THE UNIVERSITY OF WARWICK

WMG

An Introduction to Fault Tree Analysis (FTA)

Dr Jane Marshall

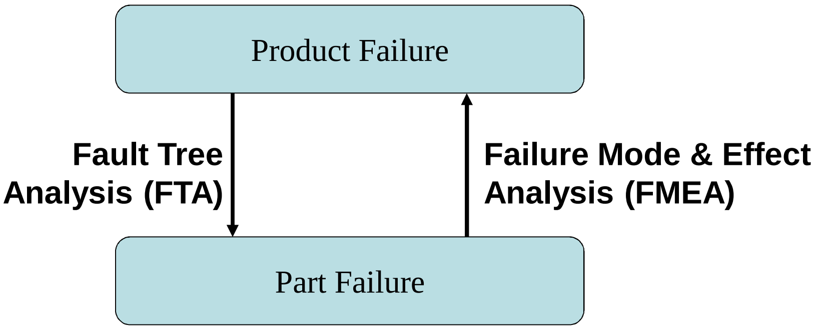
Product Excellence using 6 Sigma Module

WMG

Objectives

– Understand purpose of FTA
– Understand & apply rules of FTA
– Analyse a simple system using FTA
– Understand & apply rules of Boolean algebra

Relationship between FMEA & FTA



PEUSS 2011/2012 FTA Page 3

Fault Tree Analysis

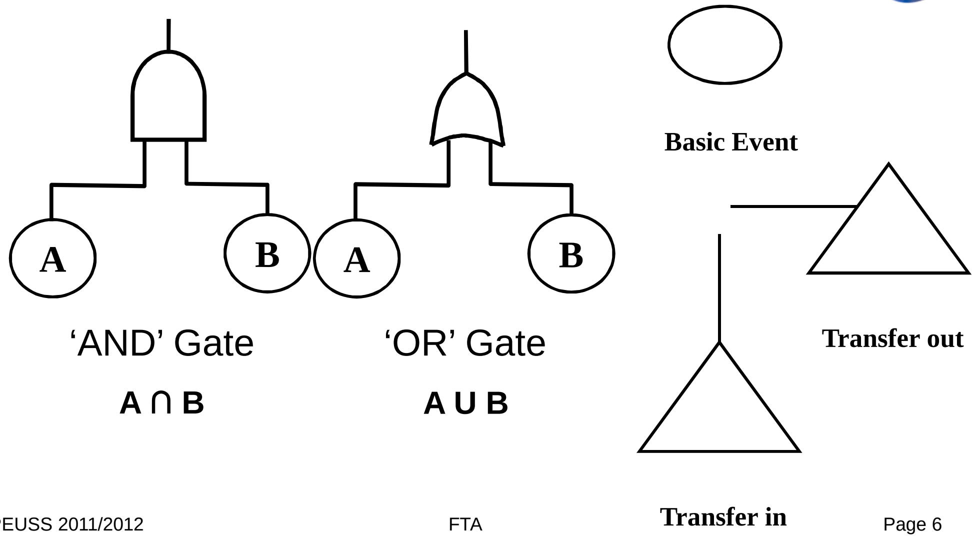
- Is a systematic method of System Analysis
- Examines System from Top → Down
- Provides graphical symbols for ease of understanding
- Incorporates mathematical tools to focus on critical areas

PEUSS 2011/2012 FTA Page 4

Fault tree analysis (FTA)

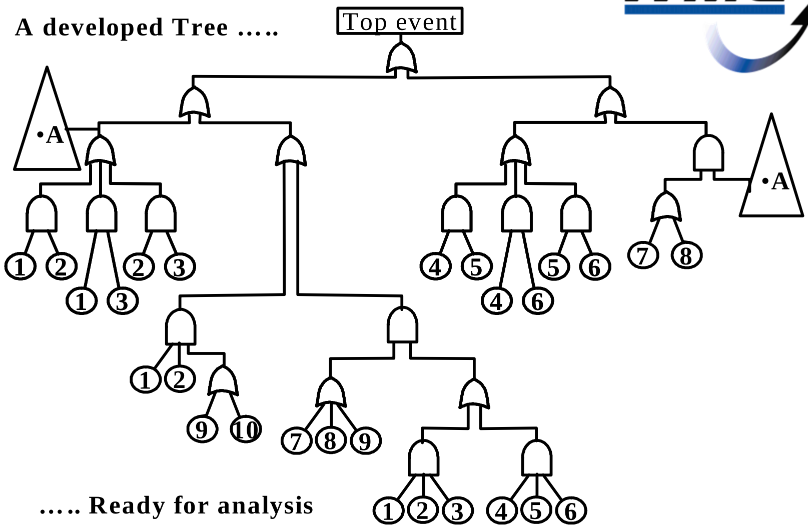
- Key elements:
  - Gates represent the outcome
  - Events represent input to the gates
- FTA is used to:
  - investigate potential faults;
  - its modes and causes;
  - and to quantify their contribution to system unreliability in the course of product design.

Symbols



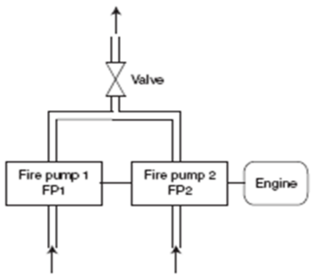
Example Fault Tree

A developed Tree …..



….. Ready for analysis

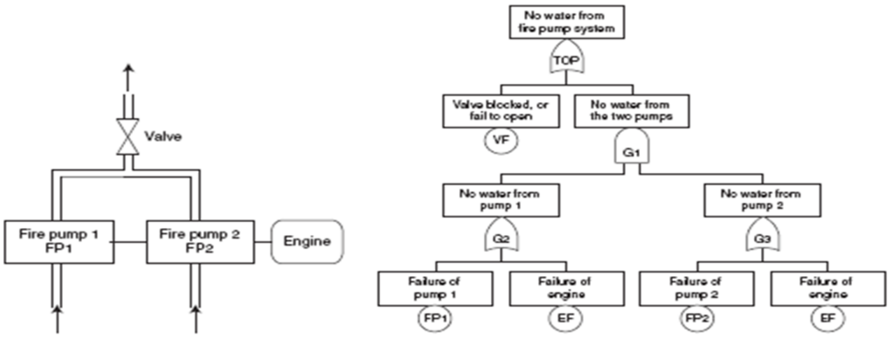
Example: redundant fire pumps



TOP event = No water from fire water system
Causes for TOP event:
VF = Valve failure
G1 = No output from any of the fire pumps
G2 = No water from FP1 G3 = No water from FP2
FP1 = failure of FP1
EF = Failure of engine
FP2 = Failure of FP2

Source: http://www.ntnu.no/ross/srt/slides/fta.pdf

Example: redundant fire pumps



Source: http://www.ntnu.no/ross/srt/slides/fta.pdf

Example

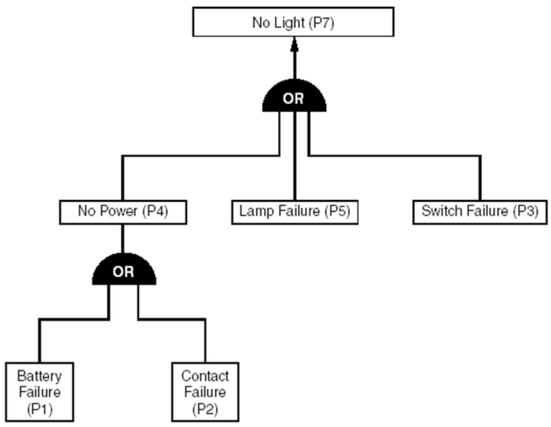
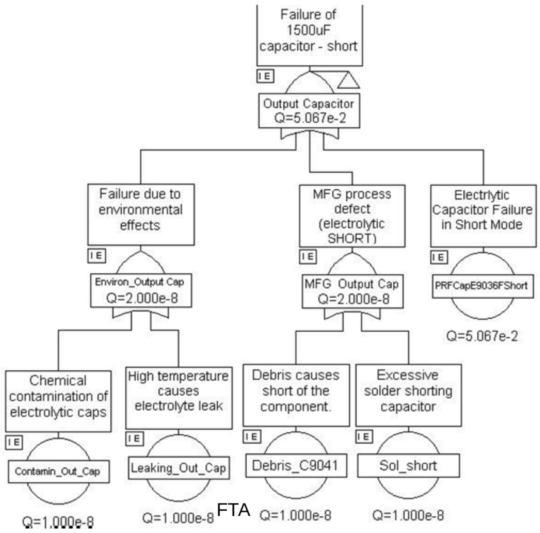


Figure 11.5 FTA of the vehicle headlamp.

Example



Methodology (Preliminary Analysis)

- Set System Boundaries
- Understand Chosen System
- Define Top Events

Methodology (Rules)

1. The “Immediate, Necessary & Sufficient” Rule
2. The “Clear Statement” Rule
3. The “No Miracles” Rule
4. The “Complete-the-Gate” Rule
5. The “No Gate-to-Gate” Rule
6. The “Component or System Fault?” Rule

Methodology (Rules - 1) – immediate, necessary and sufficient cause

Immediate

Closest in space, time and derivation of the event above

Necessary

There is no redundancy in the statement or gate linkage
The event above could not result from a sub set of the causal

Sufficient

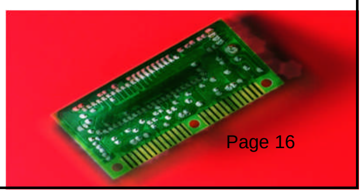
The events will, in all circumstances and at all times, cause the event above

Methodology (Rules - 2) – The clear statement rule

Write event box statements clearly, stating precisely what the event is and when it occurs

Methodology (Rules - 3) – The ‘component or systems fault’ rule

If the answer to the question:
“Can this fault consist of a component failure?” is **Yes**,
– Classify the event as a “State of component fault”
If the answer is **No**,
– Classify the event as a “state of system fault”



Methodology (Rules - 4) – no miracles rule

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

Methodology (Rules - 5) – the complete gate rule

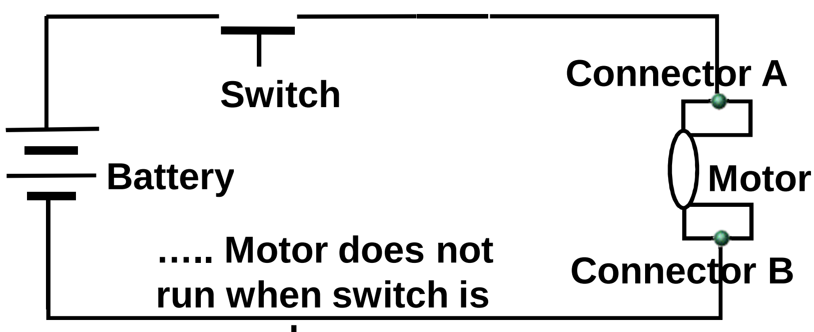
All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken

Methodology (Rules - 6) no gate to gate rule

Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates

PEUSS 2011/2012 FTA Page 19

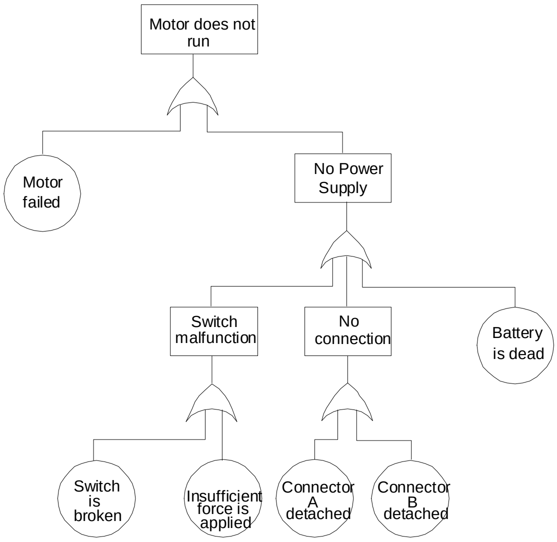
Fault Tree Example



….. Motor does not run when switch is pressed

PEUSS 2011/2012 FTA Page 20

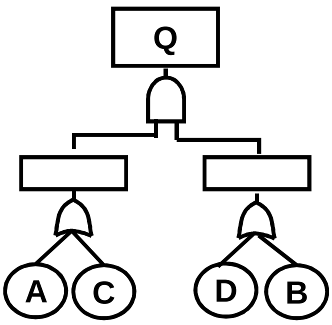
Fault Tree Example



top event …..

motor does not run
when switch is pressed

Qualitative Analysis (Combination of Gates)



Algebraic representation is:

$Q = (A \cup C) \cap (D \cup B)$

$\cup$ or gate $\cap$ and gate

Qualitative Analysis (Cut Sets)

A listing taken directly from the Fault Tree of the events, ALL of which must occur to cause the TOP Event to happen

Qualitative Analysis (Cut Sets)

Algebraic representation is:

$Q = (A \cup C) \cap (D \cup B)$

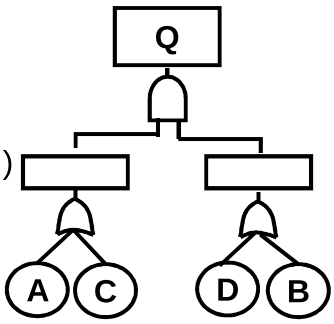
which can be re-written as:

$Q = (A \cap D) \cup (A \cap B) \cup (C \cap D) \cup (C \cap B)$

$Q = (A \bullet D) + (A \bullet B) + (C \bullet D) + (C \bullet B)$

… which is a listing of Groupings ...each of which is a Cut Set

AD AB CD BC



Qualitative Analysis (Minimal Cut Sets)

A listing, derived from the Fault Tree Cut Sets and reduced by Boolean Algebra, which is the smallest list of events that is necessary to cause the Top Event to happen

Qualitative Analysis (Boolean Algebra)

Commutative laws

$A \cap B = B \cap A$

$A \cup B = B \cup A$

Associative laws

$A \cap (B \cap C) = (A \cap B) \cap C$

$A \cup (B \cup C) = (A \cup B) \cup C$

Distributive laws

$A \cap (B \cup C) = A \cap B \cup A \cap C$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Commutative laws

$A \bullet B = B \bullet A$

$A + B = B + A$

Associative laws

$A \bullet (B \bullet C) = (A \bullet B) \bullet C$

$A + (B + C) = (A + B) + C$

Distributive laws

$A \bullet (B + C) = A \bullet B + A \bullet C$

$A + (B \bullet C) = (A + B) \bullet (A + C)$

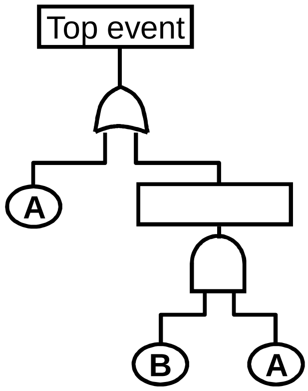
Qualitative Analysis (Boolean Reduction)

Idempotent laws

A • A = A
A +A = A

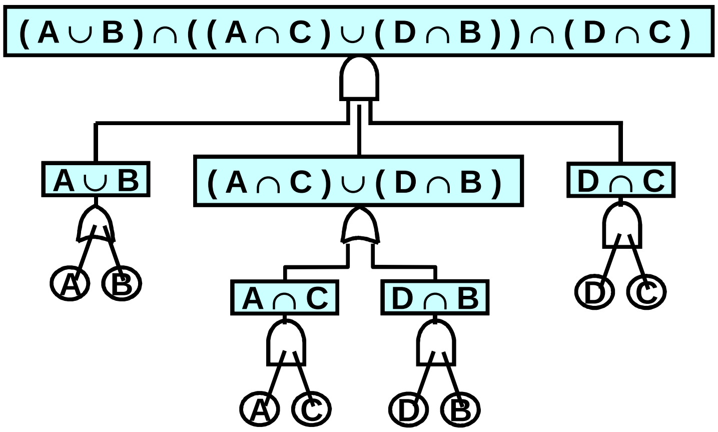
Absorption law

A + (A • B) = A



Exercise in deriving Cut Sets

.....



Solution .....

$(A \cup B) \cap ((A \cap C) \cup (D \cap B)) \cap (D \cap C)$

$\equiv (A + B) \bullet (A \bullet C + D \bullet B) \bullet D \bullet C$

$\equiv AACDC + ADBDC + BACDC + BDBDC$

$\equiv ACD + ABCD + ABCD + BCD$

$\equiv ACD + BCD$

Minimal Cut Sets …… ACD, BCD

Design Analysis of Minimal Cut Sets

A Cut Set comprising several components is less likely to fail than one containing a single component

Hint .....

AND Gates at the top of the Fault Tree increase the number of components in a Cut Set

OR Gates increase the number of Cut Sets, but often lead to single component Sets

Benefits and limitations

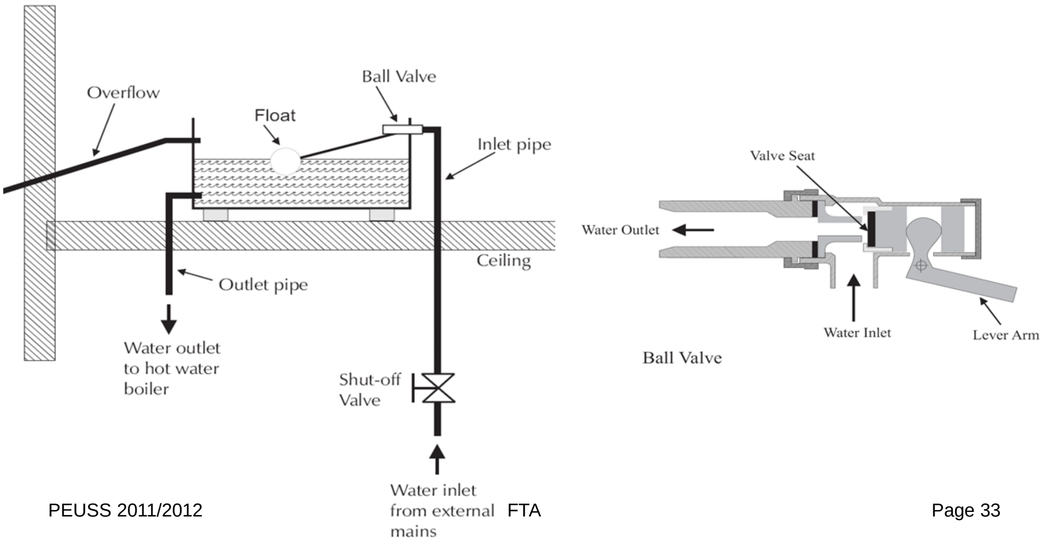
- Prepared in early stages of a design and further developed in detail concurrently with design development.
- Identifies and records systematically the logical fault paths from a specific effect, to the prime causes
- Allows easy conversion to probability measures
- But may lead to very large trees if the analysis is extended in depth.
- Depends on skill of analyst
- Difficult to apply to systems with partial success
- Can be costly in time & effort

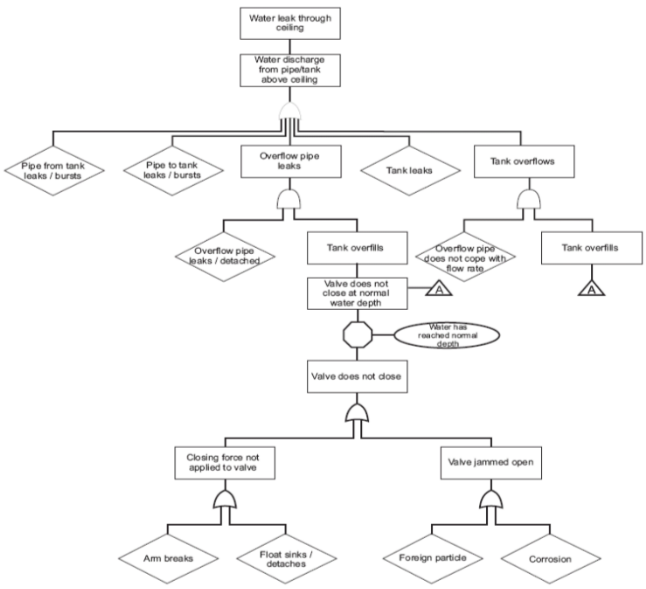
Software

- Software packages available for reliability tools
- Relex
- Relia soft
- others

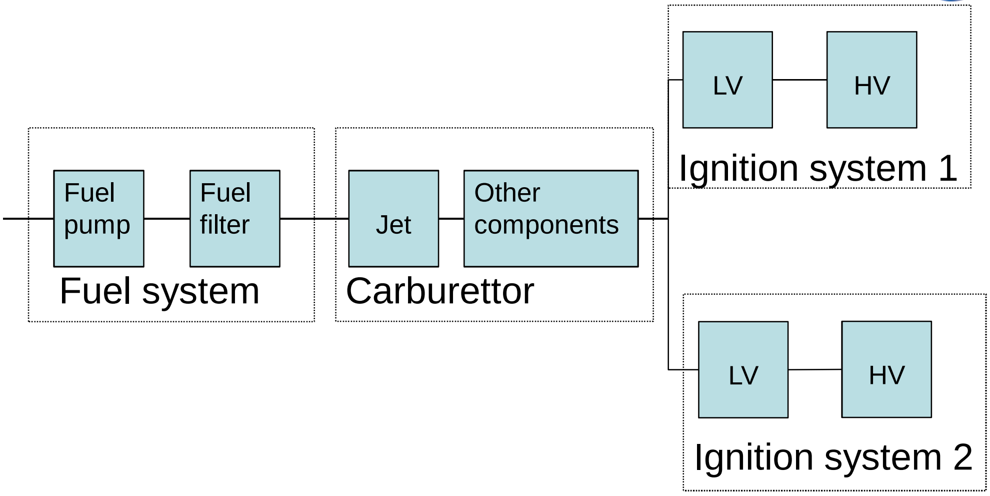
Exercise 1

TOP EVENT = WATER LEAKS THROUGH CEILING

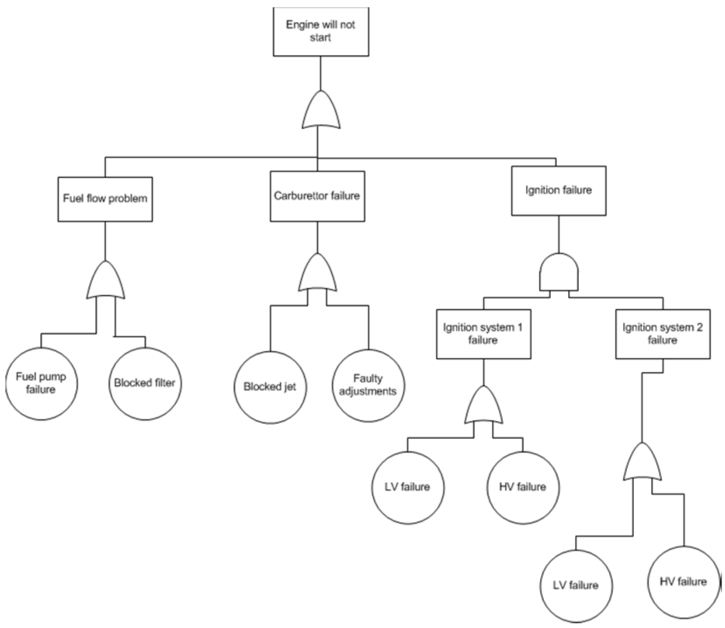




RBD of an engine



PEUSS 2011/2012 FTA Page 35



PEUSS 2011/2012 FTA Page 36