An Introduction to Fault Tree Analysis

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

TOP Event

OR Gate

Intermediate Event

AND Gate

Fire Detection System Fails to Detect a Fire

Failure to Detect Smoke

Failure to Detect Heat

Water Deluge System Fails to Activate

Pump Fails to Start

Nozzles Blocked

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

UNAVAILABILITY

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Causal Relation</th>
</tr>
</thead>
<tbody>
<tr>
<td>![OR symbol]</td>
<td>OR</td>
<td>Output event occurs if at least one of the input events occur.</td>
</tr>
<tr>
<td>![AND symbol]</td>
<td>AND</td>
<td>Output event occurs if all input events occur.</td>
</tr>
<tr>
<td>![Vote symbol]</td>
<td>Vote</td>
<td>Output event occurs if at least $m$ of the input events occur.</td>
</tr>
</tbody>
</table>
# Fault Tree Symbols - Gates

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Causal Relation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="priority_and.png" alt="Priority AND symbol" /></td>
<td>Priority AND</td>
<td>Output event occurs if all input events occur in sequential order from left to right.</td>
</tr>
<tr>
<td><img src="not.png" alt="Not symbol" /></td>
<td>Not</td>
<td>Output event occurs if the input event does not occur.</td>
</tr>
</tbody>
</table>
## Fault Tree Symbols - Events

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Intermediate</strong></td>
<td>System or component event description.</td>
</tr>
<tr>
<td><img src="image1.png" alt="Symbol" /></td>
<td>Basic</td>
<td>Basic event for which failure and repair data is available. Usually represents a component failure.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Symbol" /></td>
<td>House</td>
<td>Represents definitely occurring or definitely not occurring events.</td>
</tr>
</tbody>
</table>
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

System Fails to Trip When Hazard Occurs

Sensor 1 Fails
Sensor 2 Fails
Sensor 3 Fails
Sensor 4 Fails

S1
S2
S3
S4
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.

Valve Fails to Close on Demand

Valve Type A
Fitted and Failed to Close

Valve Type B
Fitted and Failed to Close

Valve Type A
Fails to Close

Valve Type B
Fails to Close

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 \( V \cdot \overline{P} \) – 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

- Sonic detector (SD1)
- Concentration detector (CD1)
- Computer
- Alarm
- Operator
- Push button (BP)
- Relay
- Relay contacts
- Blowdown valve (V3)
- P/C (P/O) valve
- Isolation valve
- LEAK indicator

Diagram showing the components and their connections in a gas leak detection system.
## Gas Leak Detection System - Component Failure Modes

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

Leak detection system fails

V1 fails to close

V2 fails to close

V3 fails to open

V1 power to valves

V2 power to valves

V3 power to valves

1 1 1
Gas Leak Detection System - Solution

- Computer fails to issue trip signal
  - 4
    - Computer failure
    - Gas leak not detected
      - COMP
      - CD1
      - SD1
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

Minimal Cut Sets:
1. BD
2. ABC
Fault Tree Structures

Fault tree representation is not unique
Boolean Algebra

Variables

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

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

\[ TOP = B \cdot (A.D + \textcolor{red}{A.A.C} + B.D + C.D + \textcolor{blue}{B.A.C} + \textcolor{green}{C.A.C}) \]

Reduction Laws:

**Idempotent:**
\[ XX = X \quad X + X = X \]

**Absorption:**
\[ X + X.Y = X \]

\[ TOP = B \cdot (A.D + A.C + B.D + C.D) \]

\[ TOP = \textcolor{red}{B.A.D} + \textcolor{blue}{B.A.C} + \textcolor{green}{B.B.D} + \textcolor{blue}{B.C.D} \]

\[ TOP = \textcolor{blue}{B.A.C} + B.D\]
Fault Tree Analysis II

Top Event Probability

Component Failure Probability

Minimal Cut Set Failure Probability

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
- \( \lambda \) – failure rate

(Note: mean time to failure \( \mu = \frac{1}{\lambda} \) )
Maintenance Policy - Unscheduled Maintenance

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

STEADY-STATE

- As $t \to \infty$, $Q_\infty \to \frac{\lambda}{\lambda + \nu}$

$\lambda$ – failure rate $= \frac{1}{\mu}$

$\mu$ – mean time to failure

$\nu$ – repair rate $= \frac{1}{\tau}$

$\tau$ – mean time to repair
Maintenance Policy – Unscheduled Maintenance

Average Cycle

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

\( \mu \) – mean time to failure
\( \tau \) – mean time to repair

Note: \( \mu \gg \tau \)

\[ \therefore \mu + \tau \approx \mu \]

i.e. (failure rate) x (mean time to repair/restore)
Maintenance Policies - Scheduled Maintenance

- If: $\theta$ - time between inspections

- Time to restore = detection time + repair time

- $R_{AV}$ - average restoration time.

\[
R_{AV} = \frac{\theta}{2} + \tau
\]

\[
Q_{AV} = \lambda R_{AV}
\]

\[
= \lambda \left( \frac{\theta}{2} + \tau \right)
\]

$\theta \gg \tau$

\[
Q_{AV} \approx \frac{\lambda \theta}{2}
\]
Maintenance Policies - Scheduled Maintenance

- More accurately:

\[ Q_{AV} = \frac{1}{\theta} \int_{0}^{\theta} (1 - e^{-\lambda t}) \, dt \]

\[ = \frac{1}{\theta} \left[ t + \frac{e^{-\lambda t}}{\lambda} \right]_{0}^{\theta} \]

\[ = \frac{1}{\theta} \left( \theta + \frac{e^{-\lambda \theta}}{\lambda} \right) - \frac{1}{\theta} \left( 0 + \frac{e^{-0}}{\lambda} \right) \]

\[ = 1 - \frac{1 - e^{-\lambda \theta}}{\lambda \theta} \]
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 \( C_1 = A \quad C_2 = B.C \quad C_3 = B.D \quad C_4 = D.E.F \)

assume all failure probabilities = 0.1

\[
\]

\[
\]

\[
= [0.1 + 0.01 + 0.01 + 0.001] - [0.001 + 0.001 + 0.0001 + 0.001 + 0.0001] + [0.0001 + 0.000001 + 0.000001 + 0.000001] - [0.000001]
\]

\[
= [0.121] - [0.00321] + [0.000112] - [0.000001]
\]

\[
= 0.117901
\]

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 \(\approx 5 \times 10^9\)
    - No. of elements in third term \(\approx 1.7 \times 10^{14}\)
    - - 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

\[
P[\text{TOP}] = [P(C_1) + P(C_2) + P(C_3) + P(C_4)] - [P(C_1 \cdot C_2) + P(C_1 \cdot C_3) + P(C_1 \cdot C_4) + P(C_2 \cdot C_3) + P(C_2 \cdot C_4) + P(C_3 \cdot C_4)] + [P(C_1 \cdot C_2 \cdot C_3) + P(C_1 \cdot C_2 \cdot C_4) + P(C_1 \cdot C_3 \cdot C_4) + P(C_2 \cdot C_3 \cdot C_4)] - [P(C_1 \cdot C_2 \cdot C_3 \cdot C_4)]
\]

\[
= [0.121] - [0.00321] + [0.000112] - [0.000001]
\]

\[
= 0.117901
\]

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

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

If \( C_1 = A \), \( C_2 = B.C \), \( C_3 = B.D \), \( C_4 = D.E.F \)

all failure probabilities = 0.1

\[ = 1 - (1 - 0.1)(1-(0.1)^2)^2(1-(0.1)^3) \]

\[ = 0.118792 \]

\[ Q_{LOW} \leq Q_{SYS} \leq Q_{MCSU} \leq Q_{RE} \]

\[ 0.11779 \leq 0.117901 \leq 0.118792 \leq 0.121 \]
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
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.

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>STATE</th>
<th>PROBABILITY</th>
<th>CRITICAL FOR A ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series</td>
<td>(•,B)</td>
<td>q_B</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>(•,\overline{B})</td>
<td>1 - q_B</td>
<td>Yes</td>
</tr>
<tr>
<td>Parallel</td>
<td>(•,B)</td>
<td>q_B</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(•,\overline{B})</td>
<td>1 - q_B</td>
<td>No</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th></th>
<th>States</th>
<th>Critical for A?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>1</td>
<td>W</td>
<td>W</td>
</tr>
<tr>
<td>2</td>
<td>W</td>
<td>W</td>
</tr>
<tr>
<td>3</td>
<td>W</td>
<td>F</td>
</tr>
<tr>
<td>4</td>
<td>W</td>
<td>F</td>
</tr>
<tr>
<td>5</td>
<td>F</td>
<td>W</td>
</tr>
<tr>
<td>6</td>
<td>F</td>
<td>W</td>
</tr>
<tr>
<td>7</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>8</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

- \( I_A = \frac{5}{8} \)
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

\[ G_A = (1 - q_B)(1 - q_C)(1 - q_D) \]
\[ + (1 - q_B)(1 - q_C)q_D \]
\[ + (1 - q_B)(q_C)(1 - q_D) \]
\[ + (1 - q_B)q_C q_D + q_B(1 - q_C)(1 - q_D) \]
\[ = (1 - q_B) + q_B(1 - q_C)(1 - q_D) \]

\[ G_A = 0.944 \]

\[ q_A = q_C = 0.1 \]
\[ q_B = q_D = 0.2 \]

<table>
<thead>
<tr>
<th>States</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>Critical for A?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>W</td>
<td>W</td>
<td>F</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>W</td>
<td>F</td>
<td>W</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>W</td>
<td>F</td>
<td>F</td>
<td>Y</td>
</tr>
<tr>
<td>5</td>
<td>F</td>
<td>W</td>
<td>W</td>
<td>Y</td>
</tr>
<tr>
<td>6</td>
<td>F</td>
<td>W</td>
<td>F</td>
<td>N</td>
</tr>
<tr>
<td>7</td>
<td>F</td>
<td>F</td>
<td>W</td>
<td>N</td>
</tr>
<tr>
<td>8</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>N</td>
</tr>
</tbody>
</table>
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

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

i.e. $G_i(q)$ 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

\[ I_{FV_A} = \frac{q_A}{Q_{SYS}} = \frac{0.1}{0.1504} = 0.6649 \]
\[ I_{FV_B} = \frac{q_B(q_C + q_D - q_C q_D)}{Q_{SYS}} = \frac{0.2(0.1 + 0.2 - 0.02)}{0.1504} = 0.3723 \]
\[ I_{FV_C} = \frac{q_C q_B}{Q_{SYS}} = \frac{0.02}{0.1504} = 0.1330 \]
\[ I_{FV_D} = \frac{q_D q_B}{Q_{SYS}} = \frac{0.04}{0.1504} = 0.2660 \]
## Importance Measures Summary

<table>
<thead>
<tr>
<th>Component</th>
<th>Structural</th>
<th>Birnbaum</th>
<th>Fussell-Vesely</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.625</td>
<td>0.944</td>
<td>0.6649</td>
</tr>
<tr>
<td>B</td>
<td>0.375</td>
<td>0.252</td>
<td>0.3723</td>
</tr>
<tr>
<td>C</td>
<td>0.125</td>
<td>0.144</td>
<td>0.1330</td>
</tr>
<tr>
<td>D</td>
<td>0.125</td>
<td>0.162</td>
<td>0.2660</td>
</tr>
</tbody>
</table>
System Failure Intensity

- $w_{SYS}(t)$ is the system failure intensity at time $t$.

- This can be determined from:

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

- 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

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

Unrevealed failures R1/PB/SW2/L2 –

inspection interval = 4380 hours
Tank Level Control System – FT(1)

- Tank Overfills
- Pump Motor energised too long
- Relay R2 contacts closed too long
- Relay R2 contacts fail closed
- Relay R2 remains energised

Diagram:

- GEN2
- PUMP (P)
- RELAY 2
- RELAY 1
- SWITCH 1
- SWITCH 2
- PUSH BUTTON (PB)
- POWER SUPPLY (GEN1)
- TANK (T)
- OUTLET VALVE (VAL)
Tank Level Control System – FT(2)

- Relay R2 remains energised
- Power across the PB/R1 contacts section
- Switch SW1 remains closed
- Relay R1 contacts closed
- Switch SW2
- Push button (PB)
- Relay 1
- Relay 2
- Switch 1
- Switch 2
- Power supply (GEN1)
- Gen 2
- Pump (P)
- Tank (T)
- Control trip
- Outlet valve (VAL)
Tank Level Control System – FT(2)

- R1 remains energised
- SW2 remains closed
- Switch 2 fails closed
- Level sensor 2 fails

---

- GEN2
- PUMP (P)
- RELAY 2
- RELAY 1
- SWITCH 1
- SWITCH 2
- PUSH BUTTON (PB)
- POWER SUPPLY (GEN1)
- TANK (T)
- OUTLET VALVE (VAL)
- CONTROL L1
- TRIP L2

- R2 remains
- SW2 remains
- Switch 2 fails
- Level sensor 2 fails

---

- R1
- L2
- SW2
Tank Level Control System - MCS

Minimal Cut Sets

<table>
<thead>
<tr>
<th>#</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R2</td>
</tr>
<tr>
<td>2</td>
<td>SW1, PB</td>
</tr>
<tr>
<td>3</td>
<td>SW1, R1</td>
</tr>
<tr>
<td>4</td>
<td>SW1, SW2</td>
</tr>
<tr>
<td>5</td>
<td>SW1, L2</td>
</tr>
<tr>
<td>6</td>
<td>L1, PB</td>
</tr>
<tr>
<td>7</td>
<td>L1, R1</td>
</tr>
<tr>
<td>8</td>
<td>L1, SW2</td>
</tr>
<tr>
<td>9</td>
<td>L1, R1</td>
</tr>
</tbody>
</table>
Tank Level Control System

Top Event Probability = $7.5 \times 10^{-4}$
Top Event Frequency = $7.72 \times 10^{-5}$ per hour

<table>
<thead>
<tr>
<th>Rank</th>
<th>Component</th>
<th>Fussell Vesely</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R2</td>
<td>0.781</td>
</tr>
<tr>
<td>2</td>
<td>SW1</td>
<td>0.215</td>
</tr>
<tr>
<td>3</td>
<td>R1</td>
<td>0.080</td>
</tr>
<tr>
<td>4</td>
<td>SW2</td>
<td>0.068</td>
</tr>
<tr>
<td>5</td>
<td>PB</td>
<td>0.067</td>
</tr>
<tr>
<td>6</td>
<td>L1</td>
<td>0.004</td>
</tr>
<tr>
<td>7</td>
<td>L2</td>
<td>0.003</td>
</tr>
</tbody>
</table>
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