ENG
ENGINEERING DEPARTMENT

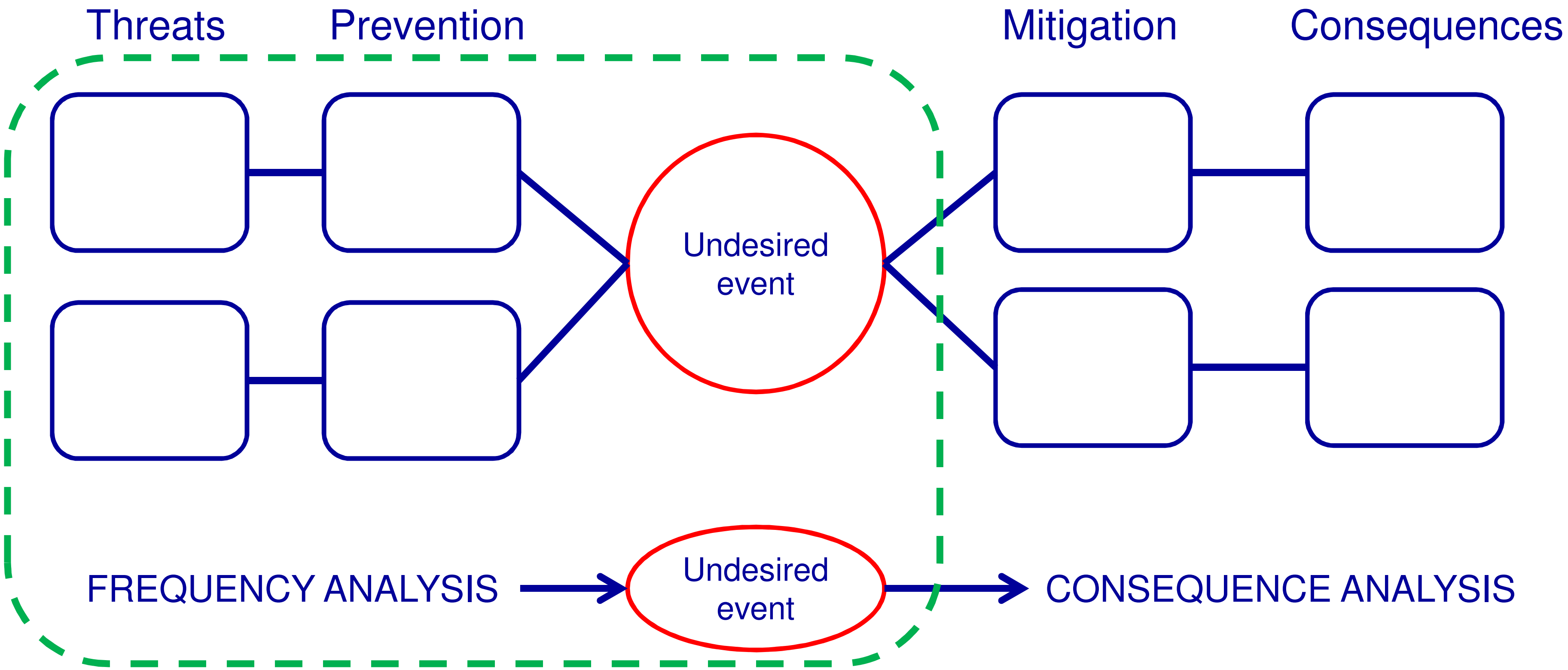
LANCASTER
UNIVERSITY

Science and Technology
at Lancaster

FTA – EXAMPLES

DR. RICHARD DAWSON

What is fault tree analysis?



An FTA could be thought of as a quantitative version of the left-hand side of a bowtie diagram

Fault tree analysis is a systematic deductive backwards (or top down) looking logic which starts with an undesired event, resolved to intermediate events and finally to initiating events.

Why FTA?

- Exhaustively identify the causes of a failure
- Identify weaknesses in a system
- Assess a proposed design for its reliability or safety
- Identify effects of human errors
- Prioritise contributors to failure
- Identify effective upgrades to a system
- Quantify the failure probability and contributors
- Optimise test and maintenance

At the end of the process you should have a really good understanding of your system which is a good place to be

Role of FTA in design

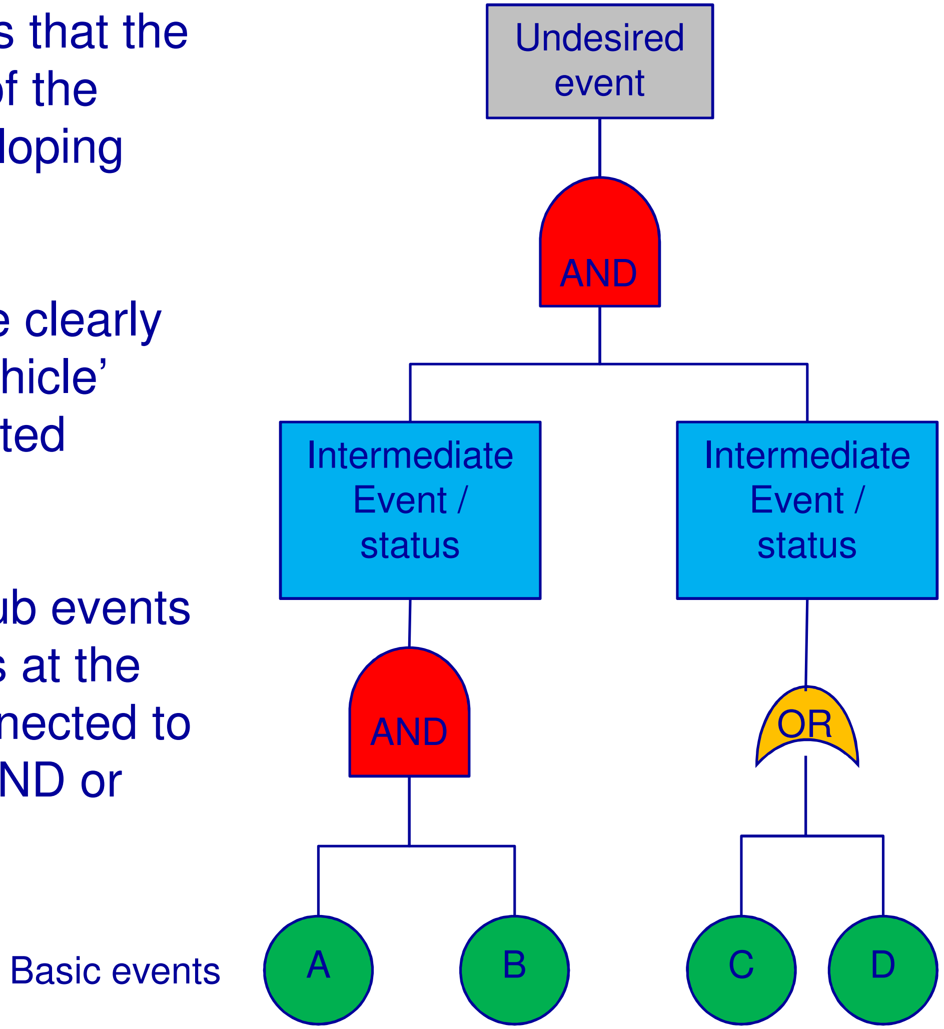
- Aid design feature selection
- Quantify design failure probability
- Evaluate potential design changes
- Optimise resources in providing a safe system
- Explore trade-offs in design
  - Alternative capabilities
  - Alternative redundancies
- Model system failures in qualitative risk assessments to satisfy regulators

A fault tree

Successful fault tree analysis requires that the engineer has a good understanding of the system (or subsystem) they are developing the analysis for.

The ‘top’ undesired event needs to be clearly defined in such as ‘car hits parked vehicle’ which would be suitable for a automated parking assist system.

The tree propagates down through sub events to the basic failures or primary events at the bottom. Events and are logically connected to the undesired event though usually AND or OR gates.



Definitions

Primary Event: An initiating fault event that requires no further development

Intermediate Event: An intermediate event is a failure resulting from the logical interaction of primary failures.

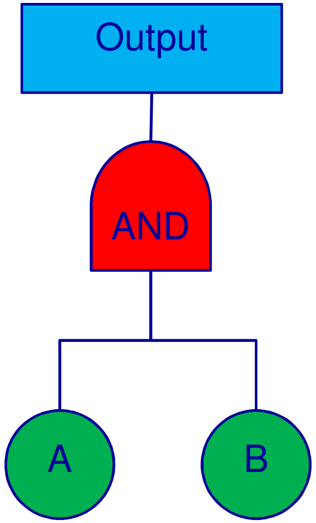
Top Event: It is an undesired event for the system under consideration and occurs as a result of occurrence of several intermediate events. Several combinations of primary failures lead to the event.

Branch: Development of any fault event results in a branch of a fault tree. A branch is complete only when all events in the branch have been developed to the level of primary failures.

AND and OR gates

AND: In a tabular form (truth table)

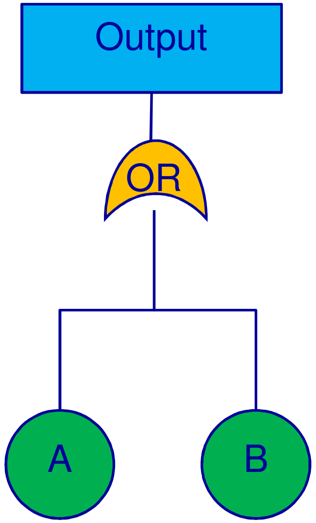
A/B	1	0
1	Output = 1	Output = 0
0	Output = 0	Output = 0



In terms of probabilities provided A and B are independent inputs the $P(Output) = P(A) \cdot P(B)$. Hence if $P(A)$ were 0.00125 and $P(B)$ were 0.0004 then $P(Output)$ would be $0.00125 \times 0.004 = 5 \times 10^{-6}$

OR: In a tabular form (truth table)

A/B	1	0
1	Output = 1	Output = 1
0	Output = 1	Output = 0

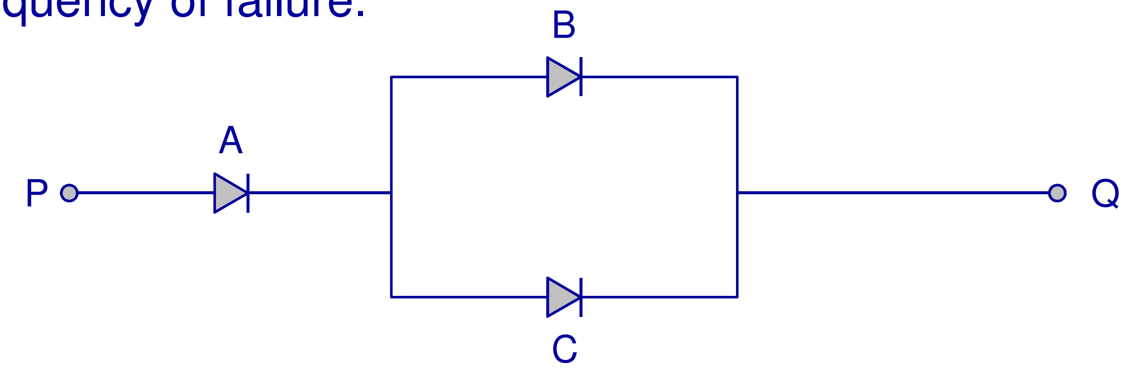


In terms of probabilities provided A and B are independent (and mutually exclusive) inputs the $P(Output) = P(A) + P(B)$. Hence if $P(A)$ were 0.00125 and $P(B)$ were 0.0004 then $P(Output)$ would be $0.00125 + 0.004 = 5.25 \times 10^{-3}$

A simple tree structure

Useful procedure for building simple fault trees.

1. Define the undesired system event
2. Working down state precisely what each fault is and when it occurs – these can be Intermediate events / failure modes that lead to the top event
   - An AND or OR gate will be below this
   - Unless we get to a basic event for the tree (or a link into another sub tree)
3. Identify if the faults which are required to generate this intermediate event propagating down the branches until basic events are reached with a well defined frequency of failure.



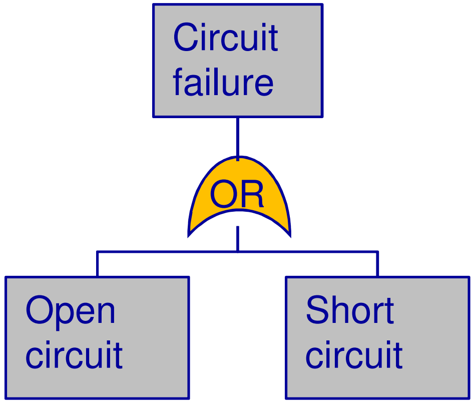
Consider the simple diode circuit above. How can this fail? Can we draw a simple fault tree?

Building fault tree

What can be define as the undesired event?

In this case it would be circuit failure, this can occur as either a short failure (becomes effectively a conductor between P and Q) **OR** as a open circuit failure between P and Q

Hence

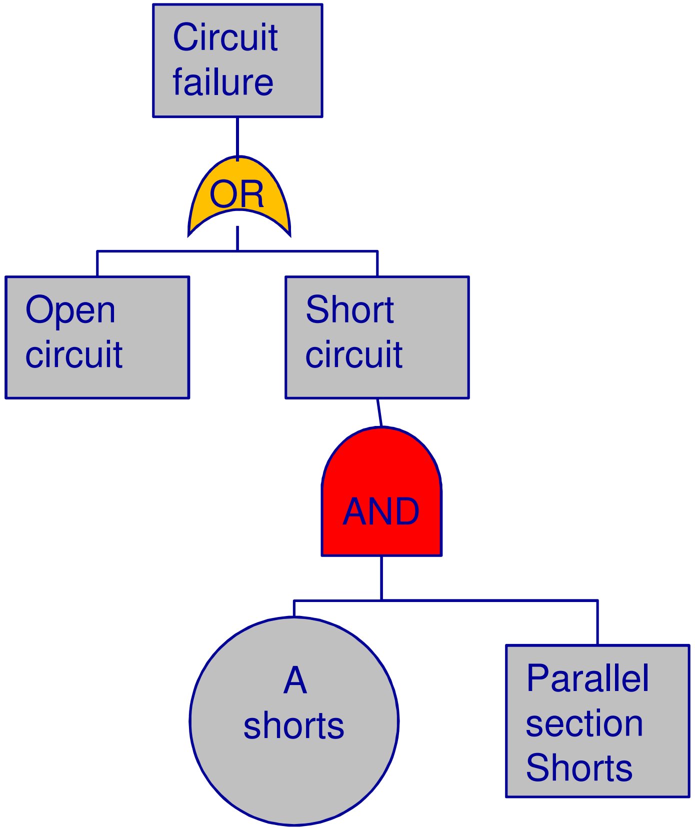


Let’s go down a branch. Starting with ‘short circuit’

A short circuit requires the failure of diode A **AND** the failure of the parallel section

Building fault tree

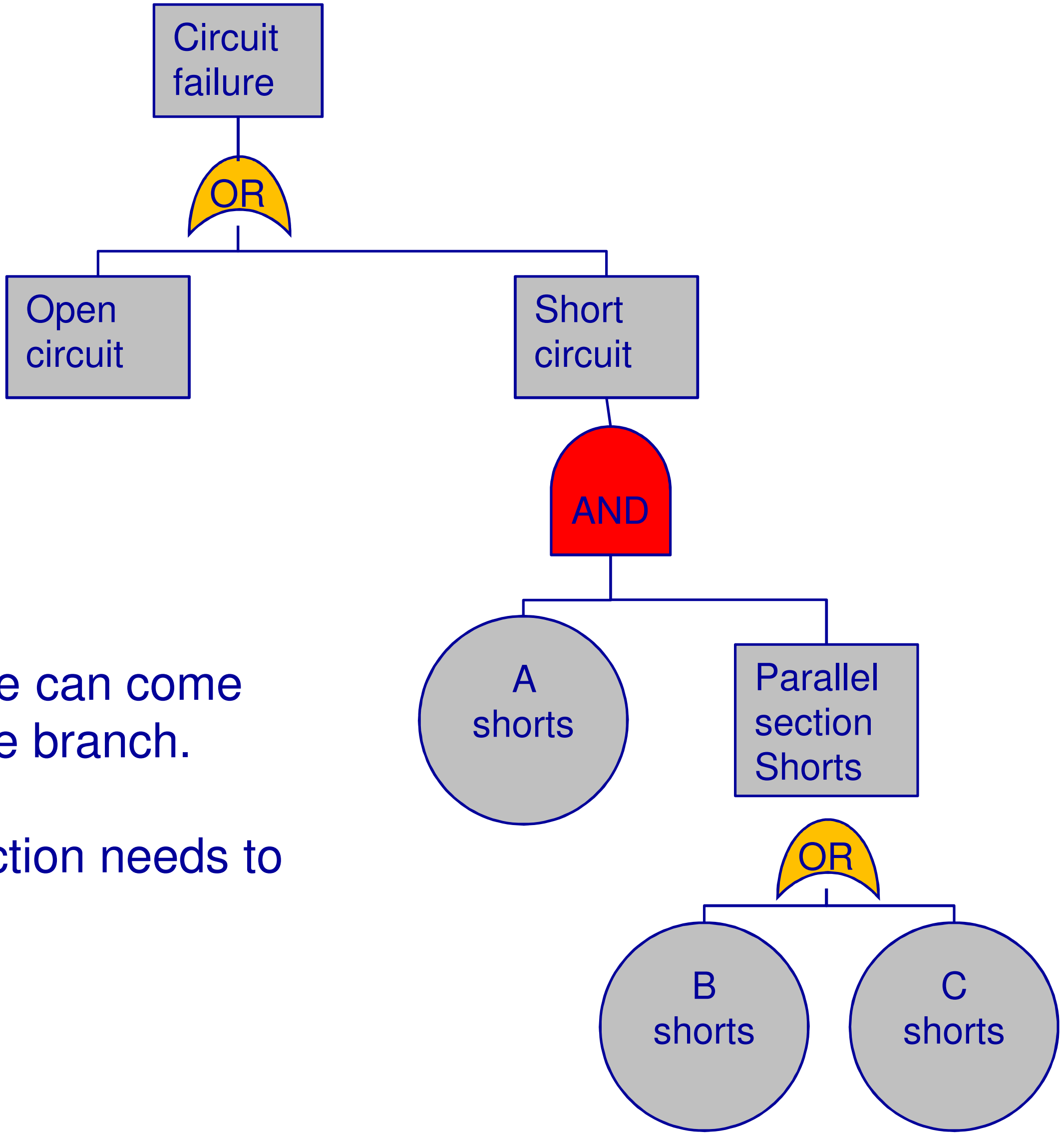
Hence



Continue down the branch from parallel section shorts. For this intermediate event to occur then either B **OR** C can short.

Building a fault tree

Hence

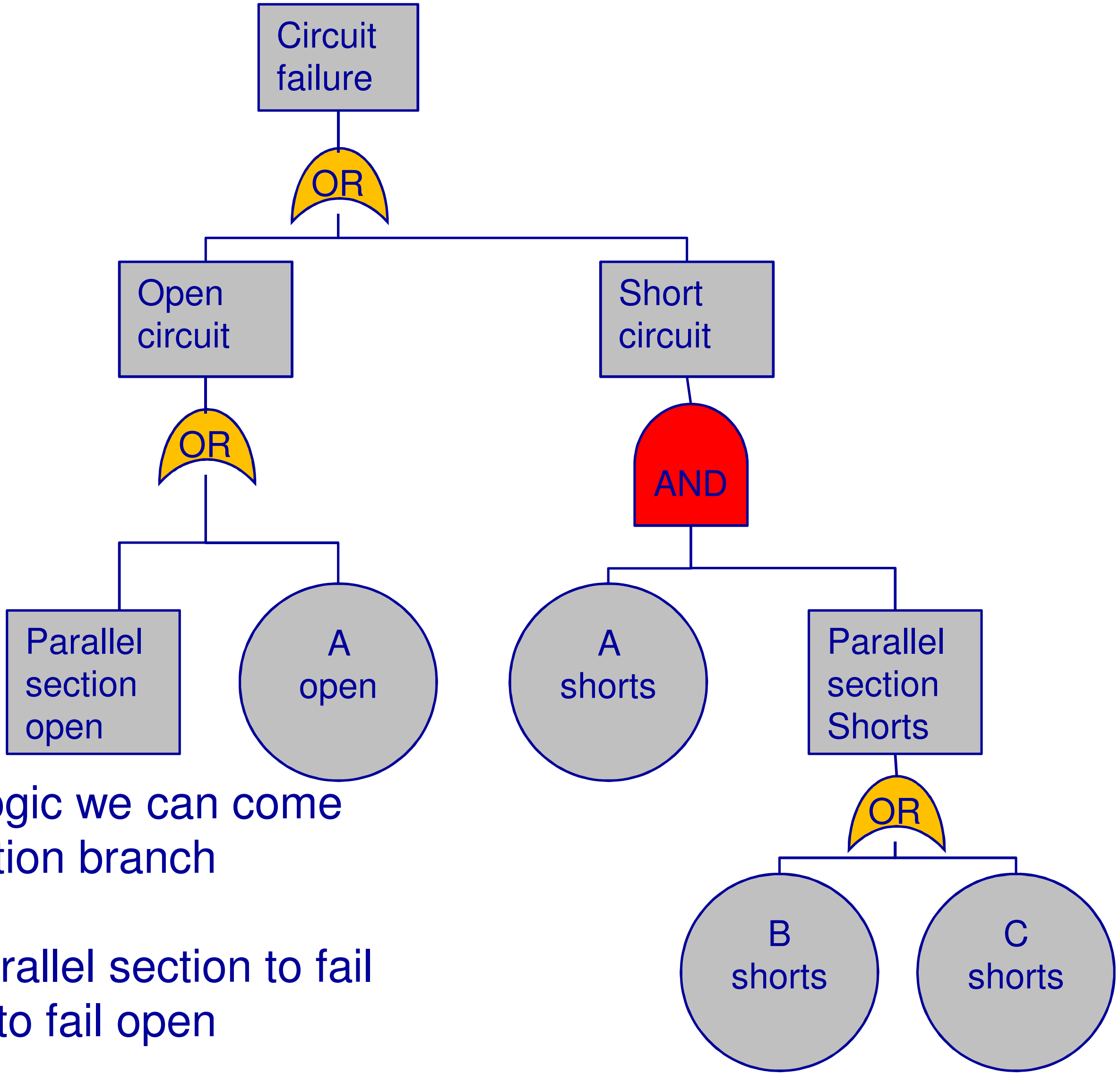


Following the same logic we can come down the open circuit failure branch.

Either A **OR** the parallel section needs to fail open

Building a fault tree

Hence

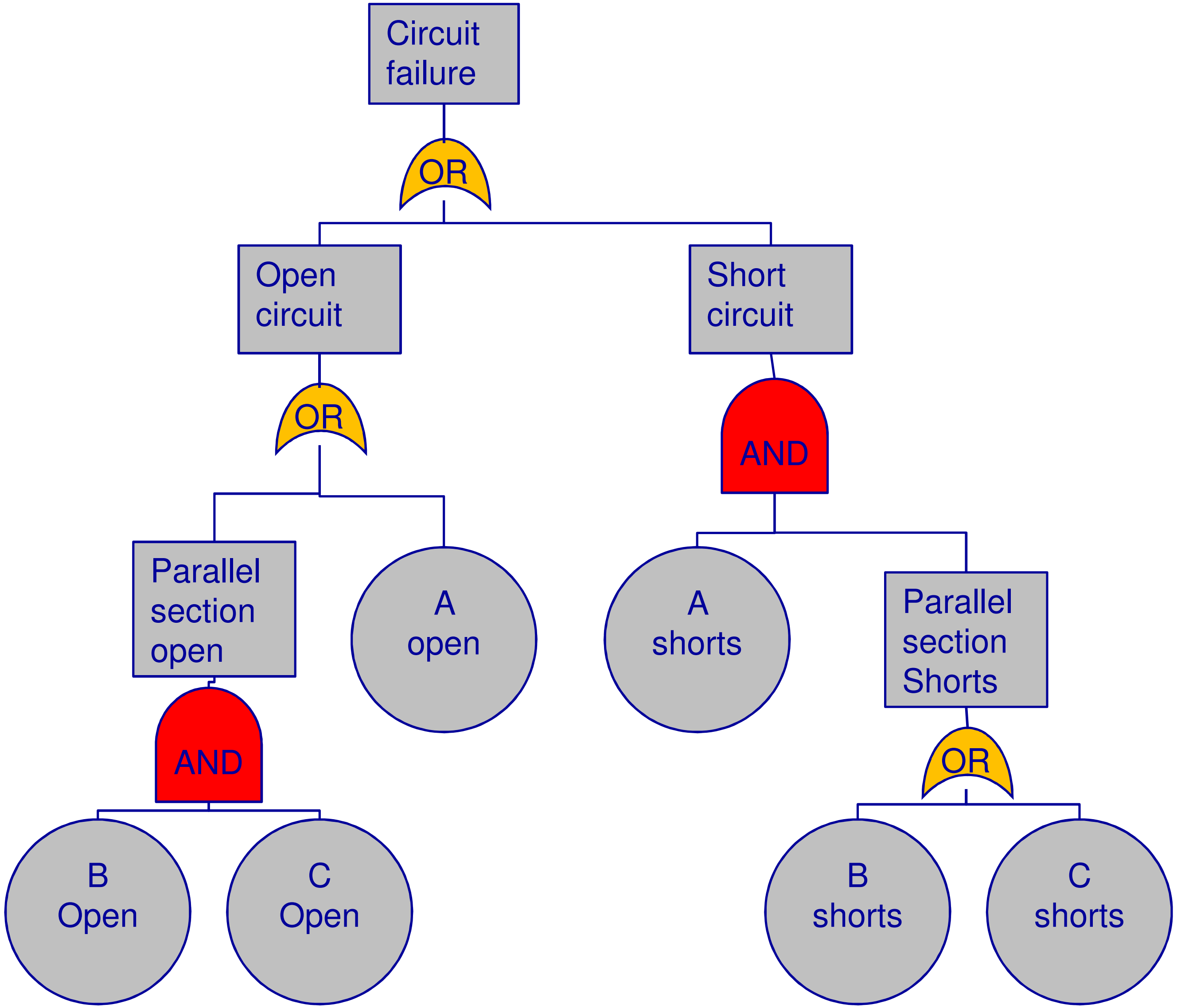


Following the same logic we can come down the parallel section branch

In this case for the parallel section to fail open C **AND** D need to fail open

Building a fault tree

Hence



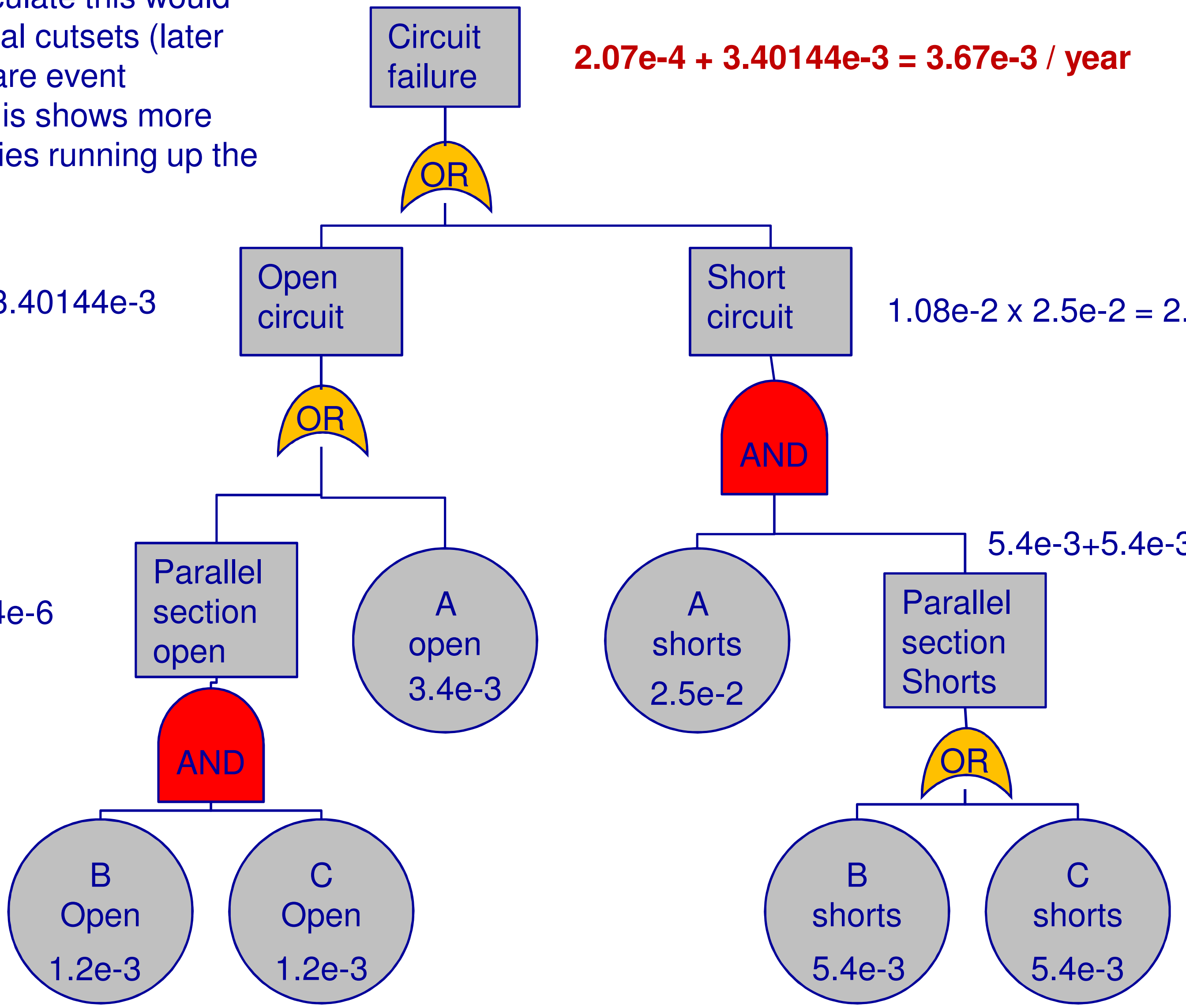
Probability of top / undesired event

Basic data: Probability A fails closed is 2.5e-2 / year and open is 3.4e-3 / year, B and C are smaller devices and identical. Probability these fail closed is 5.4e-3 / year and open is 1.2e-3 / year

Armed with this basic data we can calculate through the gates the intermediate and finally the top / undesired event as probability of failure / year.

Calculating probability

The best way to calculate this would be to sum the minimal cutsets (later slides) making the rare event approximation but this shows more clearly the probabilities running up the branches



2.07e-4 + 3.40144e-3 = 3.67e-3 / year

1.44e-6 + 3.4e-3 = 3.40144e-3 (really 3.4e-3)

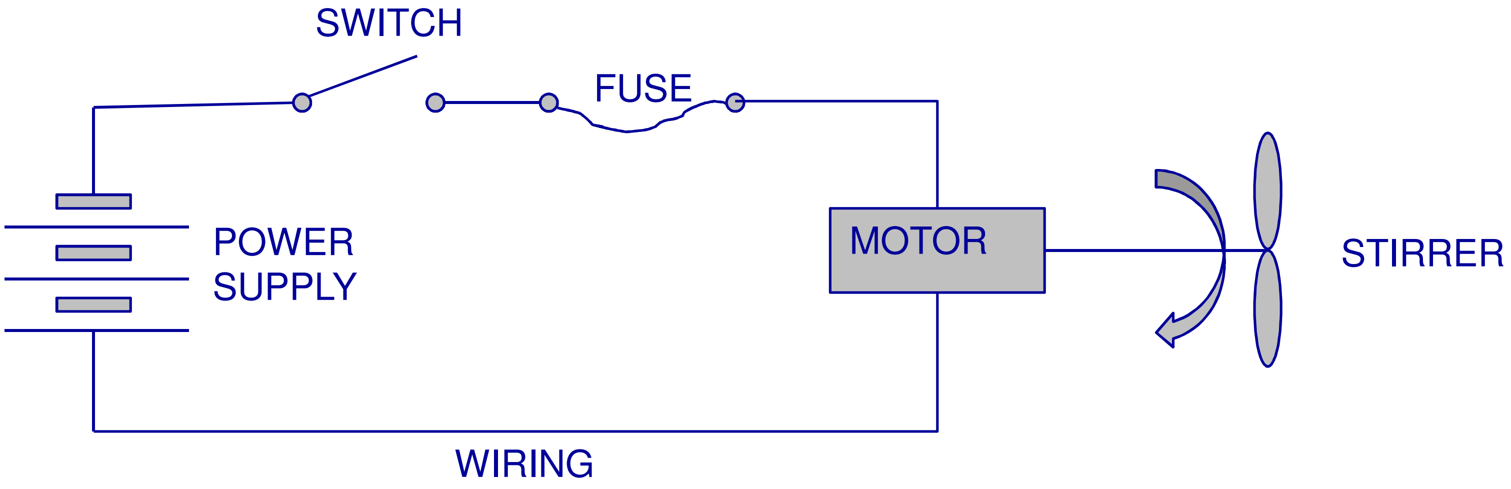
1.08e-2 x 2.5e-2 = 2.7e-04

5.4e-3+5.4e-3=1.08e-2

1.2e-3x1.2e-3= 1.44e-6

Another example

As a slightly more complex example: Suppose an process in a chemical plant requires an operator to turn on a overhead stirrer. The circuit for the system could be described as:



Can we draw a fault tree for the undesired event for this system? (There could be many undesired events)

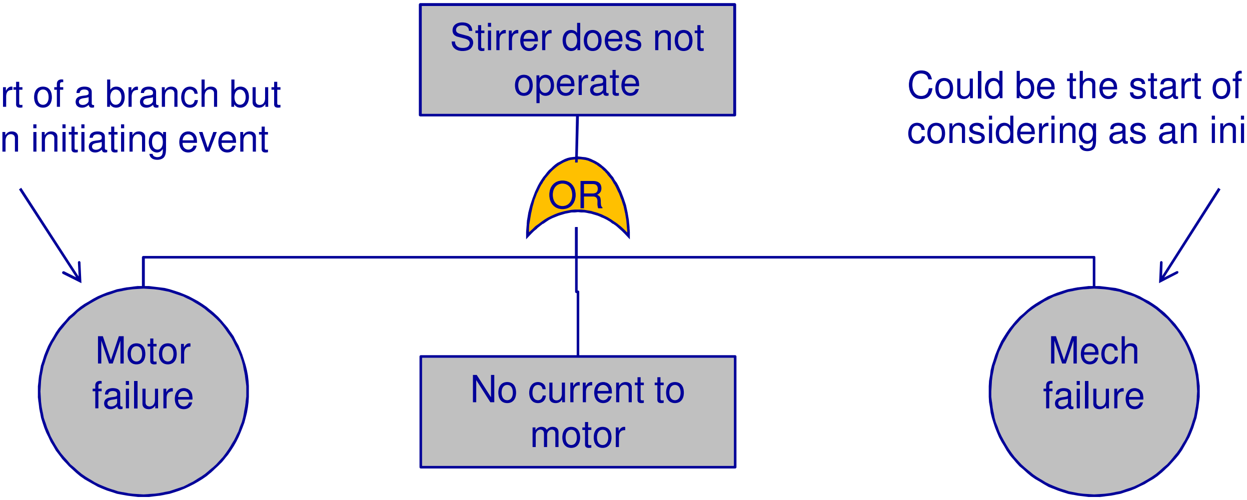
Starting the fault tree

Undesired event: Stirrer does not operate

Stirrer does not operate

Why might this occur?

We could come up with the following reasons: Motor failure **OR** No current to motor **OR** mechanical interference (many others could be considered)

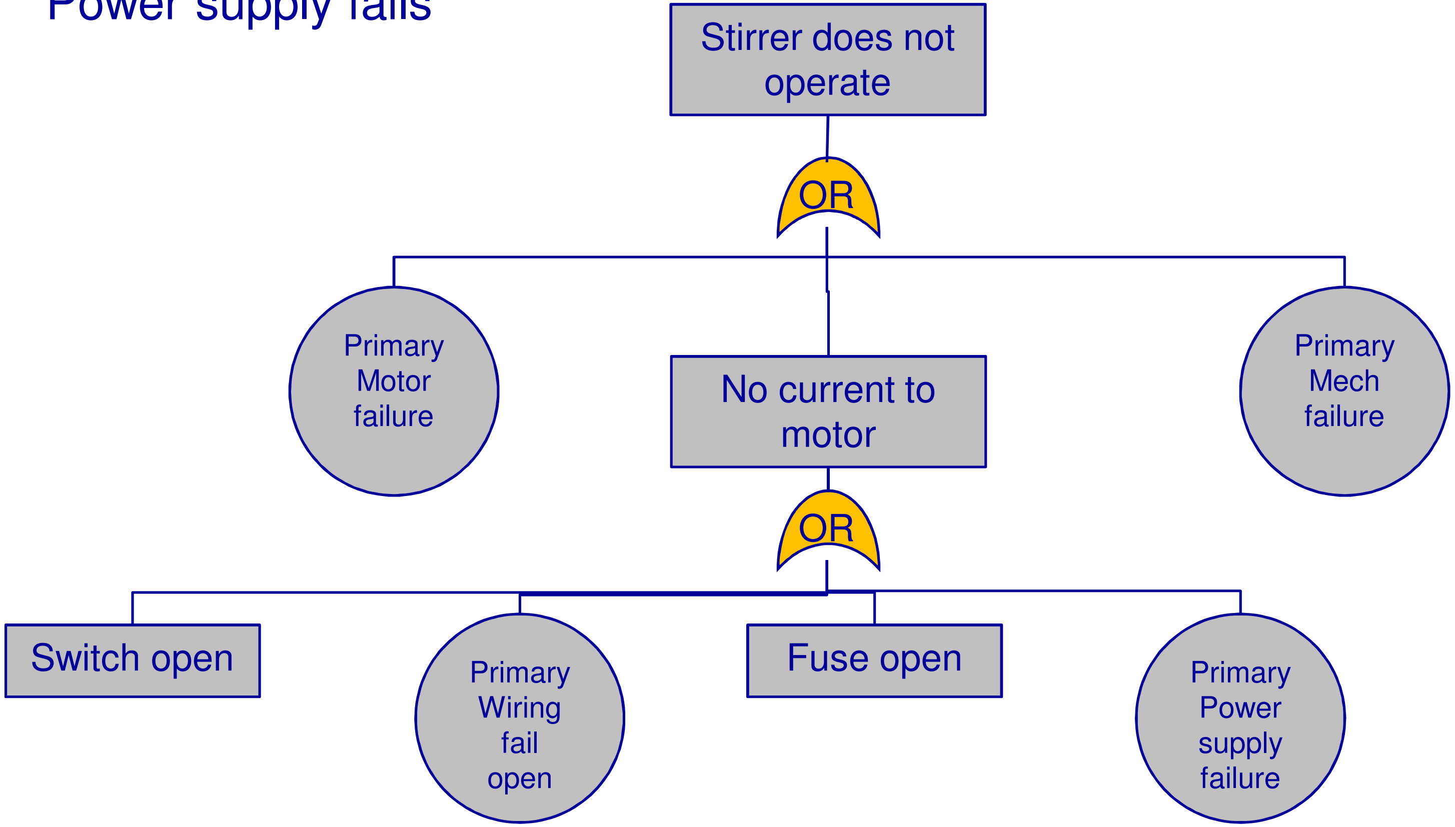


Could be the start of a branch but considering as an initiating event

Could be the start of a branch but considering as an initiating event

Extending down the tree

Continuing down the ‘No current to motor’ event, we could make a guess that this could be due to: Switch open **OR** Wiring fail open **OR** Fuse fails open **OR** Power supply fails



Extending down the tree component failure types

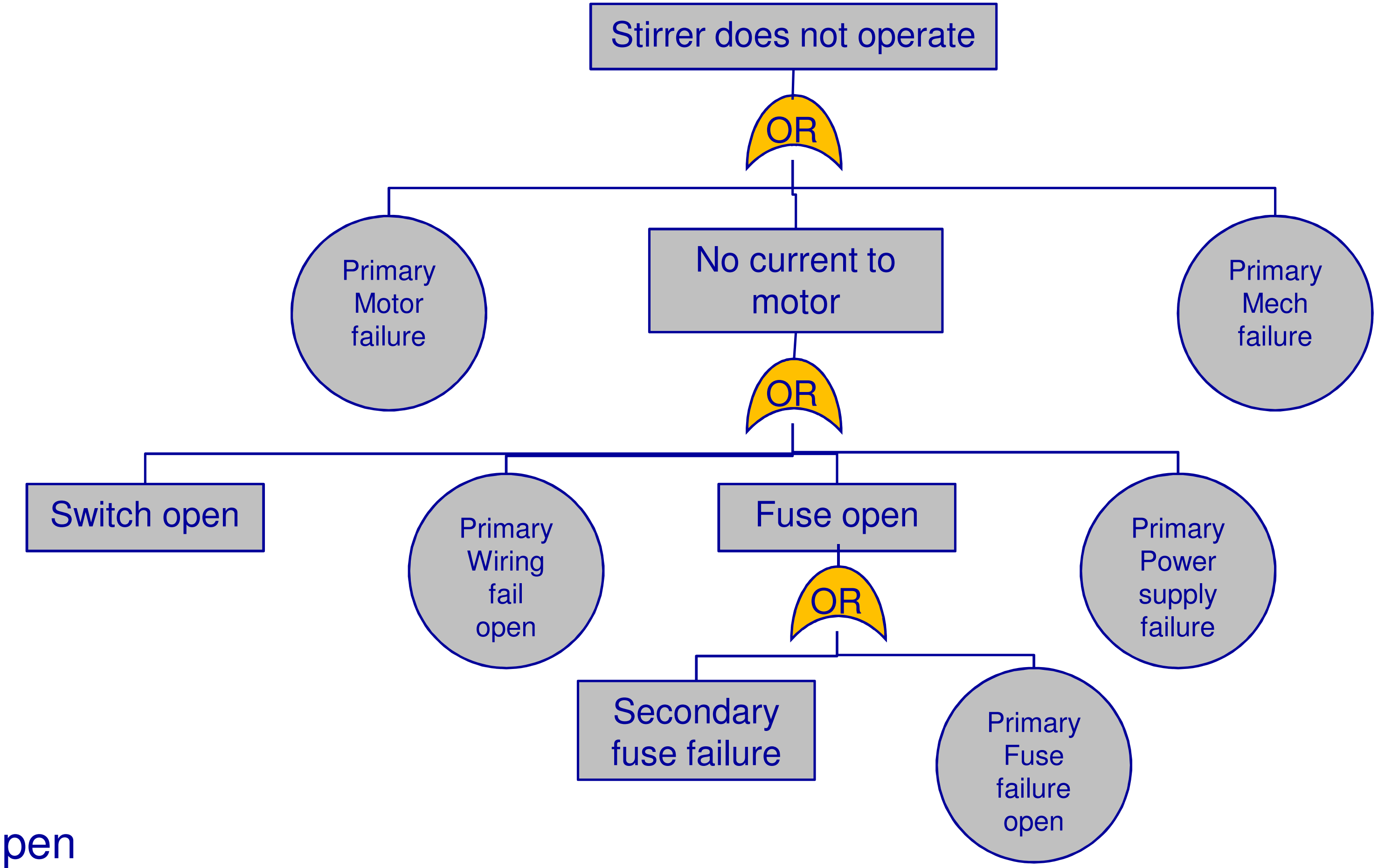
If we follow the fuse failure:

Components can ‘fail’ in three ways and we can ask ourselves which of the three are important here.
Primary: A primary failure is the inherent failure of the system element, such as some internal component problem. As such the this failure can be considered to be independent of external influences and is an initiating event.
Secondary: A secondary failure is due to external forces on the component (requires good system knowledge) and as such is an intermediate event.
Command: A command failure is effectively a desired event at the wrong time due to a chain of events (command path faults)

In the case of the fuse we can see that two failure types are possible.

Primary: Something wrong with the way the fuse was made so it fails
Secondary: Fuse fails due to overcurrent.

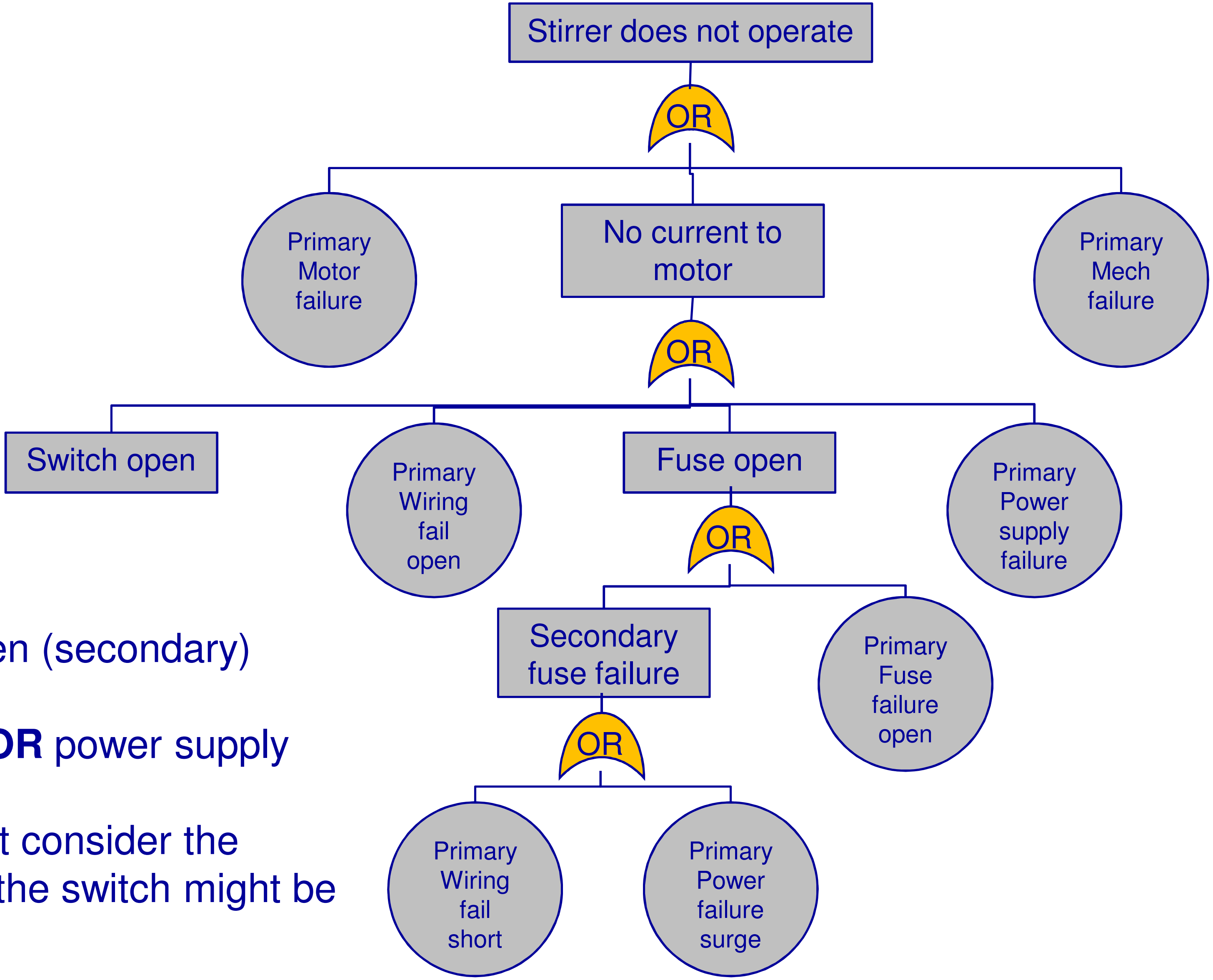
Extending down the tree



Fuse fails open

In this case this can be a primary **OR** secondary failure

Extending down the tree



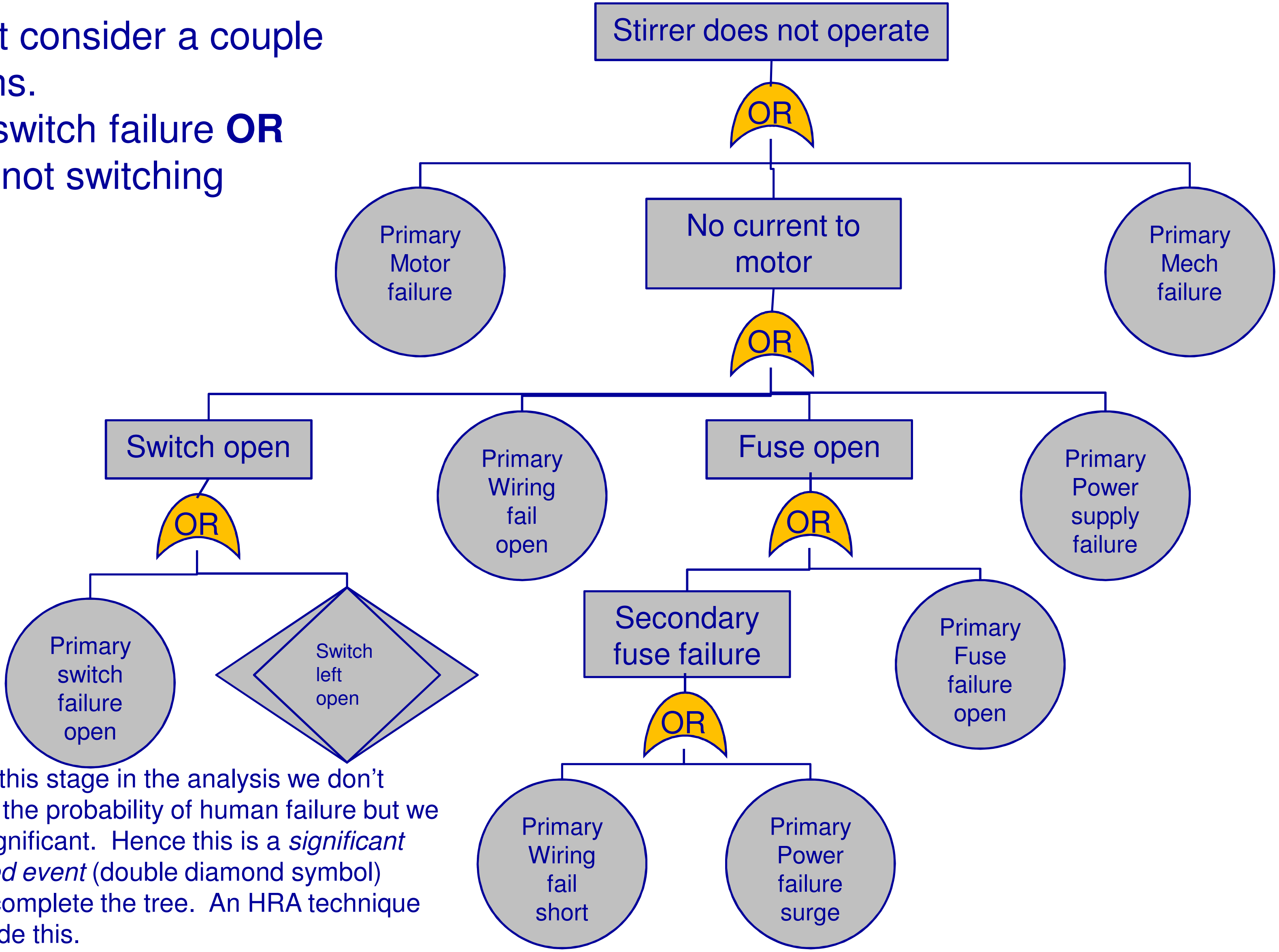
Fuse fails open (secondary)

Wiring short **OR** power supply surge

Now we might consider the reasons why the switch might be open

Extending down the tree

We might consider a couple of reasons.
Primary switch failure **OR** operator not switching switch



Perhaps at this stage in the analysis we don't understand the probability of human failure but we think it is significant. Hence this is a *significant undeveloped event* (double diamond symbol) needed to complete the tree. An HRA technique would provide this.

Cutsets and Minimal cutset

The previous examples were quite simple (so they fit easily) but hopefully it illustrates the basic principle.

CUTSET: A failure combination which causes the top undesired event to occur. Hence *A shorts, B shorts* is a cutset from the first diode circuit example.

MINIMAL CUTSET: A cutset from which you cannot remove an event and still cause the top undesired event to occur.

The difference between cutsets and minimal cutsets becomes more apparent when the same events occur in more than one branch of the tree

A minimal cutset list can be very useful as it can give us a quick route to approximating the likelihood of the top event.

The ‘rare event’ approximation states we can estimate the top event probability as being the sum of the probabilities of all of the minimal cutsets.

(This is assuming that although the cutsets are independent they can happen at the same time but this probability is sufficiently low)

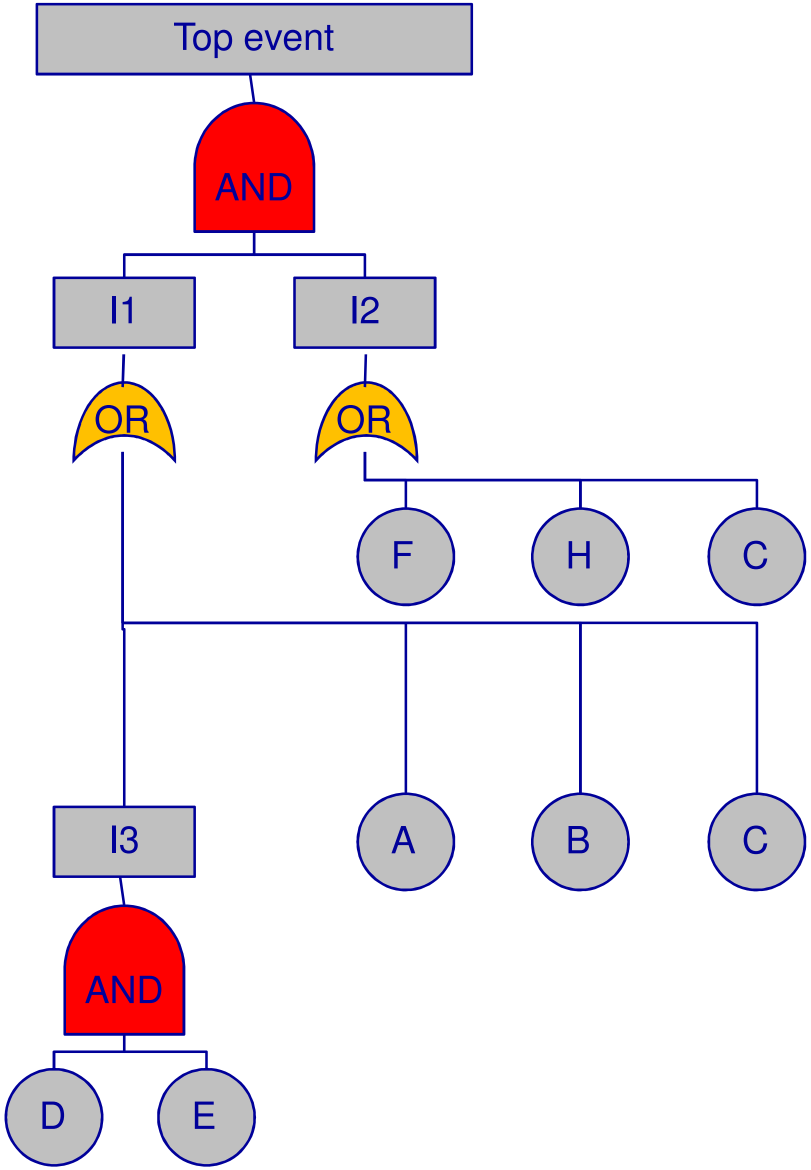
Minimal Cutsets Example

Find the minimal cutset list and so the approximate probability of the top event occuring/

BASIC METHOD: Draw out the cutset list starting form the top of the tree and gradually replacing intermediate events with events lower in the tree till expressed completely as initiating events.

Next go thought the list eliminating combinations where you can still remove one or more initiating event and the top event still occurs.

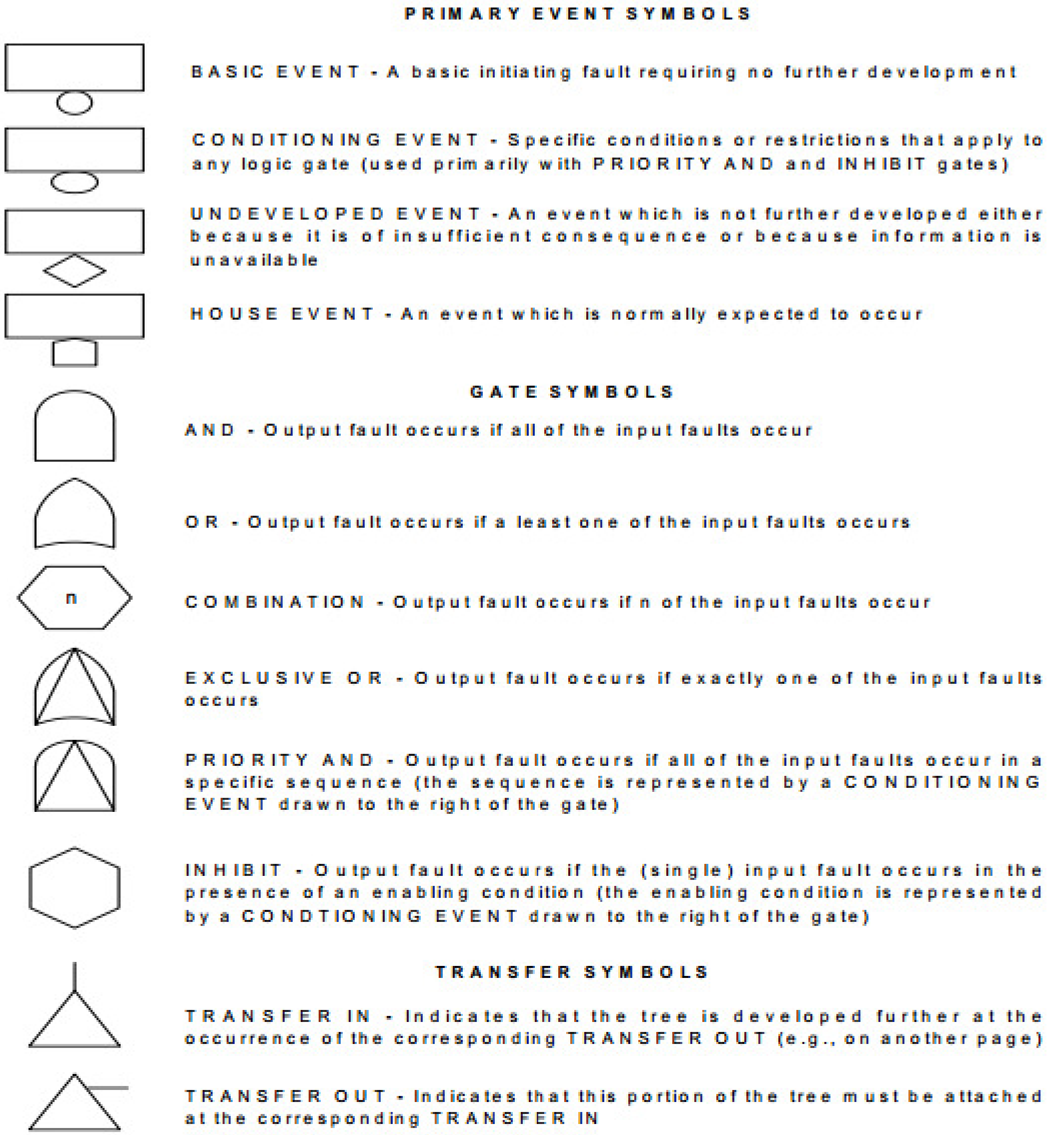
Add up the probability of the minimal cutsets to find the approximation of the top event. E.g. P(D).P(E).P(F) + P(D).P(E).P(H) + ………This assumes that is unlikely that more than one minimal cutset will be active at the same time (rare event approximation)



Important considerations

- Most FTA would be conducted in specialist software
  - Beware hidden errors in the complexity
  - Does the answer make sense, review against knowledge base?
  - Check minimal cutsets
- Write clear statements of events in boxes (be concise)
- Complete the gates
- Don’t directly connect gates
- Don’t assume a fault will cause abnormal conditions preventing a failure from propagating (no miracles rule!)
- Beware of over complicating the tree with inconsequential events (requires caution) – e.g. developing OR gates where one input dominates.

Extended symbols



PRIMARY EVENT SYMBOLS

BASIC EVENT - A basic initiating fault requiring no further development

CONDITIONING EVENT - Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT - An event which is not further developed either because it is of insufficient consequence or because information is unavailable

HOUSE EVENT - An event which is normally expected to occur

GATE SYMBOLS

AND - Output fault occurs if all of the input faults occur

OR - Output fault occurs if a least one of the input faults occurs

COMBINATION - Output fault occurs if n of the input faults occur

EXCLUSIVE OR - Output fault occurs if exactly one of the input faults occurs

PRIORITY AND - Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT - Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDTIONING EVENT drawn to the right of the gate)

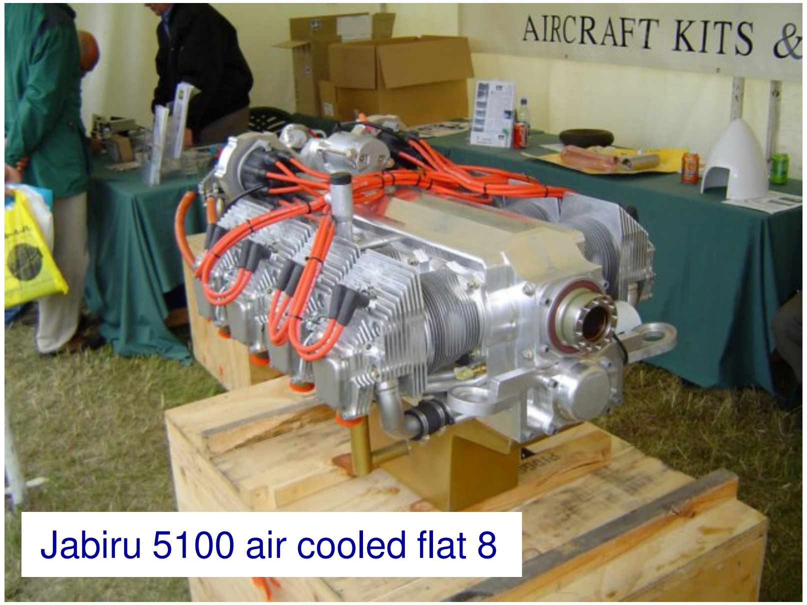
TRANSFER SYMBOLS

TRANSFER IN - Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)

TRANSFER OUT - Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

Source - NASA

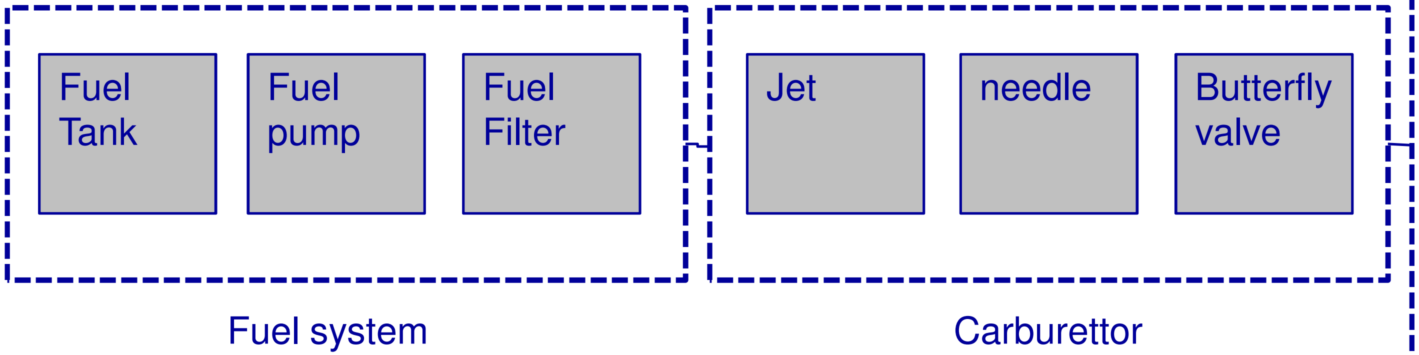
Some simple none quantitative examples

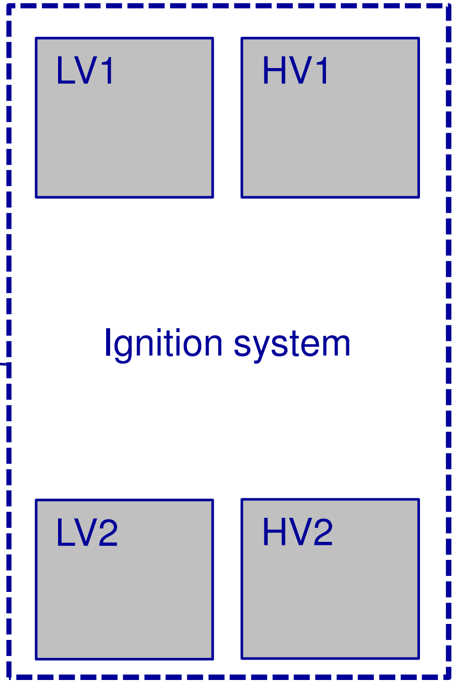


Jabiru 5100 air cooled flat 8

A dual ignition system aero engine giving redundancy in ignition system and some combustion efficiency benefits

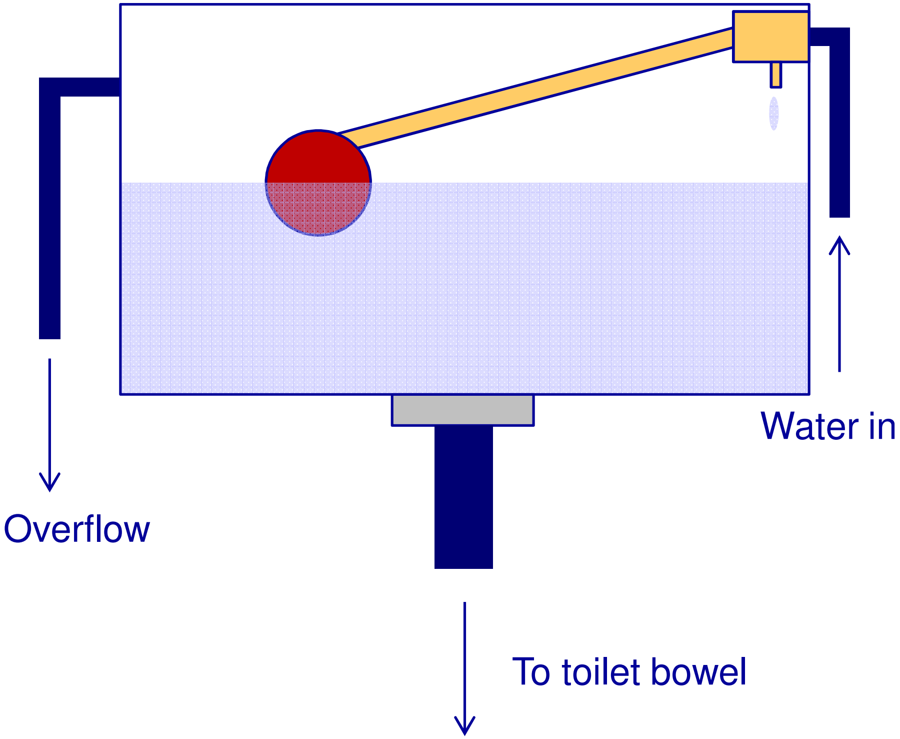
Draw a simple FTA based on the fuelling and ignition block diagram. With the top event of ‘engine fails to start’

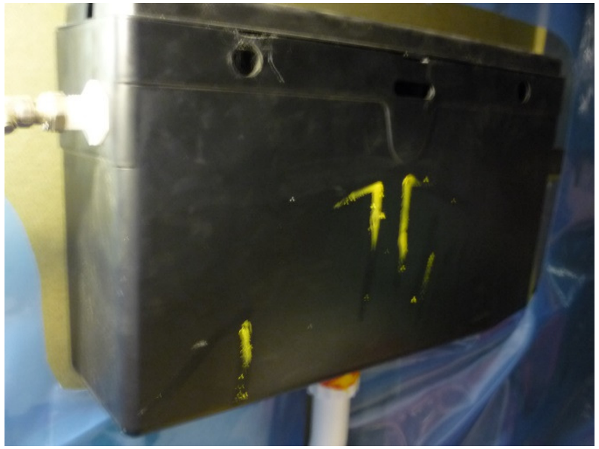




Loft conversion ensuite

Draw a simple fault tree with the top event ‘water discharge into roof space’ for toilet cistern in my roof space





Mission time example

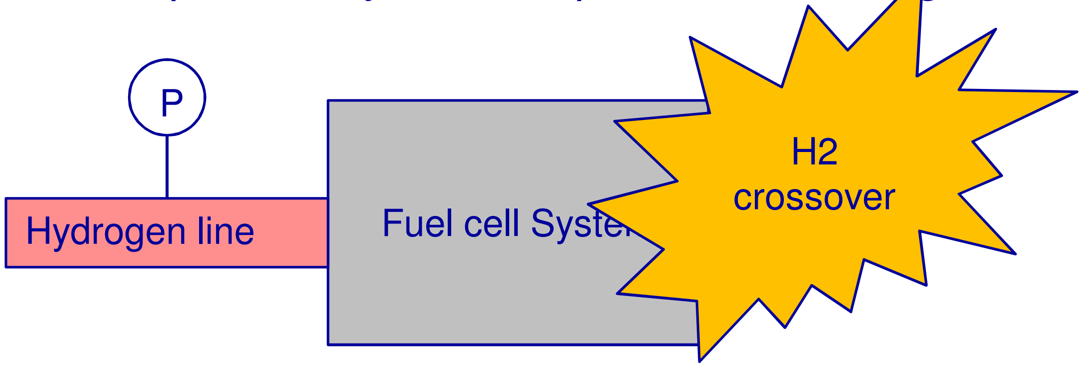
A certain fuel cell system is designed to run from the waste hydrogen produced from a refinery to offset the operating cost.

The system runs off a 100mbarg hydrogen line.

It is considered that appreciable hydrogen crossover into the air side of the fuel cell is unacceptable and will cause the system to fail.

Main tasks

(a) With the top event as 'appreciable hydrogen crossover' draw a fault tree for this failure.
(b) List the minimal cutsets
(c) Calculate the annual probability of the top event occurring



Inputs to the analysis

- Due to the nature of the plant feeding the hydrogen the system will only be online 50% of the year
- If the hydrogen pressure goes above 250mbar for greater than 1minute then the anodes are damaged and hydrogen will crossover
- If the hydrogen pressure is between 150 and 250mbar for greater than 5 minutes then and an o ring seal is slightly miss aligned or a hydrogen plate thickness is at the lower range of the manufactured tolerance then hydrogen crossover will occur.

An engineer did some investigation and found

- Monitoring the pressure for a month they found that the pressure was greater than 250mbar for longer than 1 minute 0.00001/month but was in the range of 150-250mbar for greater ant 5 minutes for 0.001/month.
- The probability of a misplaced o ring is 1.8e-4
- There are 1000 o rings in the system
- The probability of fuel plate in the lower range of thickness is 3.5e-5
- There are 500 fuel plates in the system

Best way to brake a road unicycle - Trade-offs

Downhill is most dangerous for large wheel unicycling. In racing speed needs to be maintained downhill (30kmh – 36” ungeared 30mph 36” geared). It is very easy to have the wheel runaway hence a drag braking force needs to be applied (there is no free-wheel on a unicycle)

Braking options

- No brake
  - Back pedal pressure
  - Low weight
  - Strong legs required!
    - Need to react against handlebars
- Hydraulic brake
  - Fast easy operation
  - Flexible mounting / adjustment
  - Fluid leaks air bleeding
  - Easy release
  - A little digital in operation
- Side pull calliper on ratchet lever
  - Slow to set / unset
  - Set once per use
  - More difficult to mount / adjust
  - Gradual braking

What might a FTA look like for each design with ‘fails to control downhill speed’ as the undesired event?

http://www.youtube.com/watch?feature=player_detailpage&v=wKUZOMJV-7g#t=7