COM4506/6506: Testing and Verification in Safety Critical Systems

Dr Ramsay Taylor

Contents

More Risk Assessment!

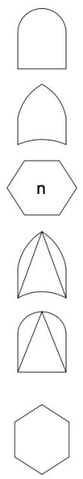
“Fault Tree Analysis (FTA) is one of the most important logic and probabilistic techniques used in [Probabilistic Risk Assessment] and system reliability assessment today.”

Fault Tree Handbook with Aerospace Applications, NASA Office of Safety and Mission Assurance

Different Hazard Analysis?

- Fault Tree Analysis is:
  - Structured (!)
  - Logical
  - Probabilistic
- Can be used in Hazard analysis
  - In Design
  - Also, in Accident Investigation

Uses Boolean Logic (sorta)



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

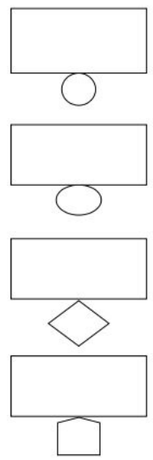
EXCLUSIVE OR - Output fault occurs if exactly one of the input faults occurs

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)

[you will also see variations on these!]

Connects “events”



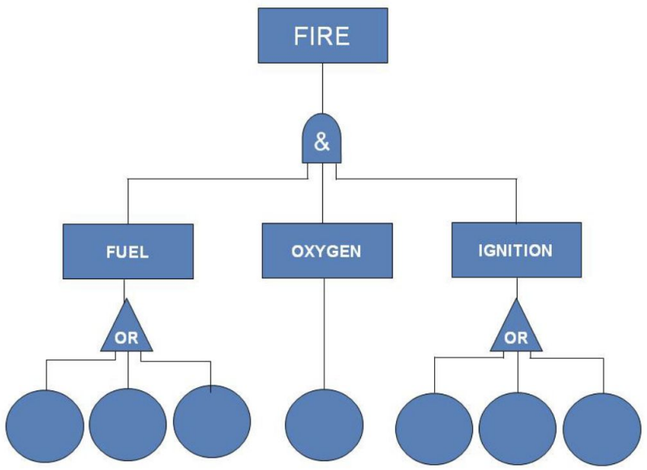
BASIC EVENT - A basic initiating fault requiring no further development

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

Fire!

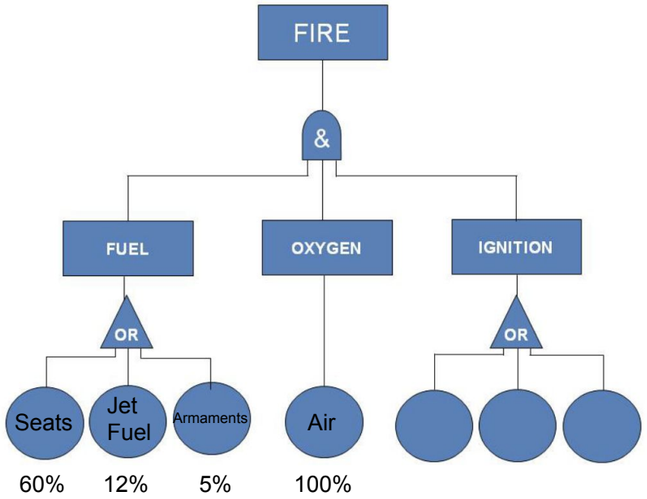


Probabilistic Modelling

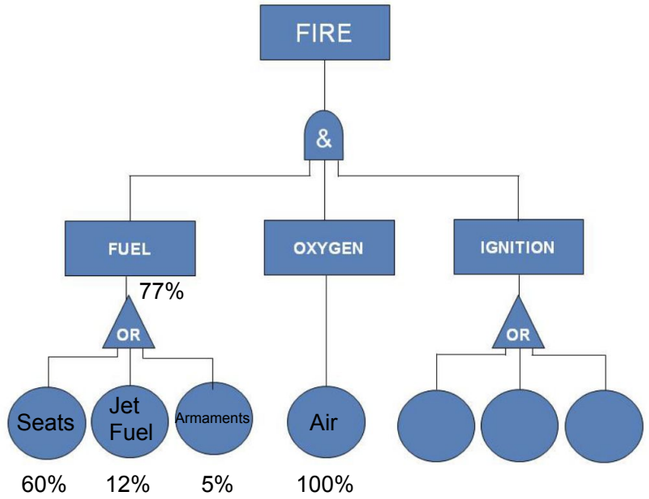
We can append probabilities to the FTA events if we have the relevant data.

This can allow us to calculate probabilities for compound events, and identify the parts of the system most in need of *mitigation*.

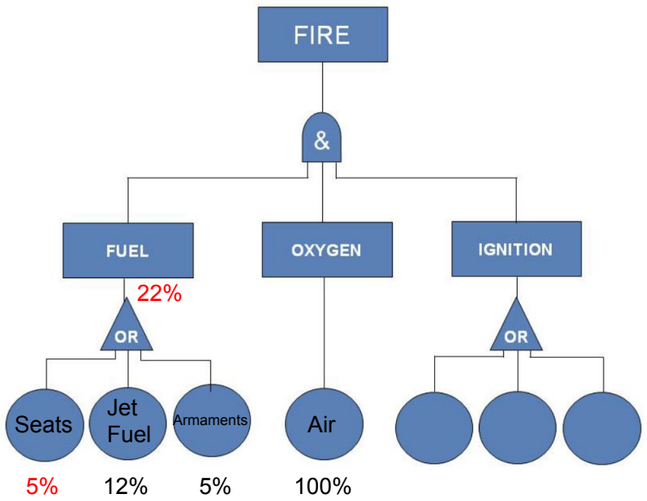
Probably Fire!



Probably Fire!



Probably Fire!



Summary

- FTA is structured and logical
- Again, it requires a structured understanding of the system!
- Can be applied probabilistically
  - Gives predictions of *likelihood* (which could feed into risk assessment!)
  - Identifies areas of maximum impact for *mitigation*.