apsys
SIMPLIFYING COMPLEXITY

Model-Based Safety Assessment: How to improve results exploitation ?

Fault tree generation from a list of minimal cutsets

Julien NIOL, Laurent SAGASPE and Jean-Pierre HECKMANN

IMBSA 2014

October 29th 2014

Aeronautical Context

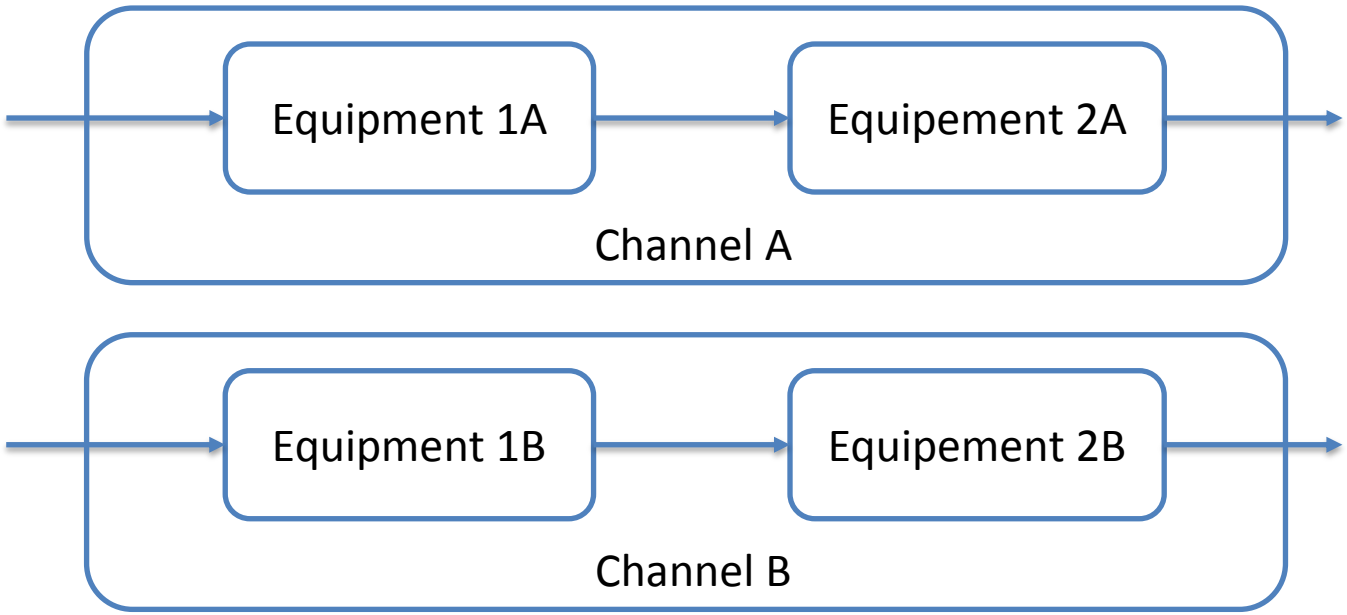
- CS 25.1309: Certification Specification for large aircrafts
  - Requirements any Aircraft shall comply to get Type Certificate
- AMC 25.1309: Accepted Mean of Compliance to CS 25.1309
  - Examples: ARP 4754, ARP 4761, DO178C…
- ARP 4761 : Recommended Practices for Safety Assessment
  - MBSA is partially covered by ARP 4761 (only as Appendix)

Aeronautical Context

- MBSA in aeronautics:
  - AltaRica Data Flow models built with Cecilia-OCAS and derivatives
  - Output: List of generated cutsets
- Major drawbacks
  - The list of MCS is not directly linked to system functional architecture
  - The list of MCS is hardly usable for V&V and consequently for certification
- Solution: Transform the MCS list in fault tree, a common and widely accepted format
  - APSYS prototype tool (Sirocco)

Example

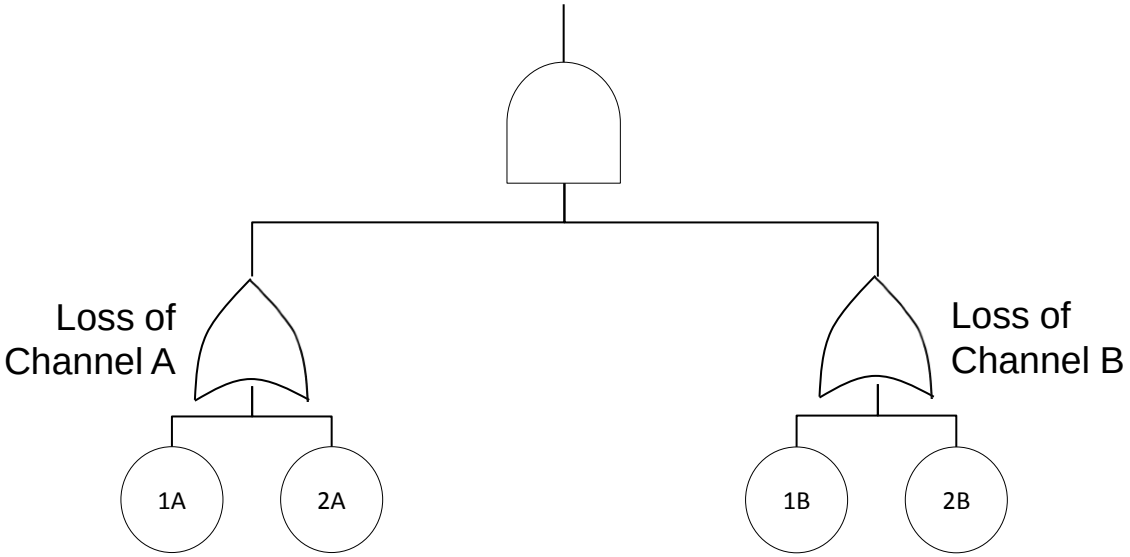
- Simple system with two independent channels



- Failure Condition: Loss of both channels

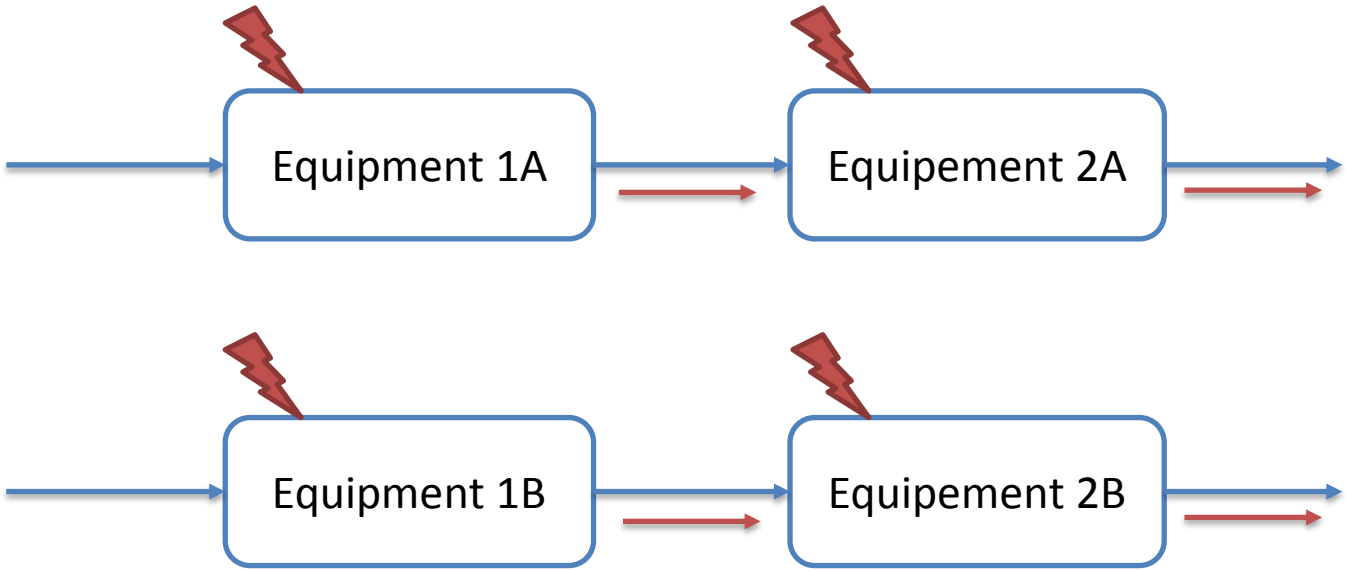
Fault Tree

- A Fault Tree is a representation of safety engineer understanding of the dysfunctional behavior of the system
- Built from a top-down and deductive approach



Model construction

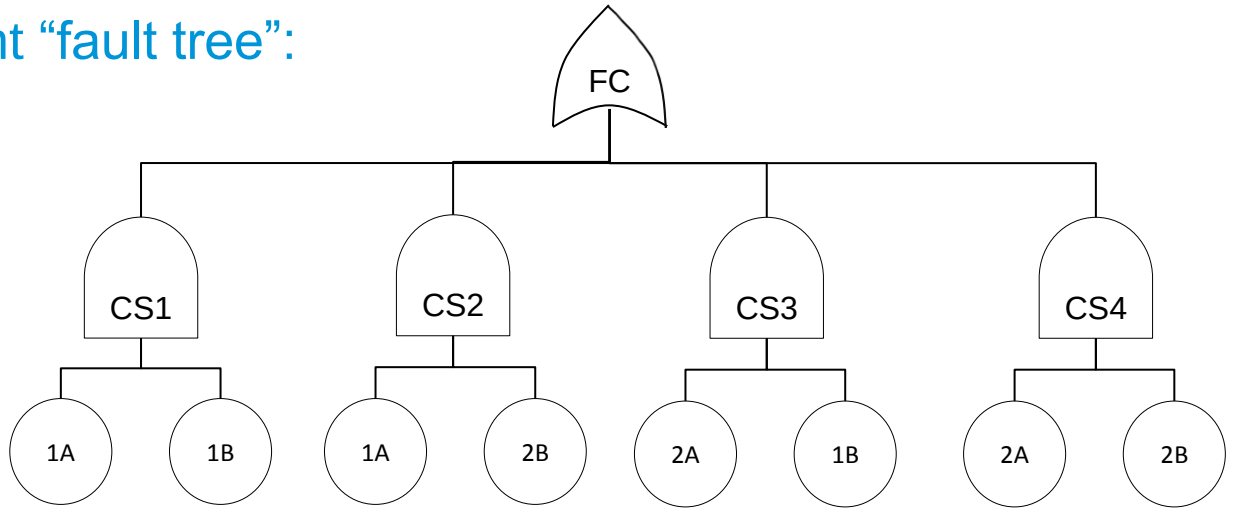
- Built from a bottom-up and inductive approach



- No global knowledge, only local knowledge

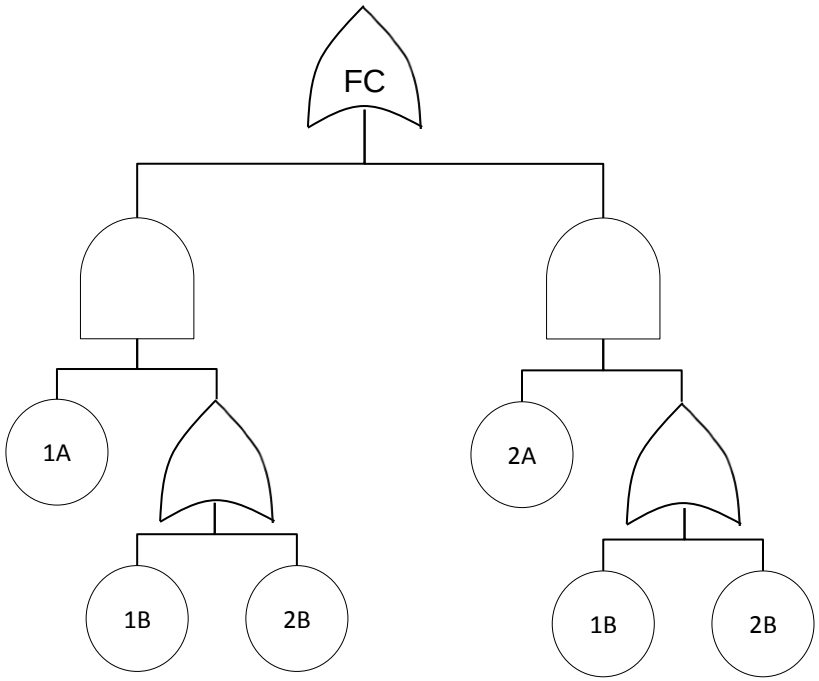
Minimal cutsets list

- Results of cutsets generation (by computer):
  - 1A and 1B
  - Or 1A and 2B
  - Or 2A and 1B
  - Or 2A and 2B
- Equivalent “fault tree”:



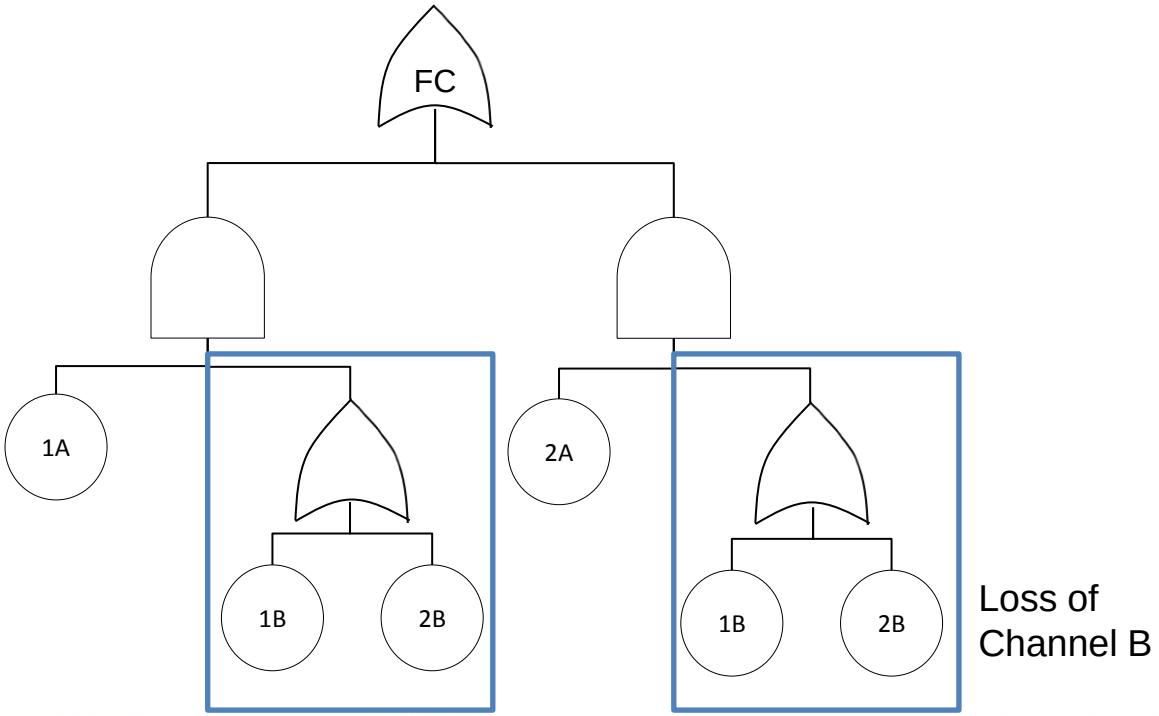
Step 1: Factorization

- 1st step: Factorization using a binary tree
- Resulting fault tree



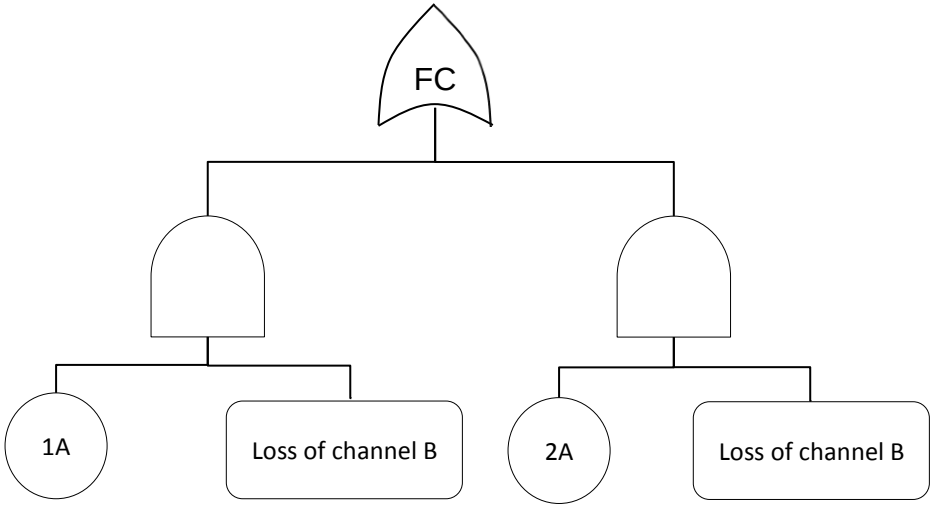
Step 2: Pattern Recognition

- 2nd step: Identifying patterns (subtree representing intermediate failure condition) for substitution



Step 2: Pattern Recognition

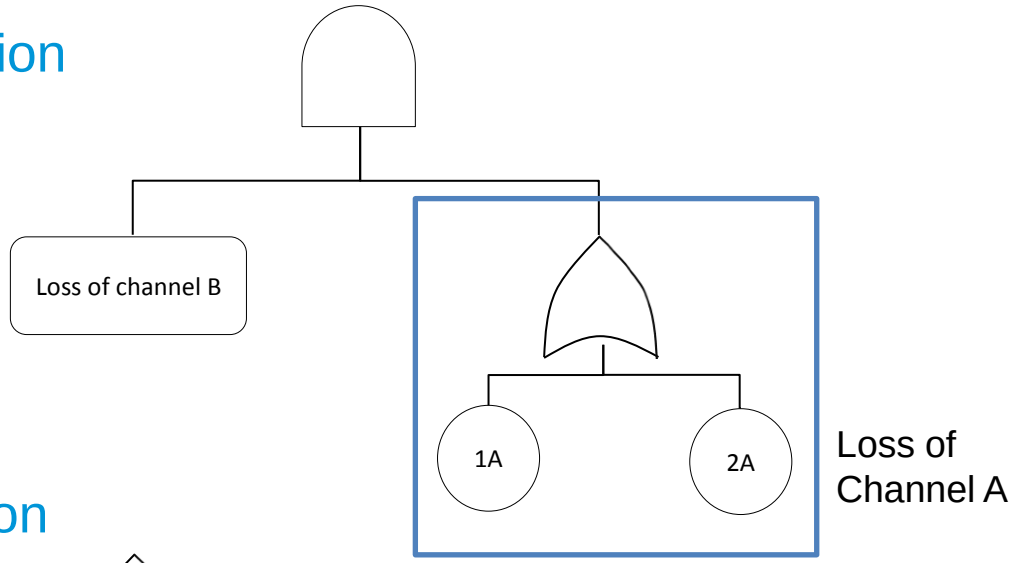
- After substitution



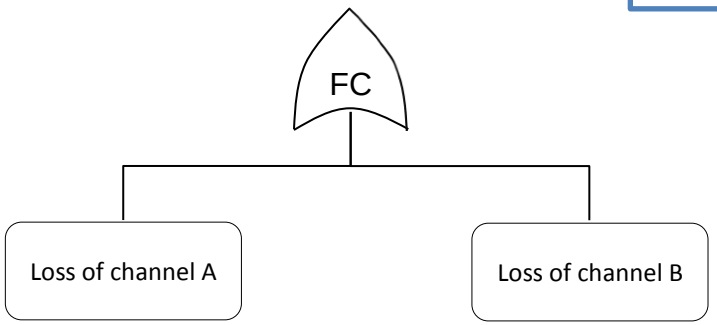
- Repetitive post-processing

Further steps

- After 2nd factorization

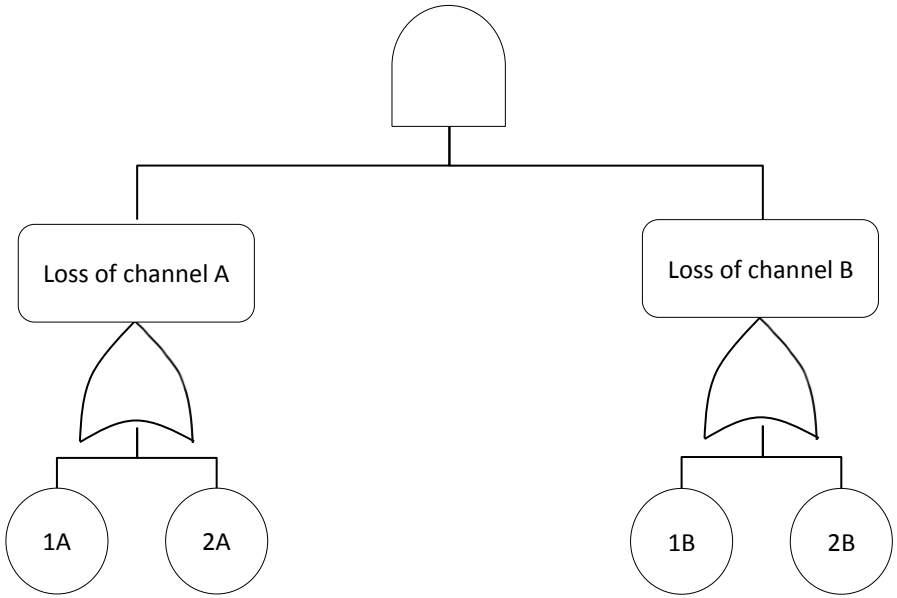


- After 2nd substitution



Resulting fault tree

- Expanding the reduced fault tree



Sirocco

- Currently implemented in Sirocco
  - Results import as list of minimal cutsets
  - Tree factorization fully automated
  - Pattern recognition by manual definition: user can select an intermediate gate to set up his pattern

Conclusion

- MBSA can be a powerful method, but it must be an accepted mean of compliance to get widely used in aeronautics.

- Next step: How to automatize pattern recognition ?

Questions ?

Thank you for your attention!