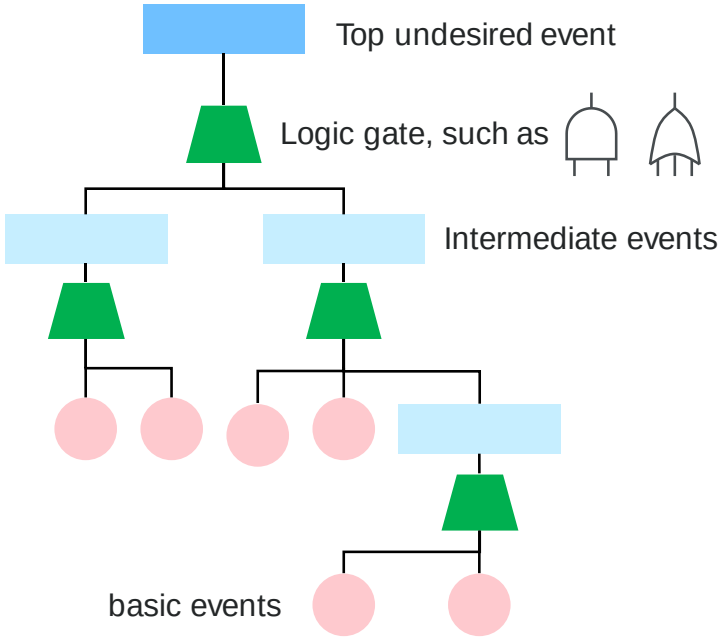
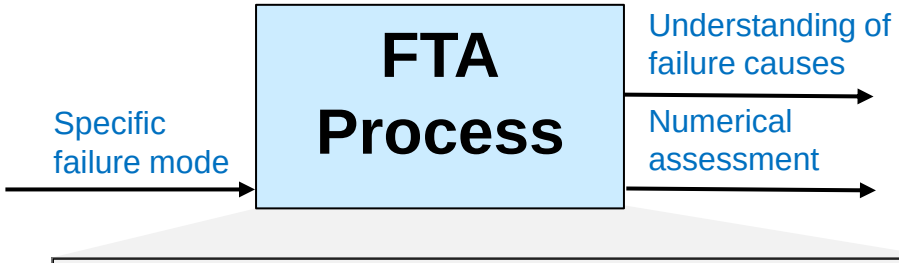
Fault Tree Analysis (FTA)

Problem
How to quantify a specific type of failure?

Difficulty
Work with an SME

- **Fault tree analysis** (**FTA**) is a top-down failure analysis in which an undesired system state (e.g., a failure mode) is analyzed using Boolean logic, combining lower-level events.
- FTA maps the relationship between faults and subsystems via a system level logic diagram.
- FTA can quantify the likelihood of failure.
- FTA can be used in the design process.
- FTA diagrams use a standard set of symbols.



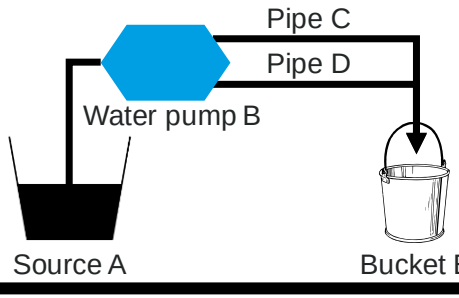


1. Define the top undesired event to investigate.
2. Identify first level contributors, just below the top level, and link these to the top level event using logical gates (e.g., AND and OR gates).
3. Identify the second level contributors and link to the first level contributors using logical gates. Continue with 3rd, 4th, etc level until basic events (root causes) are identified.
4. Construct the fault tree. Use numerical values (e.g. rates) for the basic events, if known.
5. Evaluate the fault tree.
   A. Simplify the fault tree, if possible.
   B. Determine the “cut sets,” the event combinations which cause the top event. Determine the “minimal cut sets,” the cut sets for which removing any event prevents the top event.
   C. Determine the likelihood of the top event, if numerical values are available.
6. Address (e.g., mitigate) the identified issues.

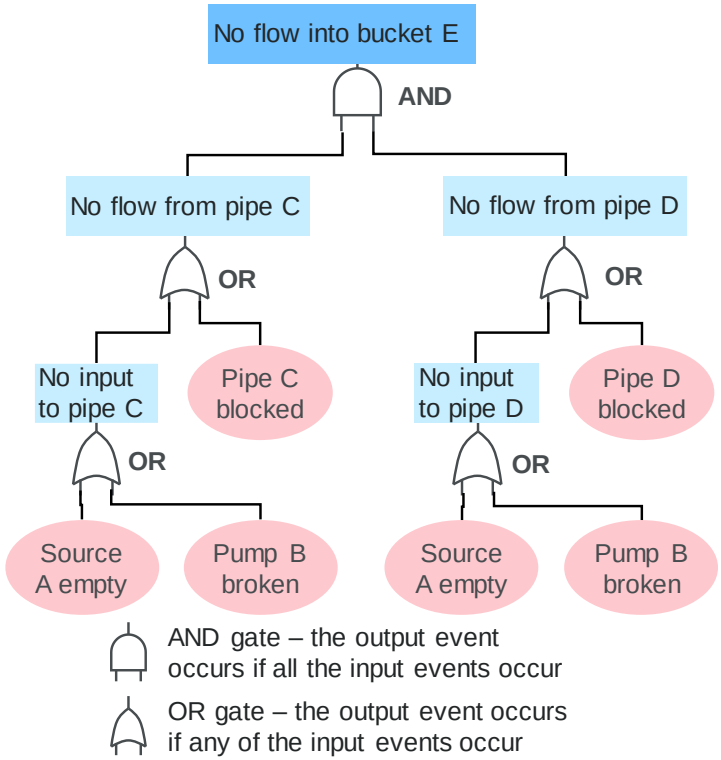
FTA – Example – Pumping Water

https://gerard-avontuur.tripod.com/Chapter2/Chapter2.html
https://commons.wikimedia.org/wiki/File:Bail_(PSF).png
https://commons.wikimedia.org/wiki/File:Half_full_bucket.svg

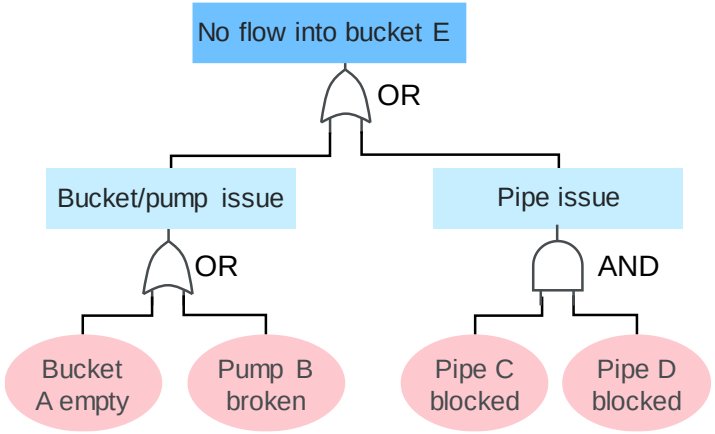
(1) Consider pumping water from Source A to Bucket E, using a pump and two pipes



(2) A fault tree of the pump system is below



(3) Using Boolean logic rules, the fault tree can be simplified to the one below



(4) The minimal cut sets are (any of these cause failure):

- Source A is empty
- Pump B is broken
- Pipe C is blocked and pipe D is blocked.

(5) If $\{P_A, P_B, \ldots\}$ are the failure probabilities for components {A, B, …} then the probability of no flow to bucket E (that is, P_E) is given by

$$P_E = 1-(1-P_A)(1-P_B)(1-P_CP_D)$$

Example: If each component has a 10% likelihood of having failed then the probability of no flow to bucket E is 20% since

$$P_E = 1-(1-0.1)(1-0.1)(1-0.1*0.1) = 0.20$$

FTA – Notes

Slide 1

1. Bell Telephone Laboratories developed FTA in 1962 for the US Air Force.
2. Fault trees visually depict the analysis process and identify the critical components related to system failure.
3. FTA is an efficient system analysis method.
4. FTA includes human errors in the analysis.
5. FTA gives qualitative & quantitative results.
6. An FTA is easily communicated to others.
7. When a specific event has an impact on several subsystems, it is called a *common cause*. Common cause failures make the analysis more challenging.
8. There are many software packages for FTA construction and analysis.
9. Disadvantages of Fault tree analysis
    A. An FTA only examines one top event.
    B. There can be too many components to meaningful understand the FTA.
    C. It is hard to capture time related factors.

Slide 2

1. Simplifying a fault tree – as in this example – can result in a large simplification and also give insight into the causes of the failure being studied.