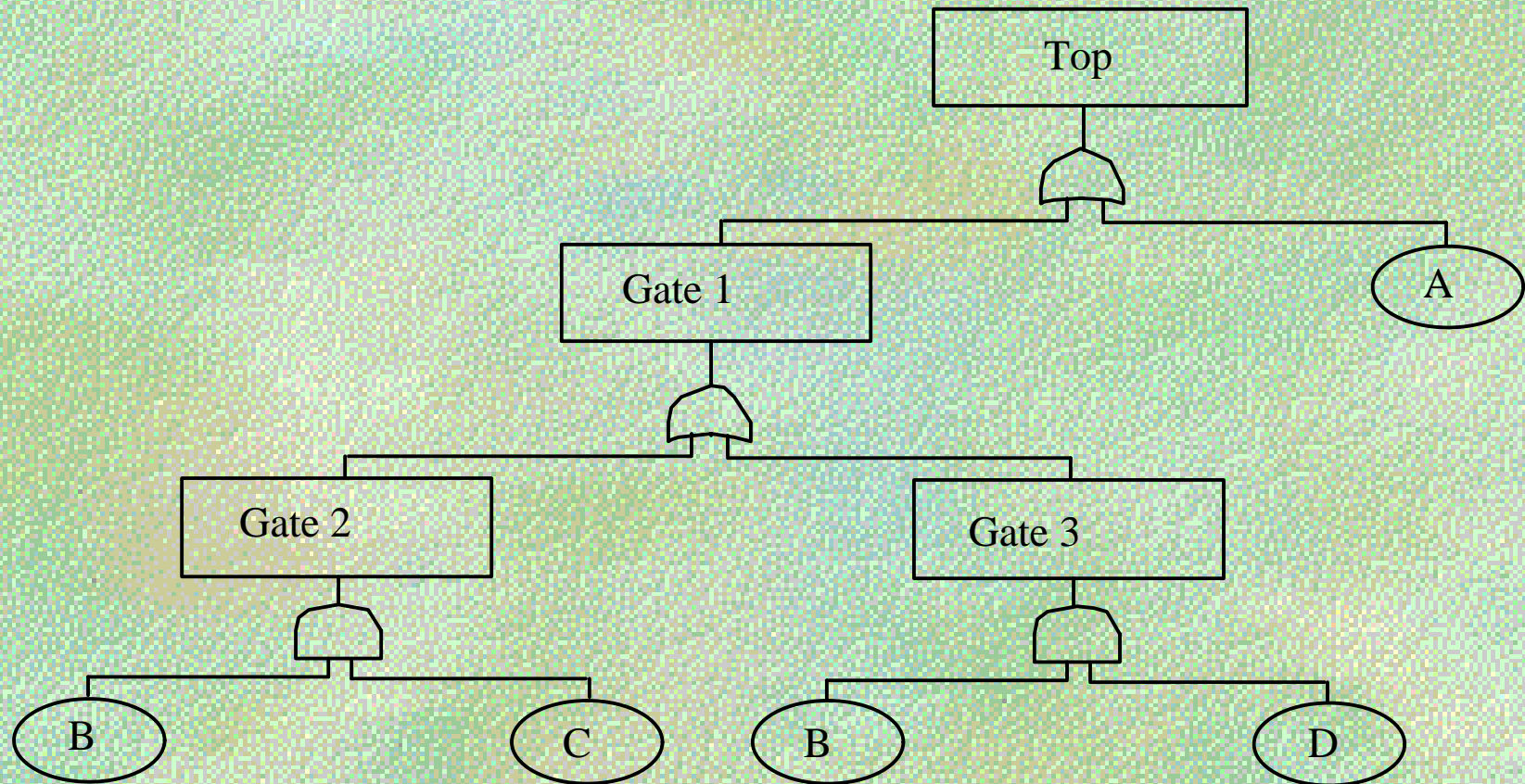


All basic event independent with prob 0.1

$$P(\text{Gate 1}) = P(A) \cdot P(B) = 0.01$$

$$P(\text{Gate 2}) = P(C) \cdot P(D) = 0.01$$

$$\begin{aligned} \text{And } P(\text{TOP}) &= P(\text{Gate 1 OR Gate 2}) \\ &= P(\text{Gate 1}) + P(\text{Gate 2}) - \\ &\quad P(\text{Gate 1}) \cdot P(\text{Gate 2}) \\ &= 0.01 + 0.01 - 0.0001 \\ &= 0.199 \end{aligned}$$



all basic events are independent and

$$Q_A = Q_B = Q_C = Q_D = 0.1$$

The minimal cut sets of the fault tree are:

A

B C

B D

$$\mathbf{T = A + BC + BD}$$

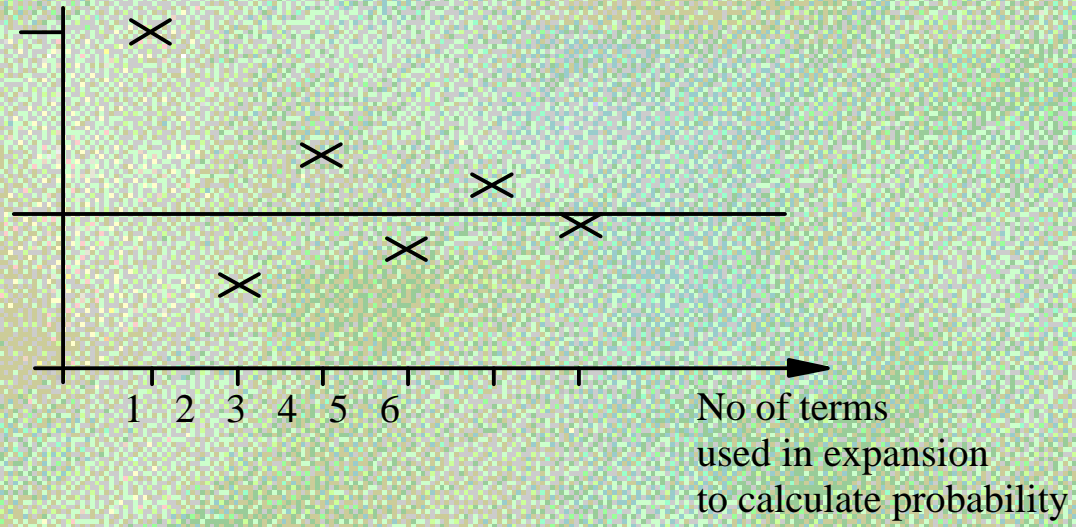
$$\mathbf{Q_S(T) = P(T) = P(A + BC + BD)}$$

Using three terms of the inclusion-exclusion expansion gives:

$$\begin{aligned}
 &= \underbrace{[P(A) + P(BC) + P(BD)]}_{\text{1ST TERM}} \\
 &\quad - \underbrace{[P(ABC) + P(ABD) + P(BCD)]}_{\text{2ND TERM}} \\
 &\quad\quad + \underbrace{[P(ABCD)]}_{\text{3RD TERM}} \\
 &= [0.1 + 0.01 + 0.0] - [0.001 + 0.001 + 0.00] + [0.000] \\
 &= [0.12] - [0.003] + [0.000] \\
 &= \mathbf{0.1171}
 \end{aligned}$$

Probability value

$Q(t)$
Exact
Probability



Convergence of Inclusion-Exclusion Expansion

$$\begin{aligned}
 P(T) = & \sum_{I=1}^{N_c} P(C_I) - \sum_{I=2}^{N_c} \sum_{J=1}^{I-1} P(C_I \cap C_J) + \\
 & + \dots + (-1)^{N_c-1} P(C_1 \cap C_2 \cap \dots \cap C_{N_c})
 \end{aligned}$$

$$\mathbf{Q_{RARE EVENT}} = \sum_{I=1}^{N_c} P(C_I)$$

$$\mathbf{Q_{LOWER}} = \sum_{I=1}^{N_c} P(C_I) - \sum_{I=2}^{N_c} \sum_{J=1}^{I-1} P(C_I \cap C_J)$$

N_c – NO OF MIN CUT SETS

$$\begin{aligned} \mathbf{Q_{EXACT}} &= \mathbf{0.1171} \\ \mathbf{Q_{RARE\ EVENT}} &= \mathbf{0.12} \\ \mathbf{Q_{LOWER}} &= \mathbf{0.117} \end{aligned}$$

Minimal Cut Set Upper Bound

$$\begin{aligned} \mathbf{Q_{MCSU}} &= \mathbf{1 - \prod_{I=1}^{N_c} (1 - P(C_I))} \\ &= \mathbf{1 - (1 - 0.1)(1 - 0.01)(1 - 0.01)} \\ &= \mathbf{0.11791} \end{aligned}$$

$$\mathbf{Q_{LOWER} \leq Q_{EXACT} \leq Q_{MCSU} \leq Q_{RARE\ EVE}}$$

Pump System Example

Component probabilities

Relay K1 contacts	K1	1×10^{-4}
Relay K2 contacts	K2	1×10^{-4}
Pressure switch	PRS	5×10^{-4}
Timer relay	TIM	3×10^{-4}
Switch	S1	5×10^{-3}

Minimal Cut Sets

K2		1×10^{-4}
PRS	S1	2.5×10^{-6}
PRS	K1	5.0×10^{-8}
PRS	TIM	1.5×10^{-7}

Top Event Probability

Rare Event

$$\begin{aligned} Q_{\text{SYS}} &= \sum_{i=1}^{N_c} Q_{C_i} \\ &= 1.027 \times 10^{-4} \end{aligned}$$

Minimal Cut Set Upper Bound

$$\begin{aligned} Q_{\text{SYS}} &= 1 - \prod_{i=1}^{N_c} (1 - Q_{C_i}) \\ &= 1.027 \times 10^{-4} \end{aligned}$$

Exact

$$Q_{\text{SYS}} = 1.026987 \times 10^{-4}$$

Importance Measures

⌘ Critical System State

For component i is a state of the remaining $(n - 1)$ components such that the failure of component i causes the system to go from a working to a failed state.

⌘ Birnbaums Measure (I_B)

The probability that the system is in a critical state for the component.

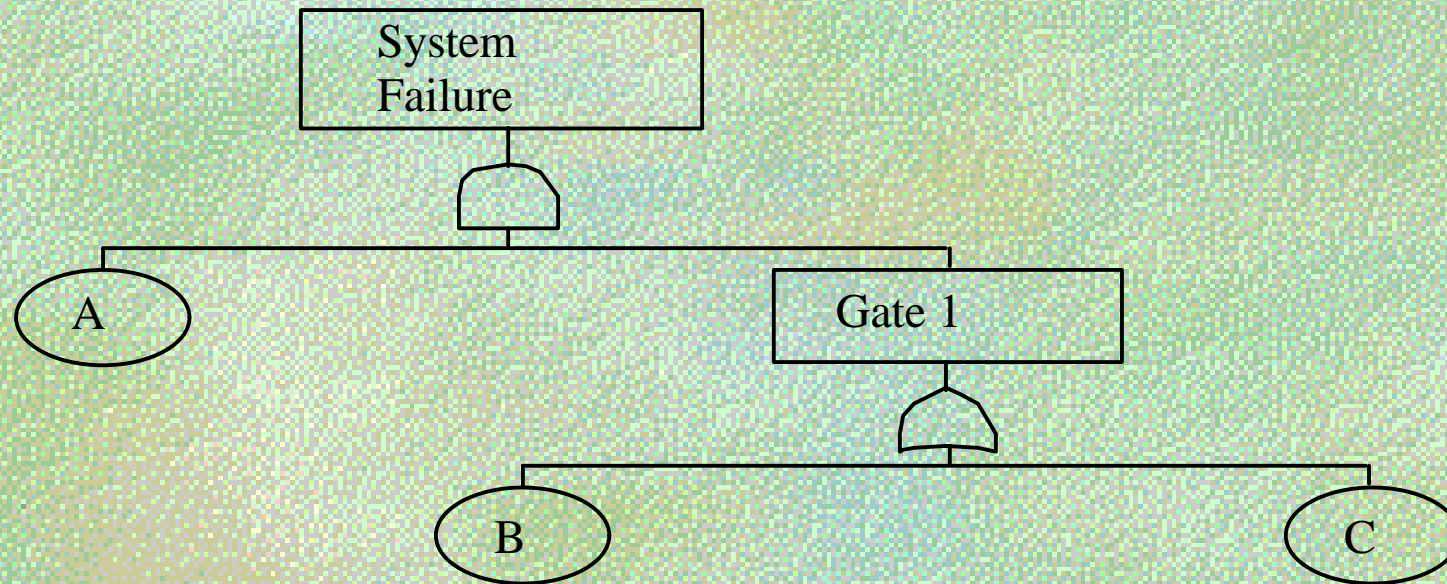
$$I_{B_i} = \frac{\partial Q_{\text{SYS}}}{\partial Q_i}$$

I_{B_i} - Birnbaum importance measure for component i

Q_{SYS} - System unavailability

Q_i - Component unavailability

Example



$$q_A = q_B = q_C = 0.1$$

Minimal Cut Sets

AB

AC

$$\begin{aligned} \mathbf{Q}_{\text{SYS}} &= \mathbf{P}(\mathbf{AB} + \mathbf{AC}) \\ &= \mathbf{Q}_A \mathbf{Q}_B + \mathbf{Q}_A \mathbf{Q}_C - \mathbf{Q}_A \mathbf{Q}_B \mathbf{Q}_C = \mathbf{0.019} \end{aligned}$$

$$\mathbf{I}_{\mathbf{B}_A} = \frac{\partial \mathbf{Q}_{\text{SYS}}}{\partial \mathbf{Q}_A} = \mathbf{Q}_B + \mathbf{Q}_C - \mathbf{Q}_B \mathbf{Q}_C = \mathbf{0.19}$$

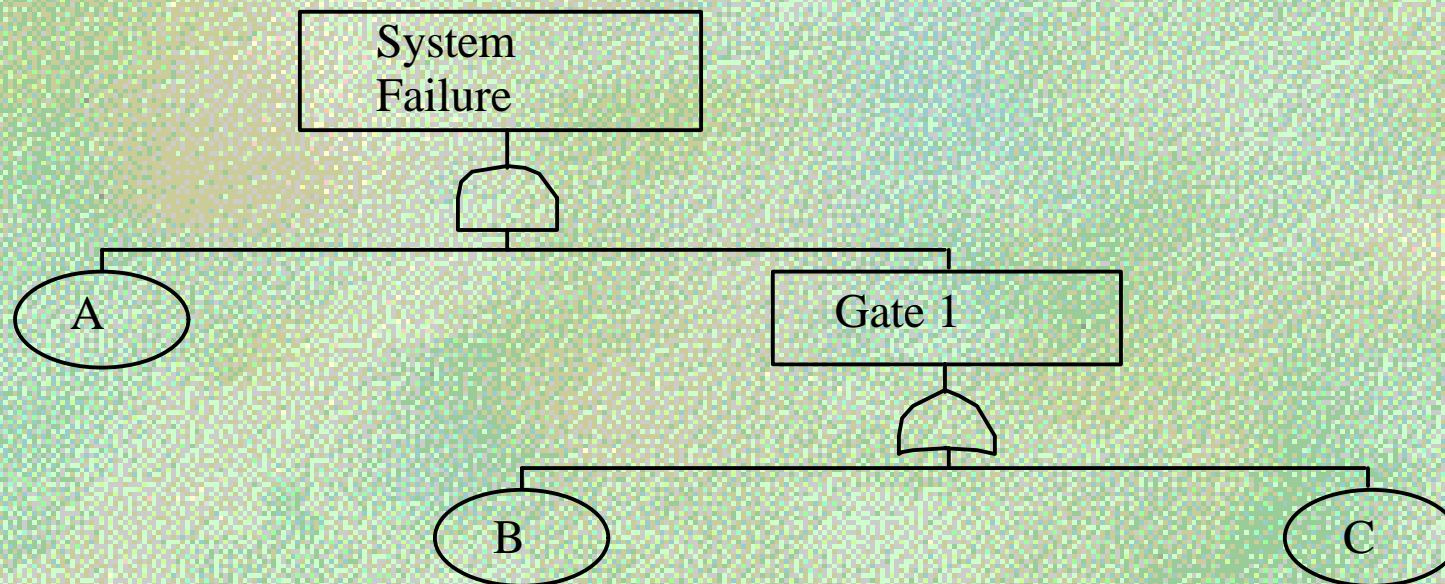
$$\mathbf{I}_{\mathbf{B}_B} = \frac{\partial \mathbf{Q}_{\text{SYS}}}{\partial \mathbf{Q}_B} = \mathbf{Q}_A (1 - \mathbf{Q}_C) = \mathbf{0.09}$$

$$\mathbf{I}_{\mathbf{B}_C} = \frac{\partial \mathbf{Q}_{\text{SYS}}}{\partial \mathbf{Q}_C} = \mathbf{Q}_A (1 - \mathbf{Q}_B) = \mathbf{0.09}$$

Fussell-Vesely Measure (I_{FV})

Probability of the union of all Minimal Cut Sets containing the component given that the system has failed.

Example



$$q_A = q_B = q_C = 0.1$$

Minimal Cut Sets

AB

AC

$$\mathbf{I_{FV_A}} = \frac{\mathbf{P(AB + BC)}}{\mathbf{Q_{SYS}}} = \frac{\mathbf{Q_{SYS}}}{\mathbf{Q_{SYS}}} = \mathbf{1.0}$$

$$\mathbf{I_{FV_B}} = \frac{\mathbf{P(AB)}}{\mathbf{Q_{SYS}}} = \frac{\mathbf{Q_A Q_B}}{\mathbf{Q_{SYS}}} = \frac{\mathbf{0.01}}{\mathbf{0.019}} = \mathbf{0.526}$$

$$\mathbf{I_{FV_C}} = \frac{\mathbf{P(AC)}}{\mathbf{Q_{SYS}}} = \frac{\mathbf{Q_A Q_C}}{\mathbf{Q_{SYS}}} = \frac{\mathbf{0.01}}{\mathbf{0.019}} = \mathbf{0.526}$$

Pump System Example

Importance Measures

	Fussell Vesely	Birnbaum
K2	0.974	0.9999
PRS	0.026	5.397×10^{-3}
S1	0.024	4.9975×10^{-4}
TIM	0.0015	4.974×10^{-4}
K1	0.0005	4.973×10^{-4}

Session 2: Advanced Features



Minimal Cut Set Failure Frequency

$W_{C_k}(D)$ – UNCONDITIONAL FAILURE
OF CUT SET K
N – COMPONENTS IN MIN CUT 1

$$W_{C_k}(D) = \sum_{I=1}^N W_I(D) \left(\prod_{\substack{J=1 \\ J \neq I}}^N Q_J(D) \right)$$

Example Min Cut Set 1 = ABC

$$W_{C_1} = W_A Q_B Q_C + W_B Q_A Q_C + W_C Q_A Q_B$$

w(t) - unconditional failure intensity

The probability that a component fails in

$$(t, t + dt) \quad \mathbf{w}(\mathbf{T}) = \lambda(\mathbf{T})[1 - \mathbf{Q}(\mathbf{T})]$$

Expected Number of Failures W(0, t)

$$\mathbf{W}(0, \mathbf{T}) = \int_0^{\mathbf{T}} \mathbf{w}(\mathbf{U}) \mathbf{dU}$$

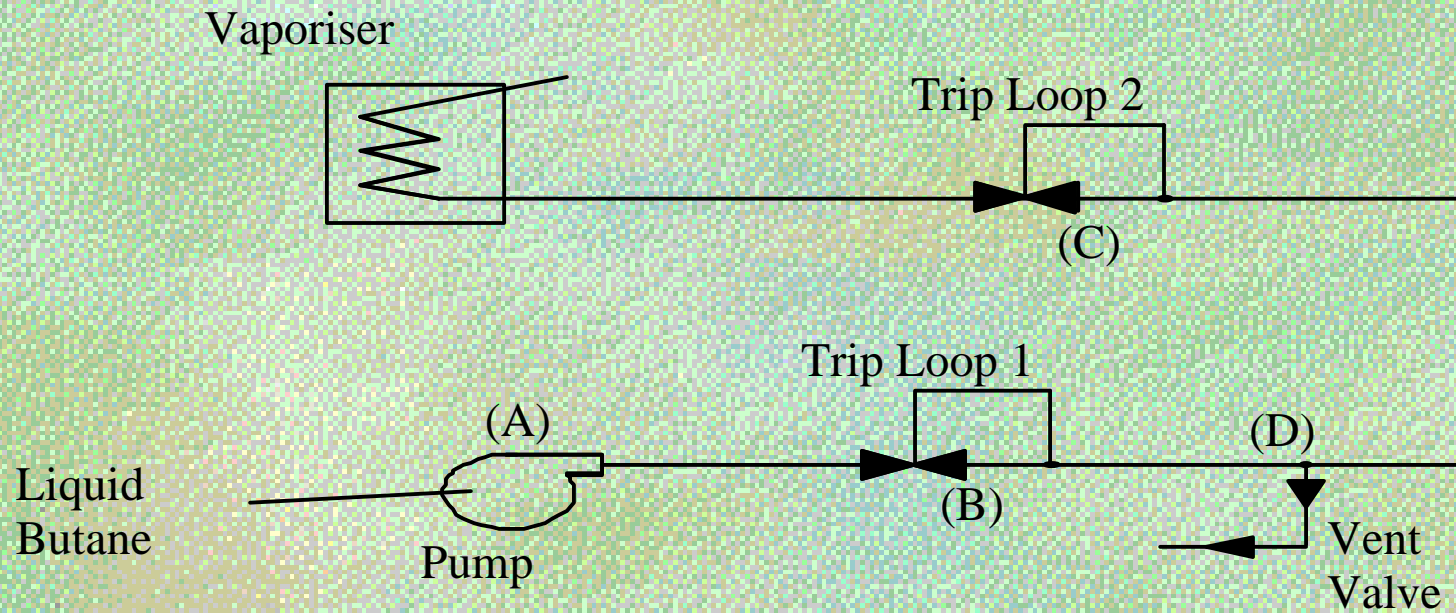
Top Event Failure Frequency

(upper bound approximation)

$$W_{\text{SYS}} = \sum_{I=1}^{N_c} W_{C_I} \left(1 - \prod_{\substack{J=1 \\ J \neq I}}^{N_c} (1 - Q_{C_J}) \right)$$

N_c – NO OF MIN CUT SETS

Initiator/Enabler Theory



Failure Modes:

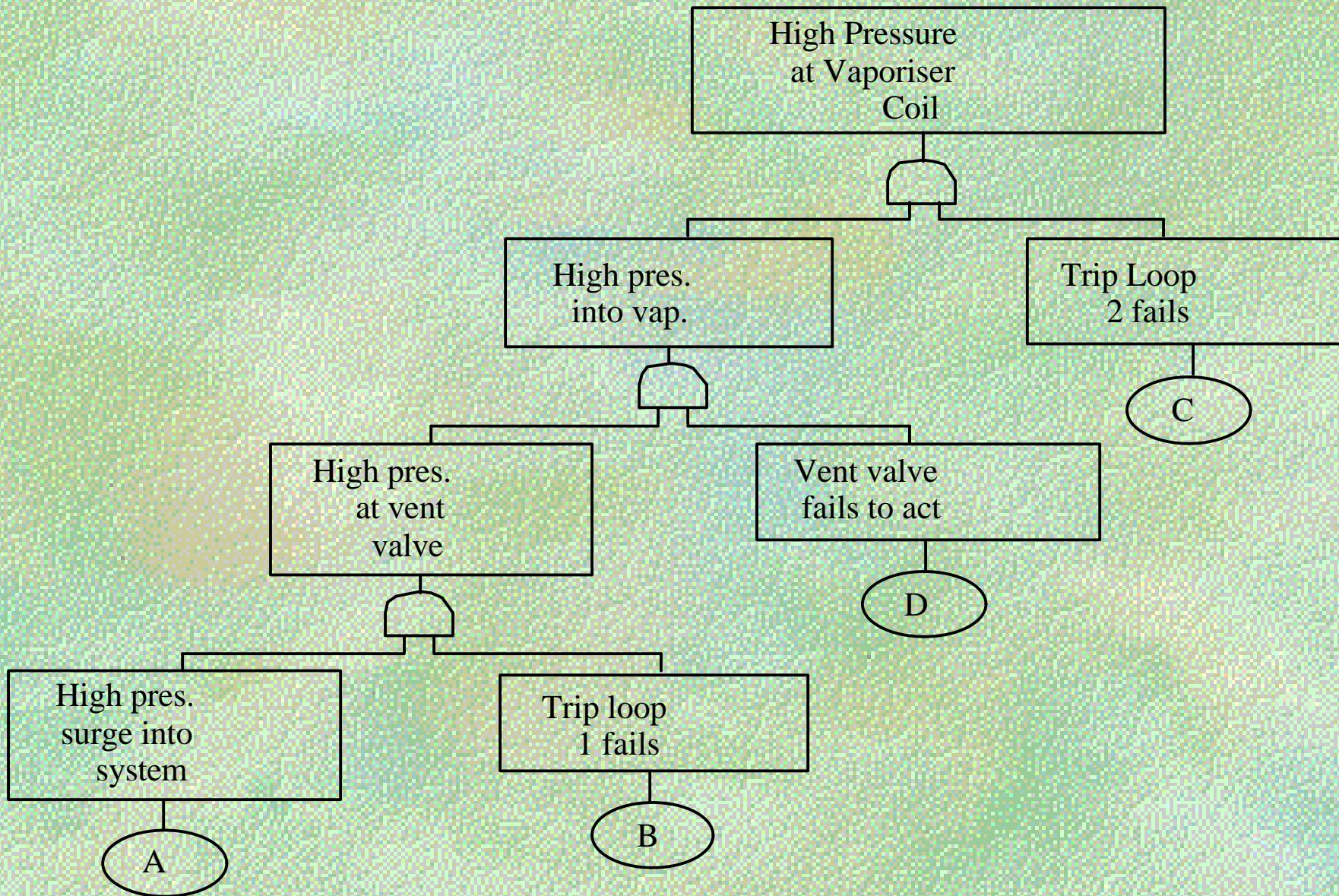
- Pump Surge (control system failure) A
- Trip Loop 1 fails to act B
- Trip Loop 2 fails to act C
- Vent Valve fails to act D

Component Data

	λ	τ	$\mathbf{W} = \lambda (1 - \mathbf{Q})$
A			$\mathbf{6.667} \times 10^{-3}$
B			$\mathbf{9.091} \times 10^{-3}$
C			$\mathbf{9.091} \times 10^{-3}$
D			$\mathbf{9.091} \times 10^{-3}$

$$+ \quad \mathbf{Q} = \frac{\lambda\tau}{\lambda\tau + 1}$$

$$* \quad \mathbf{Q} = \lambda\left(\tau + \frac{\theta}{2}\right)$$



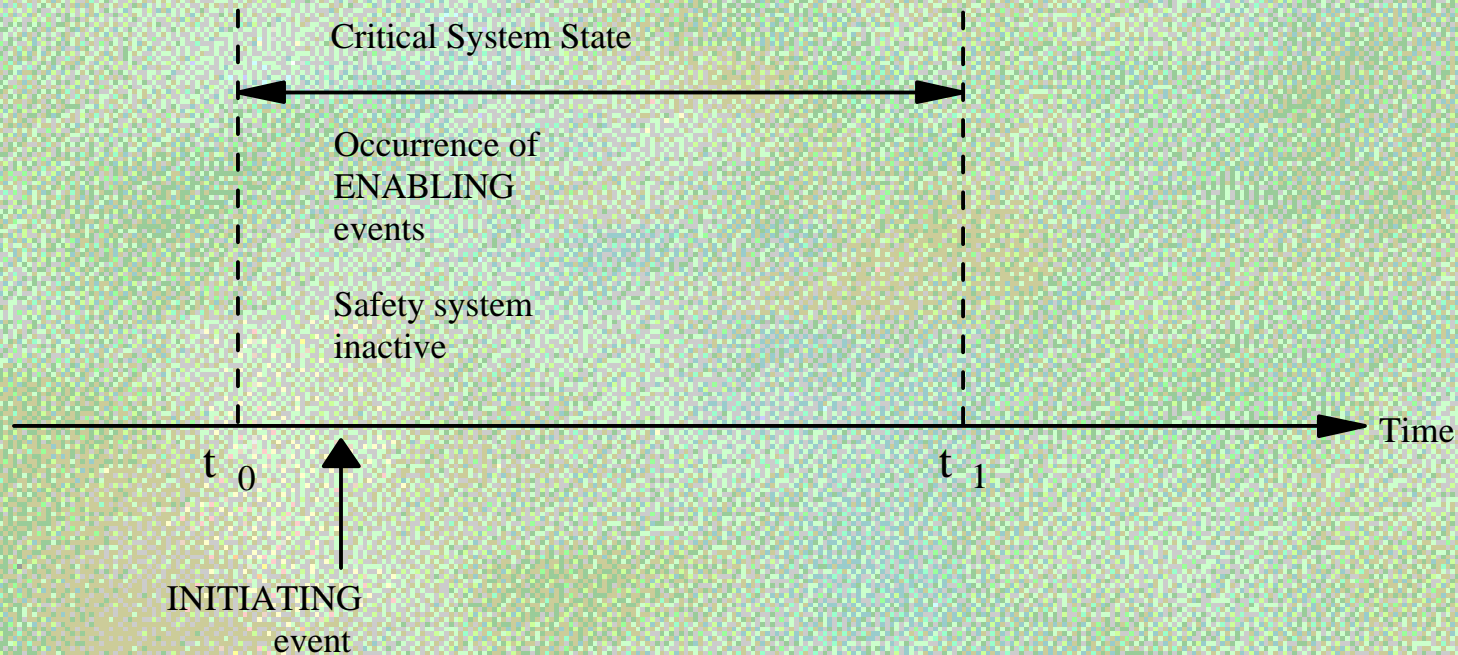
Conventional Approach

$$\begin{aligned}
 W_S(D) &= W_{C_1}(D) \\
 &= \sum_{J=1}^4 W_J(D) \prod_{\substack{I=1 \\ I \neq J}}^4 Q_I(D) \\
 &= W_A Q_B Q_C Q_D + W_B Q_A Q_C Q_D + W_C Q_A Q_B Q_D \\
 &\quad + W_D Q_A Q_B Q_C \\
 &= 5.0075 \times 10^{-6} + 2.5037 \times 10^{-5} \\
 &\quad + 2.5037 \times 10^{-5} + 2.5037 \times 10^{-5} \\
 &= 8.012 \times 10^{-5}
 \end{aligned}$$

Expected number of failures over 10 years

$$\begin{aligned}
 W(0, 87600) &= \int_0^{87600} 8.012 \times 10^{-5} D^1 \\
 &= 7.02
 \end{aligned}$$

The Window for Initiating Events



Initiating Events

Initiating events perturb system variables and place a demand on control/protection Systems to respond.

Enabling Events

Enabling events are inactive control/Protection systems which permit initiating Events to cause the top event.

Using initiator/enabler theory

$$\begin{aligned}W_S(D) &= W_{C_1}(D) \\ &= W_A Q_B Q_C Q_D \\ &= 5.0075 \times 10^{-6}\end{aligned}$$

Expected Number of Failures over 10 years

$$\begin{aligned}W(0,87600) &= \int_0^{87600} 5.0075 \times 10^{-6} D^1 \\ &= 0.4387\end{aligned}$$

Not Logic

Noncoherent Fault Trees

Barlow - “A physical system would be quite unusual (or poorly designed) if improving the performance of a component (ie by replacing a failed component by a functioning component) causes the system to deteriorate (ie change from a functioning to a failed state)”

Example

Min Cut Set **$ABC\bar{C}$**

Is not a coherent structure as

$AB\bar{C}$	→	SYSTEM FAILS
ABC	→	SYSTEM WORKS

Coherent structure consist of only:

- AND gates
- OR gates

Noncoherent Structures

Are those which do not conform to the definition of a coherent structure

This occurs if the NOT operator is used or implied

eg XOR

Laws of Boolean Algebra - Not Logic

$$\mathbf{A + \bar{A} = 1}$$

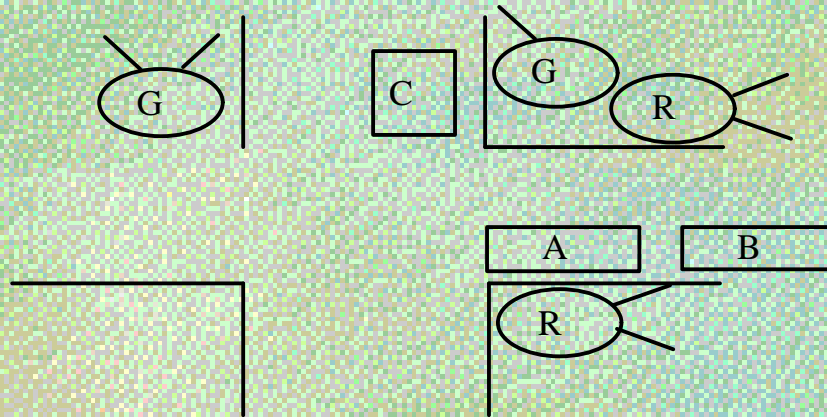
$$\mathbf{A \cdot \bar{A} = 0}$$

De Morgan's Laws

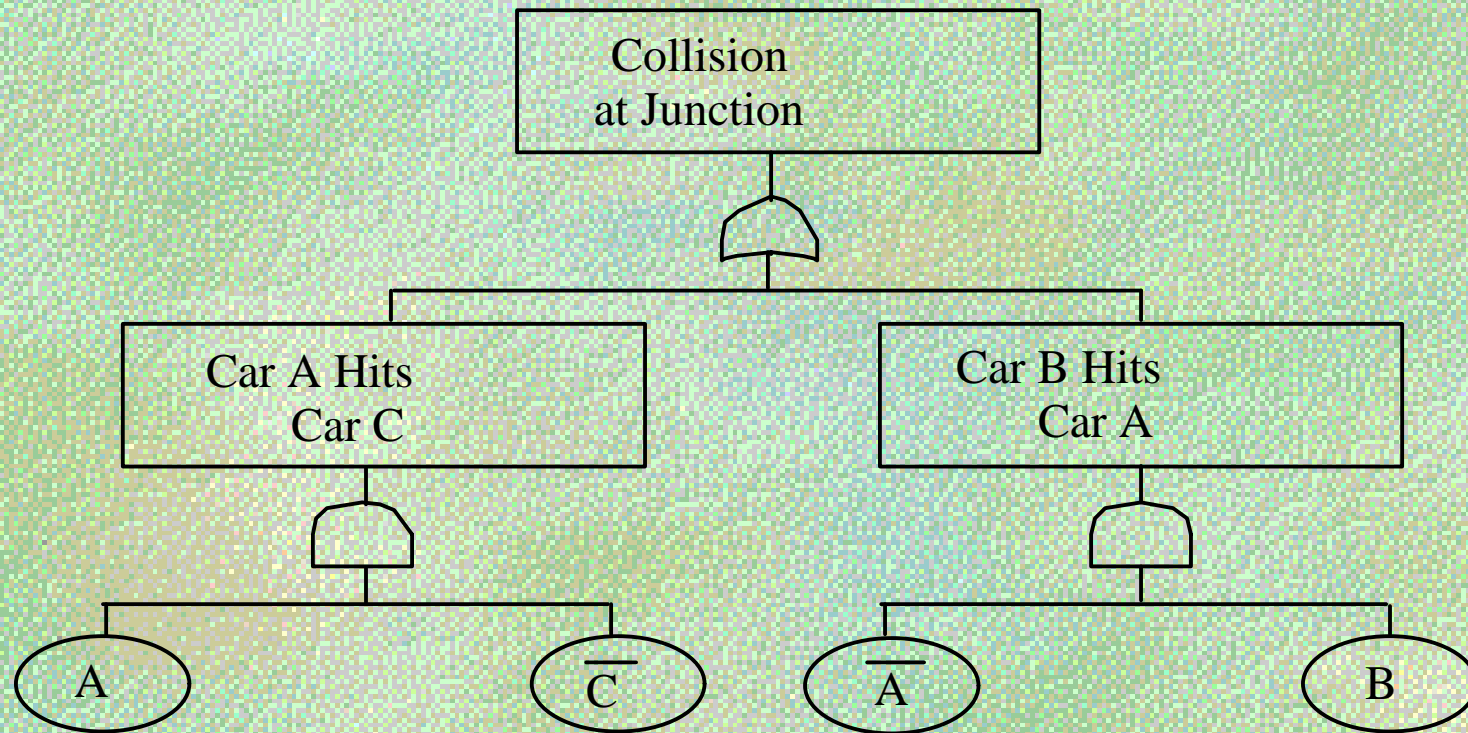
$$\overline{\mathbf{(A + B)}} = \bar{\mathbf{A}} \cdot \bar{\mathbf{B}}$$

$$\overline{\mathbf{(A \cdot B)}} = \bar{\mathbf{A}} + \bar{\mathbf{B}}$$

Road Junction Example



- A - Car A fails to stop
- B - Car B fails to stop
- C - Car C stops



$$TOP = AC + AB\bar{A}$$

Implicant Set is a combination of basic events (success or failure) which produces the top event.

Prime Implicant Set is a combination of basic events (success or failure) which is both necessary and sufficient to cause the top event.

$$\mathbf{TOP} = \mathbf{A} \overline{\mathbf{C}} + \overline{\mathbf{A}} \mathbf{B}$$

What about $\overline{\mathbf{C}}\mathbf{B}$

it is a prime implicant

Conventional approaches to fault tree reduction do not deliver all prime implicants for every non-coherent tree

SO:

$$\mathbf{TOP} = \mathbf{A} \overline{\mathbf{C}} + \overline{\mathbf{A}} \mathbf{B} + \overline{\mathbf{C}} \mathbf{B}$$

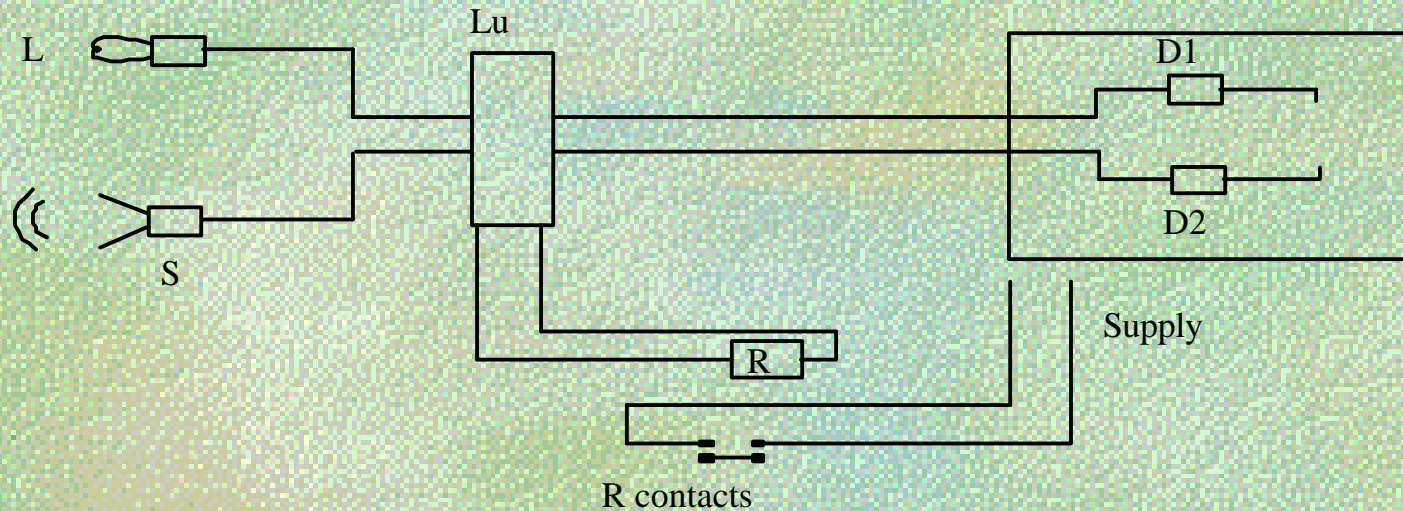
Coherent approximation

$$\mathbf{TOP} = \mathbf{A} + \mathbf{B}$$

OK if

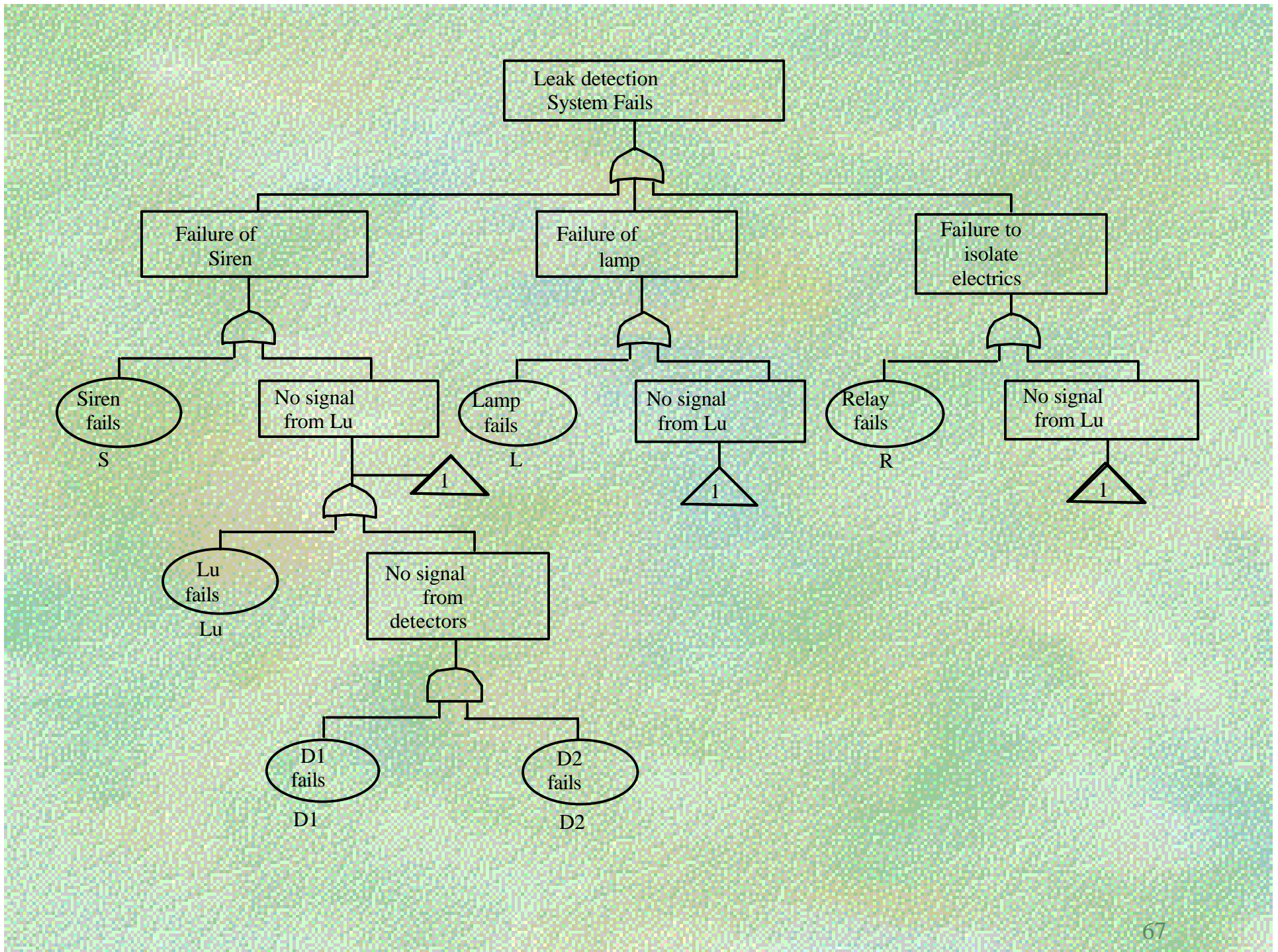
$$\mathbf{P}(\overline{\mathbf{C}}) \approx \mathbf{1}$$

Example



System Functions - on detecting gas

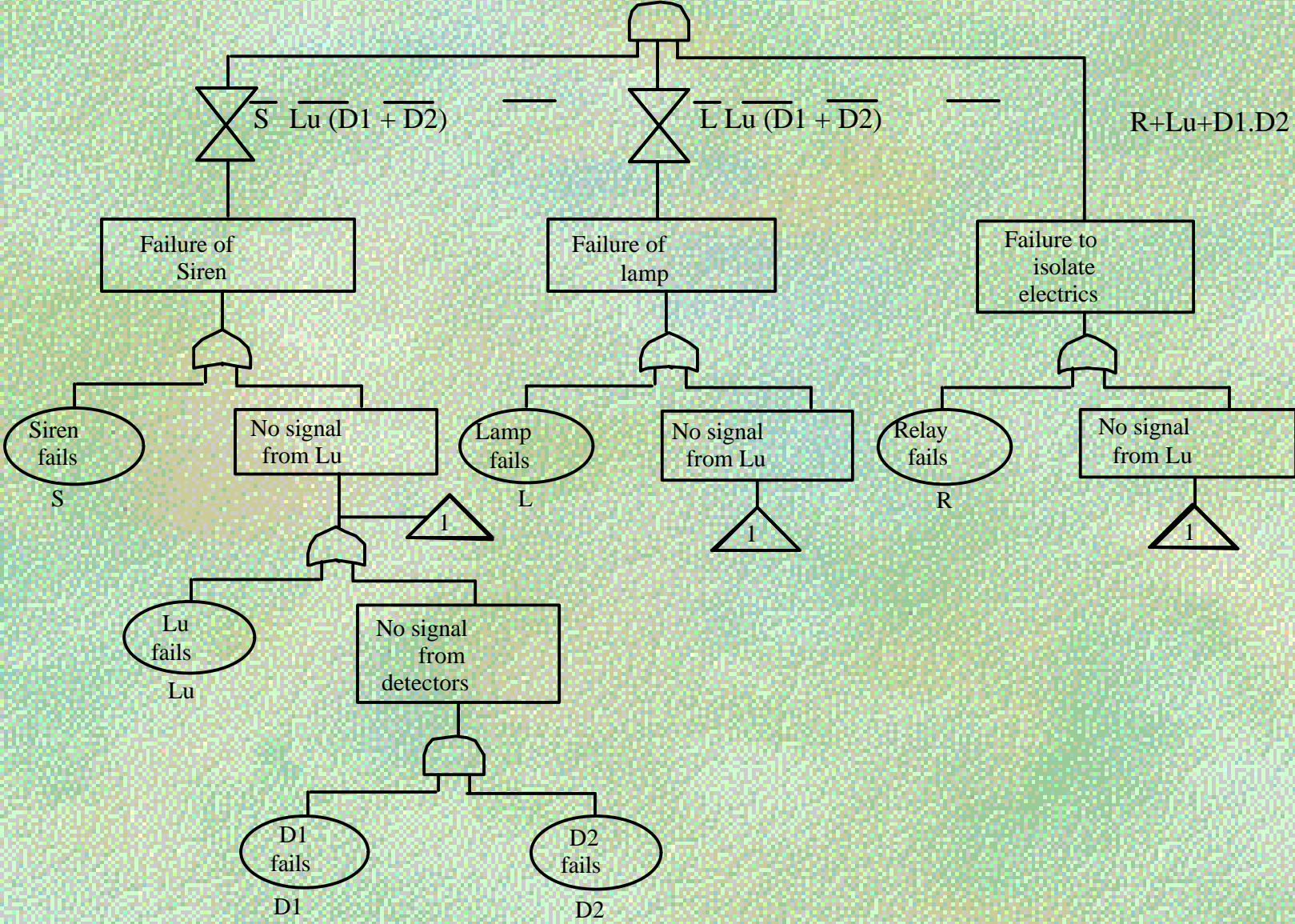
- a) to alert the operator via a lamp
- b) to alert the operator via a siren
- c) to isolate electrical ignition sources



System Outcomes

	SIREN	LAMP	ISOLATION	SYSTEM
1	W	W	W	?
2	W	W	F	
3	W	F	W	
4	W	F	F	
5	F	W	W	
6	F	W	F	
7	F	F	W	
8	F	F	F	

Operator alerted of spill (Siren and Lamp) But electric circuits active



$$\begin{aligned}
\mathbf{TOP} &= (\overline{\mathbf{S}} \overline{\mathbf{LU}} (\overline{\mathbf{D}}_1 + \overline{\mathbf{D}}_2)).(\overline{\mathbf{L}} \overline{\mathbf{LU}} (\overline{\mathbf{D}}_1 + \overline{\mathbf{D}}_2)).(\mathbf{R} + \mathbf{LU} + \mathbf{D}_1.\mathbf{D}_2) \\
&= \overline{\mathbf{S}} \overline{\mathbf{L}} \overline{\mathbf{LU}} (\overline{\mathbf{D}}_1 + \overline{\mathbf{D}}_2).(\mathbf{R} + \mathbf{LU} + \mathbf{D}_1.\mathbf{D}_2) \\
&= \overline{\mathbf{S}} \overline{\mathbf{L}} \overline{\mathbf{LU}} (\overline{\mathbf{D}}_1 + \overline{\mathbf{D}}_2).\mathbf{R}
\end{aligned}$$

Coherent Approximation

$$\mathbf{TOP} = \mathbf{R}$$

Session 3: Current Research



Problem areas in conventional Fault Tree Analysis

⌘ Qualitative Analysis

For very large fault trees it may not be possible to produce a complete list of minimal cut sets.

Solution

Evaluate only those minimal cut sets which have the most significant contribution to system failure

- Order culling
- Probability or Frequency culling

⌘ Quantitative Analysis

- Requires minimal cut sets
- Calculations are too computer intensive to perform fully

Solution

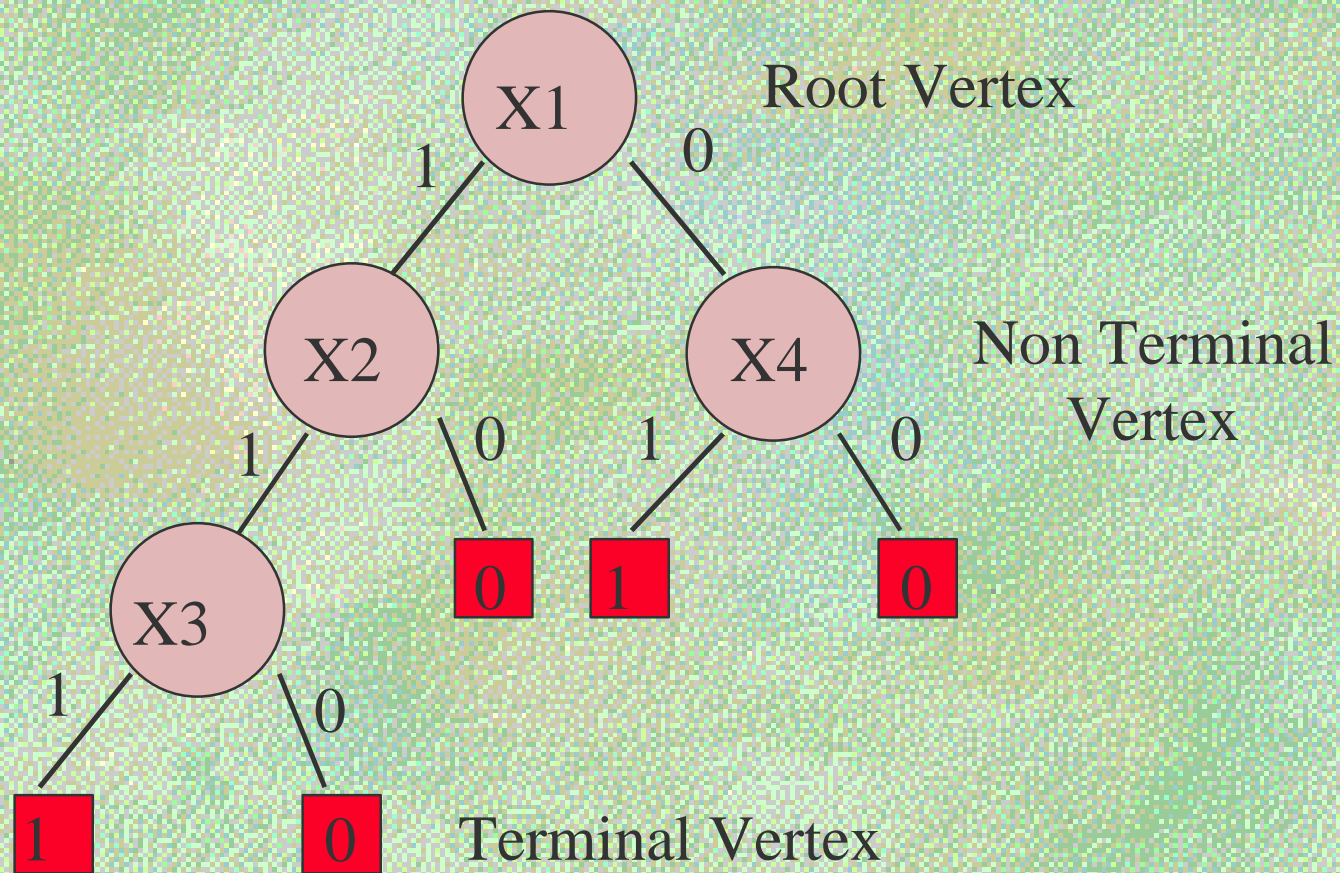
- Use most significant minimal cut sets
- Use approximate calculation techniques.

Binary Decision Diagrams

BDD's

- 1 Developed over last 5 years.
- 2 Fault Tree - Good representation of engineering failure logic
 - Poor efficiency/accuracy in mathematical calculations
- BDD - Poor representation of engineering failure logic
 - Good efficiency/accuracy in mathematical calculations.
- 3 Trade-off for improved efficiency/accuracy is conversion between FT \rightarrow BDD.
- 4 Minimal cut sets not required to perform quantification.

B.D.D. Structure

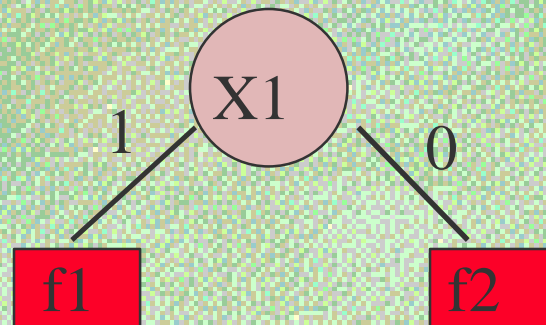


Fault Tree \rightarrow B.D.D

1. Initially requires basic events in the fault tree to be placed in an ordering.

2. Most common method - If-Then-Else Structure

* $\text{ITE}(X1, f1, f2)$ means
if $X1$ fails
then consider $f1$
else consider $f2$



Simple Conversion - ite method

Rules : $G = \text{ite}(x, g1, g2)$, $H = \text{ite}(y, h1, h2)$

$G * H =$

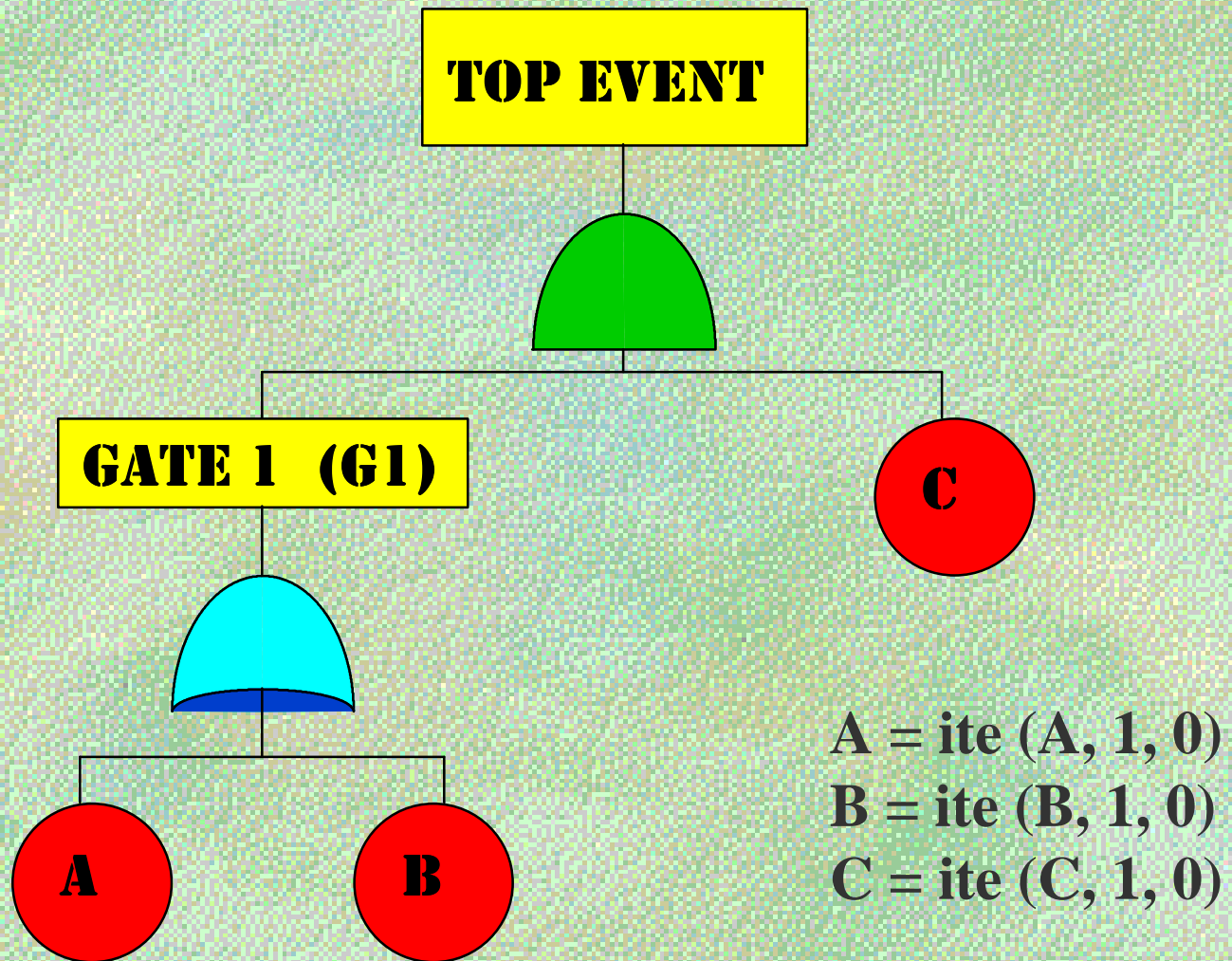
$\text{if}(x < y) \Rightarrow \text{ite}(x, g1 * H, g2 * H)$

$\text{if}(x = y) \Rightarrow \text{ite}(x, g1 * h1, g2 * h2)$

$\text{if } * = \text{AND} \quad \Rightarrow 1 * G = G, 0 * G = 0$

$\text{if } * = \text{OR} \quad \Rightarrow 1 * G = 1, 0 * G = G$

Fault Tree Structure



Simple Conversion cont...

Order

$A < B < C$

$G1 = A + B$

$= \text{ite}(A, 1, 0) + \text{ite}(B, 1, 0)$

$= \text{ite}(A, 1 + \text{ite}(B, 1, 0), 0 + \text{ite}(B, 1, 0))$

$= \text{ite}(A, 1, \text{ite}(B, 1, 0))$

$TOP = G1.C$

$= \text{ite}(A, 1, \text{ite}(B, 1, 0)).\text{ite}(C, 1, 0)$

$= \text{ite}(A, 1.\text{ite}(C, 1, 0), \text{ite}(B, 1, 0).\text{ite}(C, 1, 0))$

$= \text{ite}(A, \text{ite}(C, 1, 0), \text{ite}(B, 1.\text{ite}(C, 1, 0),$

$0.\text{ite}(C, 1, 0)))$

$= \text{ite}(A, \text{ite}(C, 1, 0), \text{ite}(B, \text{ite}(C, 1, 0), 0))$

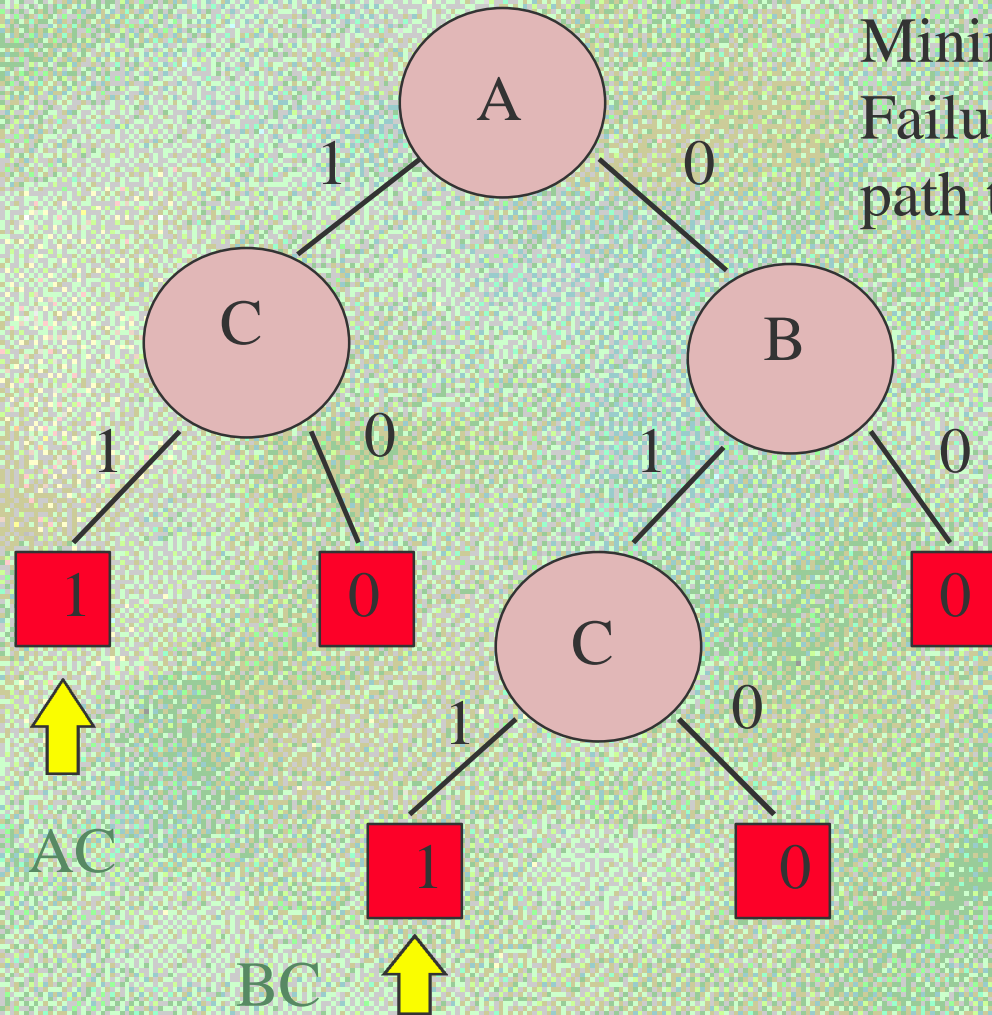


Root Vertex

1 branch

0 branch

Resulting Diagram



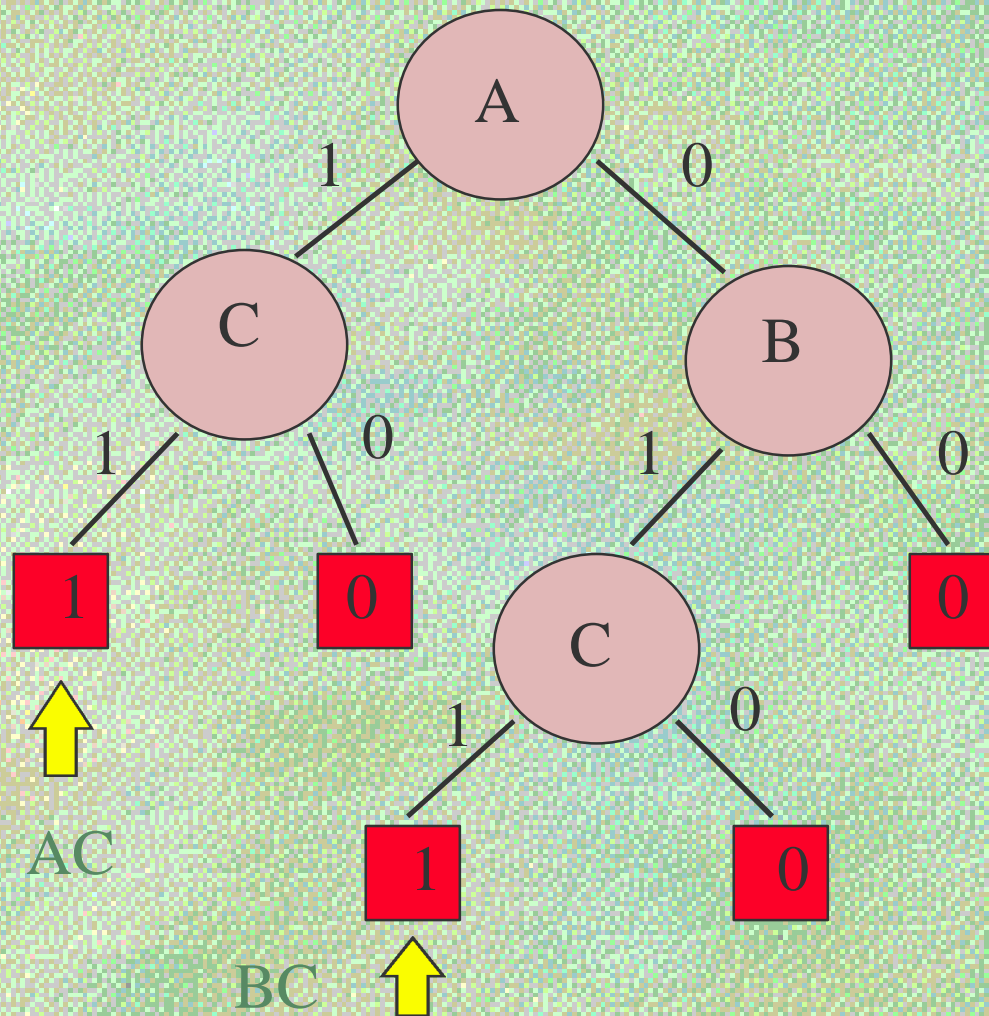
Minimal Cut Sets :-
Failure events on
path to terminal 1

Top Event Probability from B.D.D

=> Probability of the sum of disjoint paths through the bdd.

Disjoint Path - included in a path are the basic events that lie on a 0 branch on the way to a terminal 1 vertex.

Basic Events lying on a 0 branch are denoted as $\overline{X_i}$, ie. 'Not' X_i



The disjoint paths of the bdd are : AC, ABC

Top event probability : $P(AC + ABC)$

Disadvantages of BDD

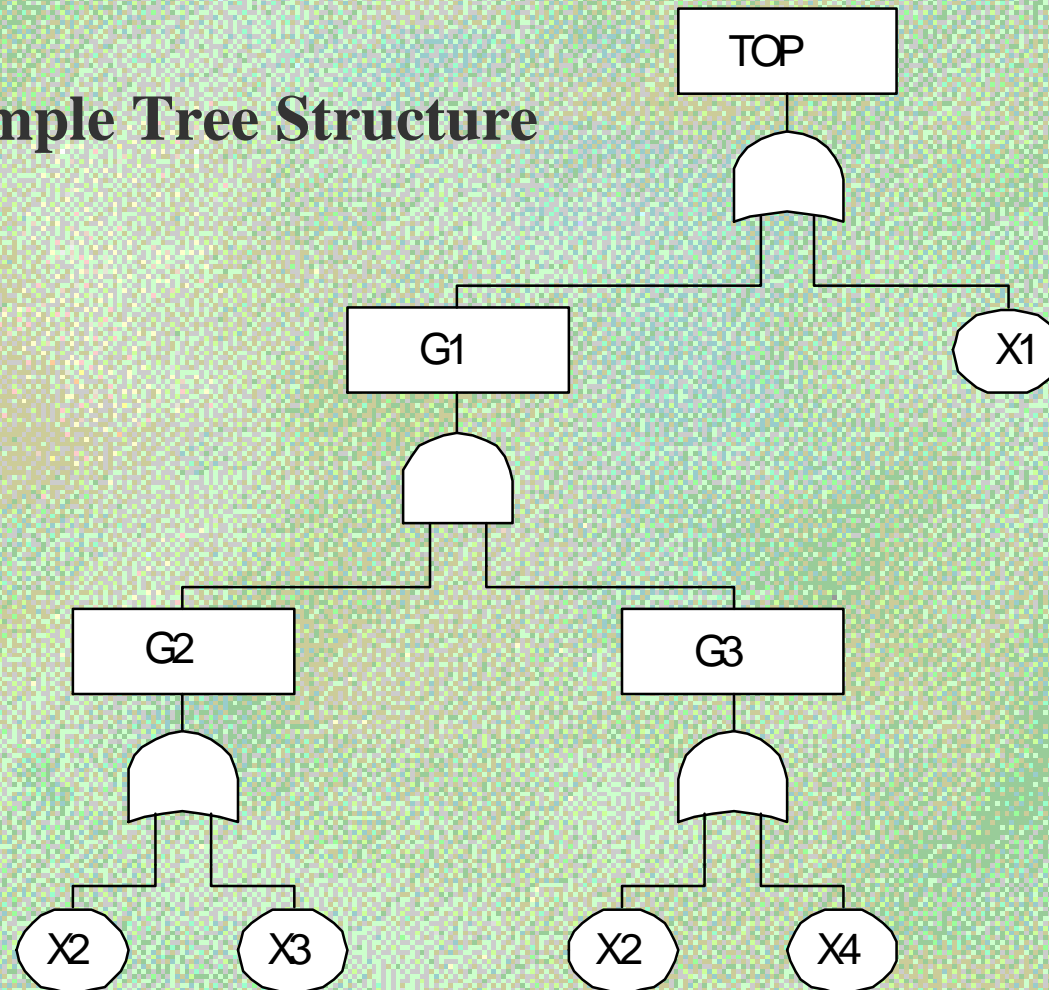
- FTA \rightarrow BDD conversion
- Poor ordering can give poor efficiency

Advantage of BDD

- improved efficiency
- improved accuracy

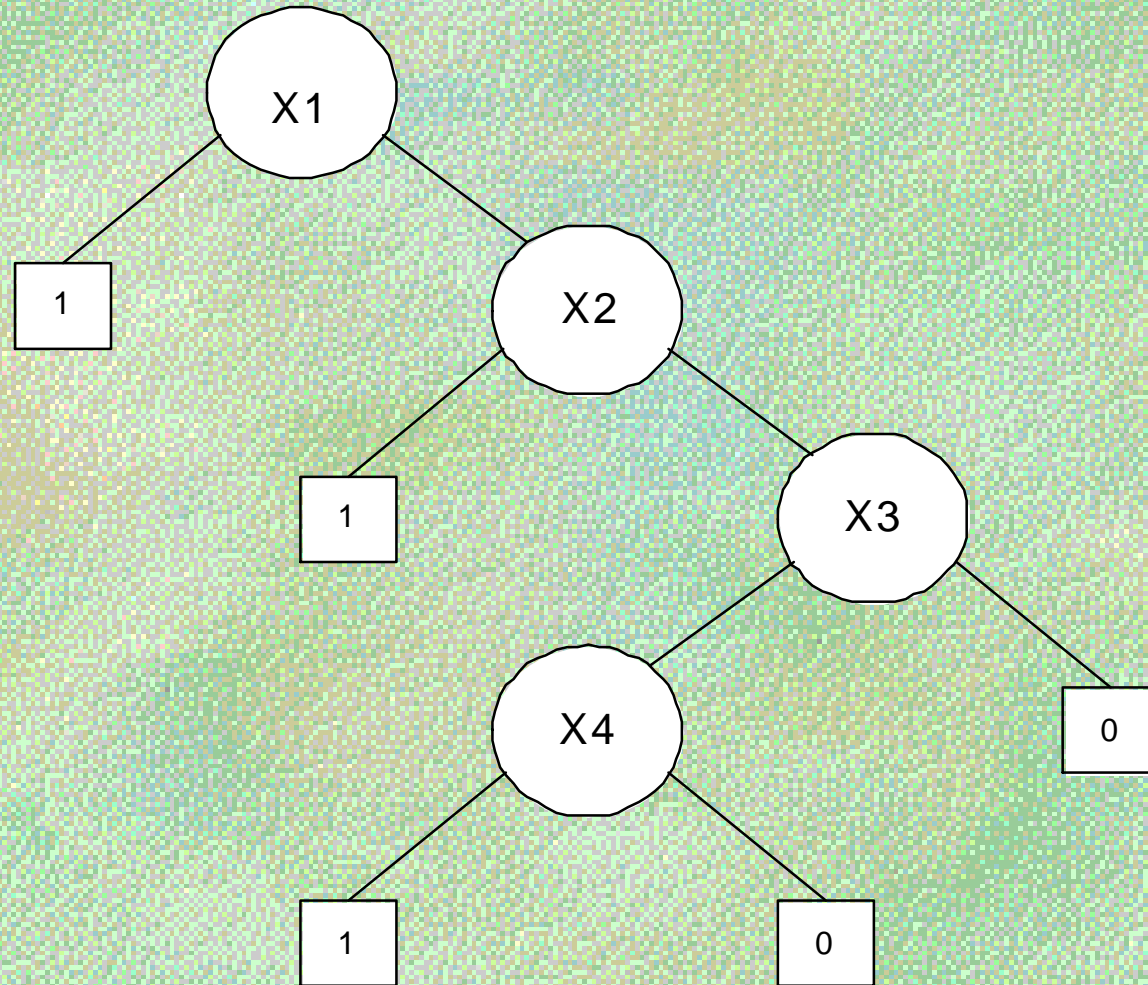
Result of Different Ordering Permutations

An Example Tree Structure



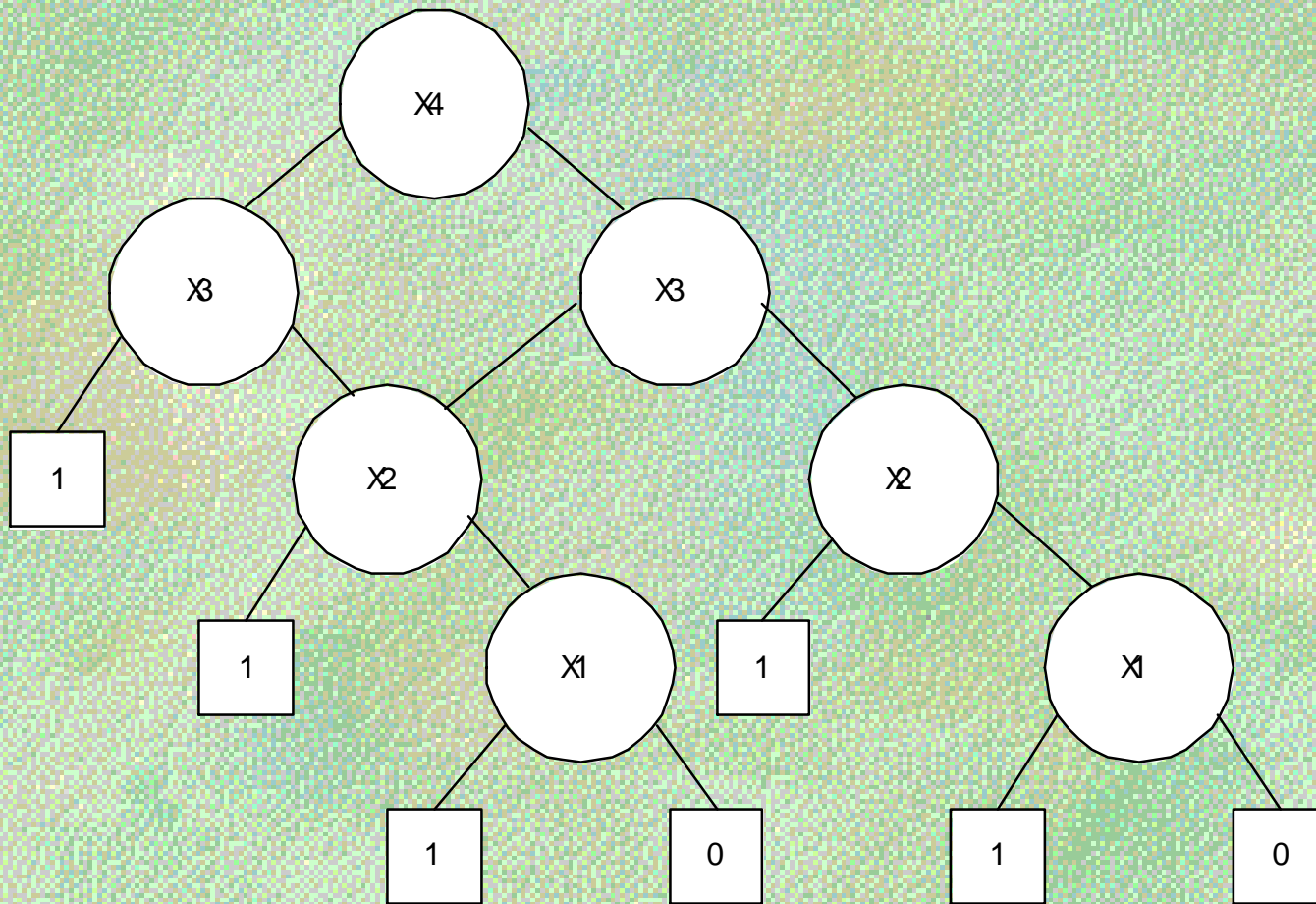
Result of Ordering :

$$X1 < X2 < X3 < X4$$

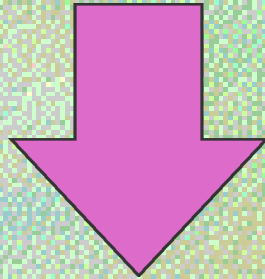


Result of Ordering :

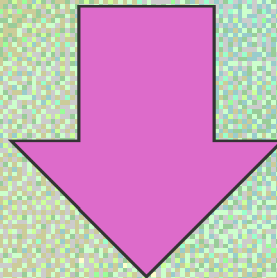
$$X4 < X3 < X2 < X1$$



FAULT TREE CHARACTERISTICS



????



**EFFICIENT B.D.D VARIABLE
ORDERING**

Training Methods

- Classifier System
- Neural Networks

Direct evaluation of Fault Tree Structure

Safety System Design Considerations

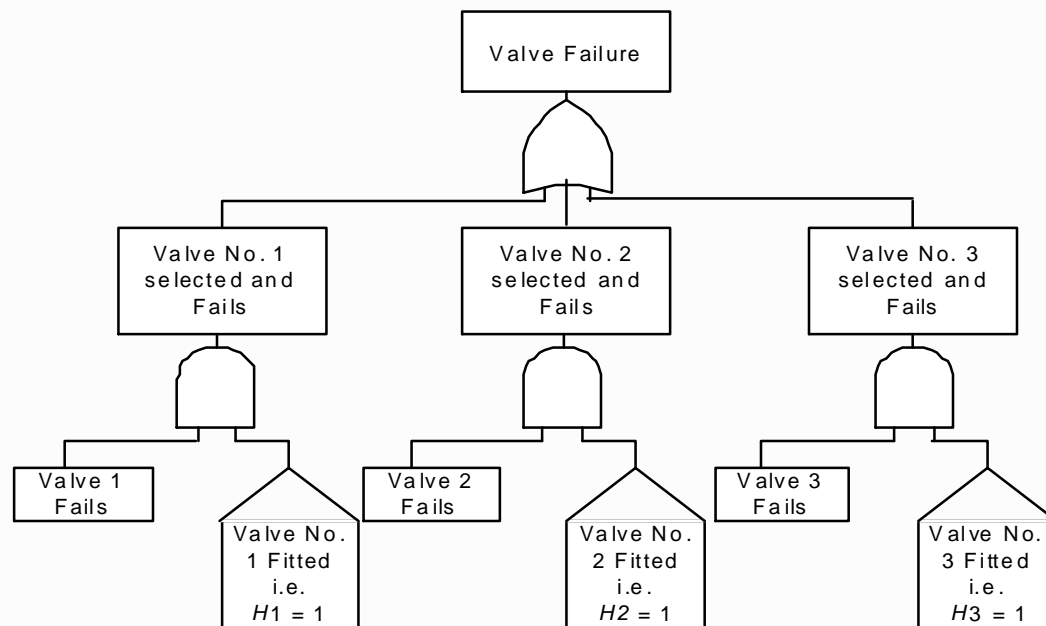
- ❖ Redundancy and diversity levels
- ❖ Component selection
- ❖ Time interval between testing the system

*Choice of design not unrestricted

System Analysis

- ❖ **Fault Trees** represent and quantify the system unavailability of each potential design
- ❖ **House events** used to construct a single fault tree representing the failure mode of EACH design

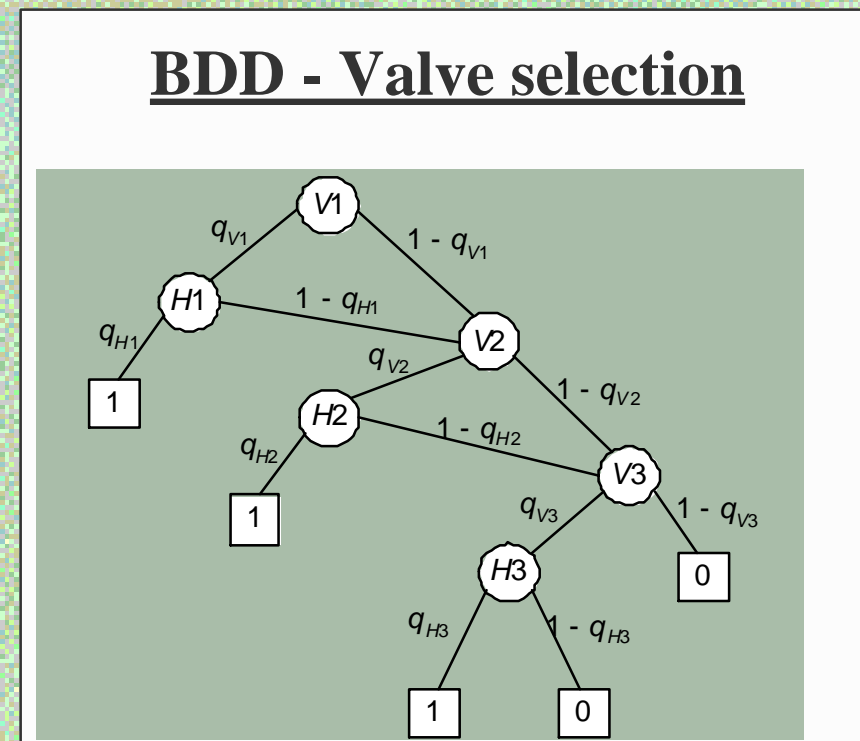
**Fault tree
representing
selection of
valve type
1,2 or 3**



System Analysis, contd.

Binary Decision Diagrams improve efficiency of system analysis
BDD

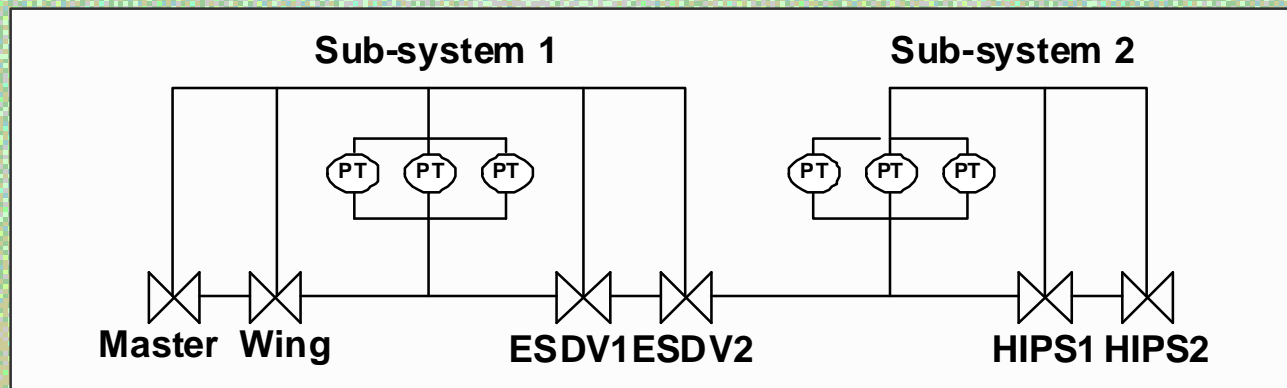
- ❖ Connecting branches
- ❖ Non-terminal vertices
 - correspond to basic events
- ❖ Terminal vertices
 - 0, i.e. system works
 - 1, i.e. system fails



The Optimisation Problem

- ❖ System performance **CANNOT** be expressed as an explicit objective function
- ❖ Most design variables are integer or Boolean
- ❖ Constraints are of both implicit and explicit type

High Integrity Protection System



Designer Options

- ❖ No. ESD valves (0,1,2)?
- v No. HIPS valves (0,1,2)?
- v No. PT's each subsystem (0 to 4)?
- v No. PT's to trip?
- v Type of valve?
- v Type of PT?
- v MTI each subsystem (1 to 104 weeks)?

Variable

E
H
 N_1, N_2
 K_1, K_2
 V_1, V_2
 P_1, P_2
 θ_1, θ_2

Limitations on Design

- ❖ Cost < 1000 units
- ❖ Maintenance Dwn Time (MDT) < 130 hours
- ❖ Spurious trip occurrences < 1 per year

Genetic Algorithms

Structure of the GA

Set up **initial population**

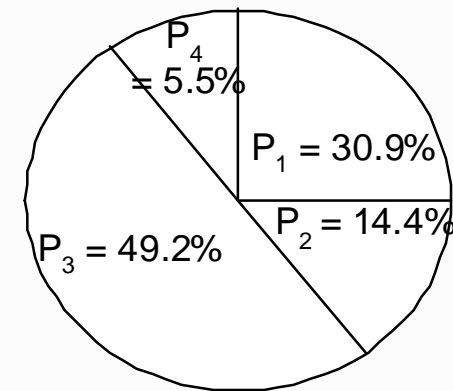
of strings

Loop

- ✦ Evaluate **fitness** of each string
- ✦ **Selection** - biased roulette wheel
- ✦ **Crossover/Mutation** on selected offspring

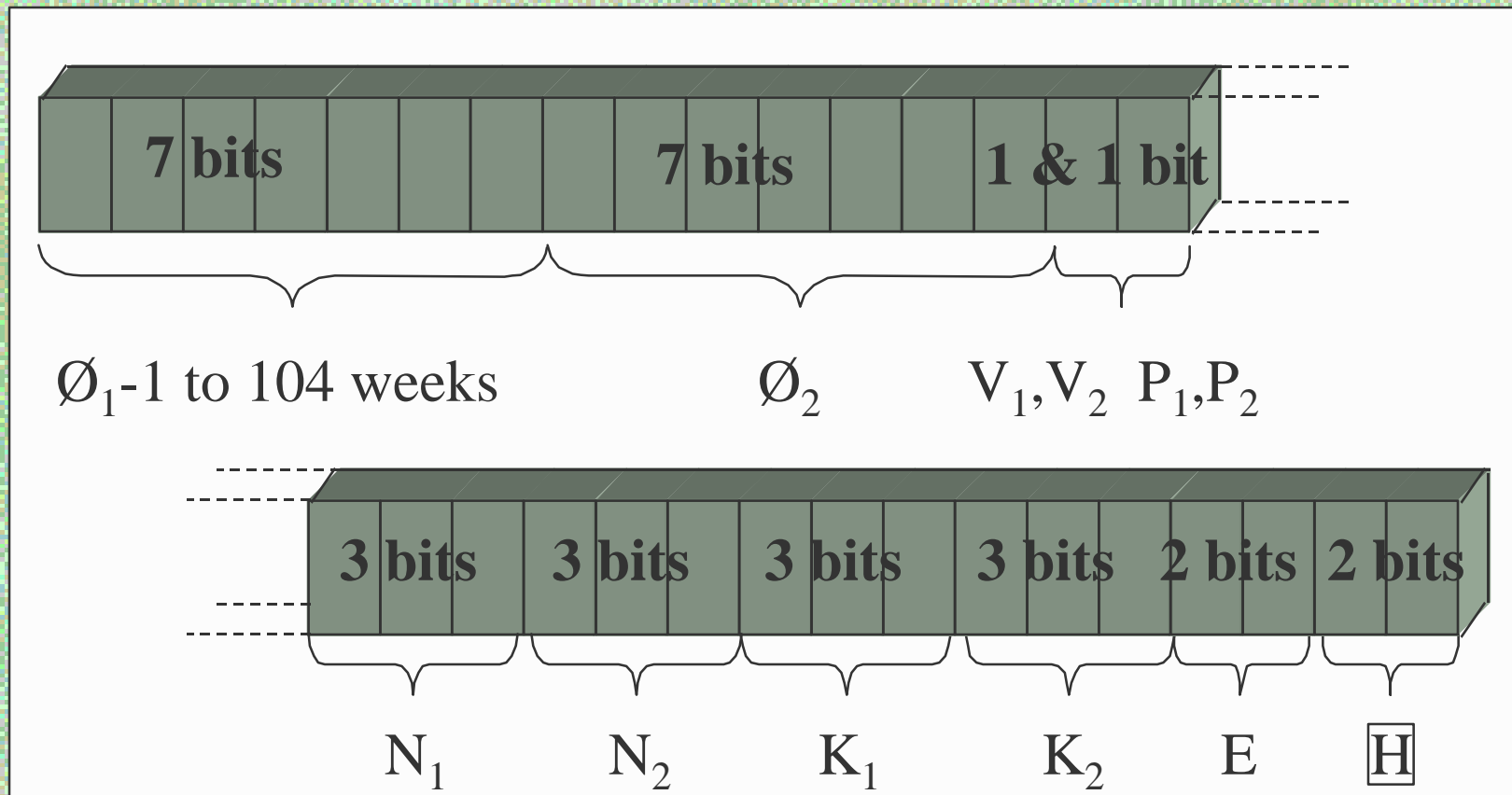
*One iteration of each loop
= **generation**

Selection Biased roulette wheel



$$P_i = \frac{\text{individual fitness of chromosome}}{\text{total fitness of gene pool}}$$

Initialising a System Design



Total = 32 bits

Evaluating Design Fitness

The fitness of each string comprises of four parts;

- ❖ Probability of system unavailability
- v Penalty due to excess cost
- v Penalty due to excess MDT
- v Penalty due to excess spurious trip frequency

As a sole fitness value;

$$Q'_{SYS} = Q_{SYS} + CP + MDTP + STFP$$

* = penalised probability of system unavailability

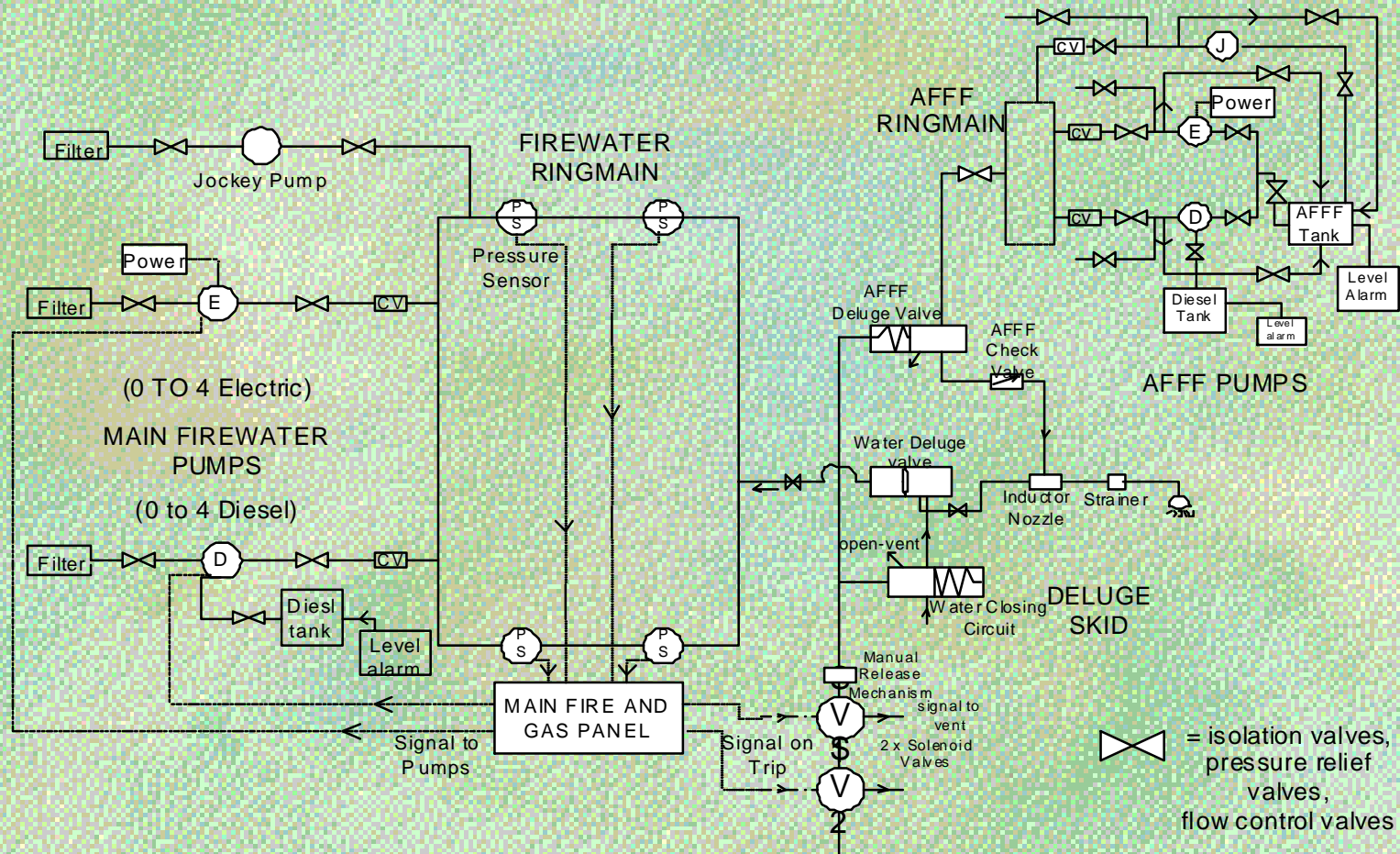
Best Design's Characteristics

	<u>Subsys 1 & 2</u>		<u>Type</u>
❖ No. ESD/HIPS valves	0	2	2
v No. PT's	3	3	1
v No. PT's to trip system	2	2	
v M.T.I.	23	57	

❖ MDT	123 hours
v Cost	842 units
v Spurious trip	0.455

<u>System</u> <u>Unavailability</u>	<u>0.0011</u>
--	---------------

Diagram of The Deluge System



Design Variables of Deluge System

- ❖ No. of electric pumps firewater system (1 to 4) – type E1 to E5
- v No. of electric pumps AFFF system (1,2) – type E6, E7
- v No. of diesel pumps firewater system (1 to 4) – type D1 to D5
- v No. of diesel pumps AFFF system (1,2) – type 6, D7
- v No. of pressure sensors firewater ringmain (1 to 4)
- v No. of sensors to trip
- v Type of pressure sensor
- v Type of water deluge valve
- v Type of afff deluge valve
- v Type of pipework
- v Maintenance interval for pump tests
- v Maintenance interval for pump and ringmain tests
- v Maintenance interval for full tests

Deluge system

- ❖ Fault tree in excess of 450 gates and 420 basic events
- ❖ Fault tree converted to 17 BDD's
- ❖ In excess of 44000000000 design variations!!