Fault Trees

Fault Trees

- FT considers the combination of events that may lead to an unsdesirable situation of the system
  (the delivery of improper service for a Reliability study, catastrophic failures for a Safety study)

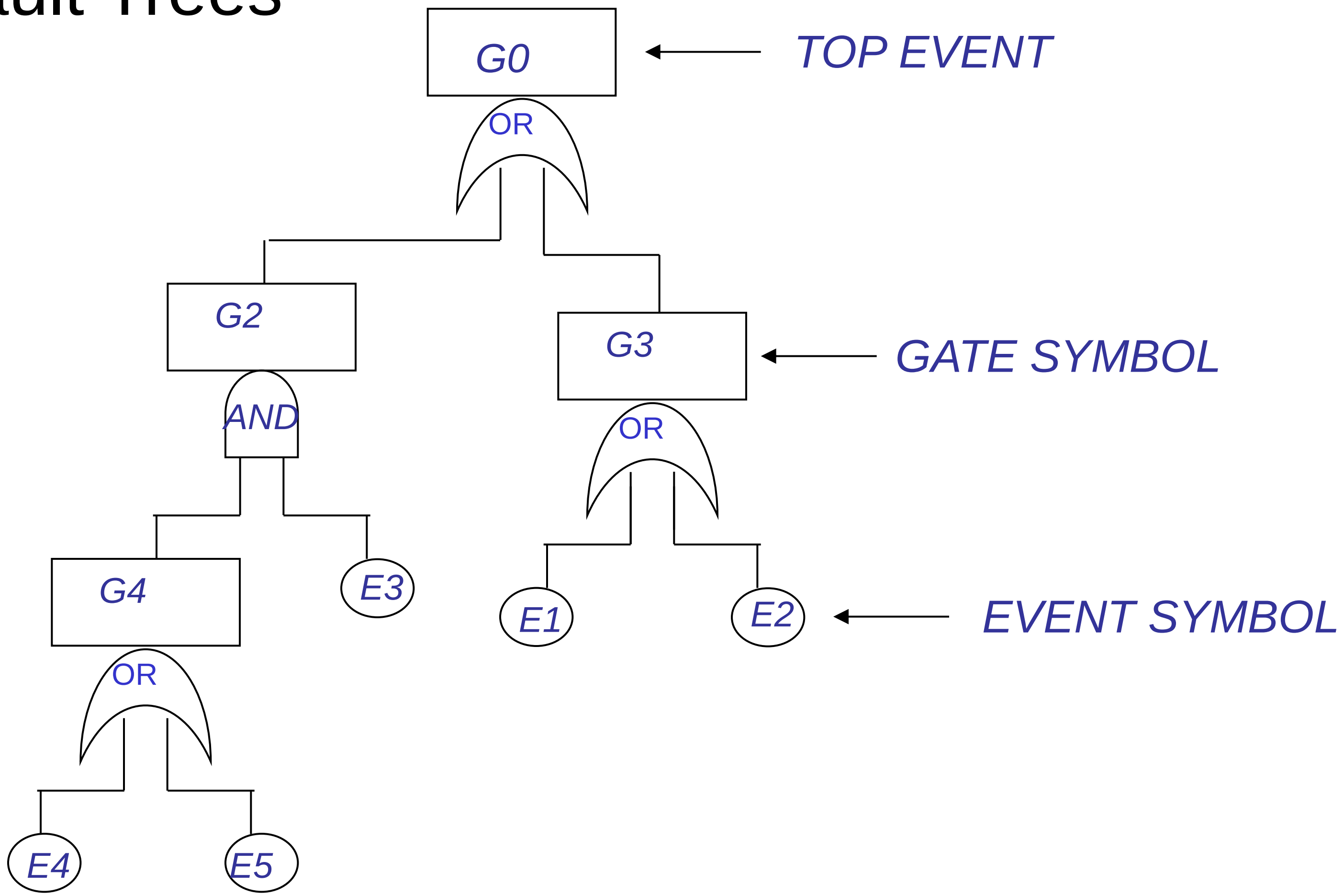
- Describe the scenarios of occurrence of events at abstract level

- Hierarchy of levels of events linked by logical operators

- The analysis of the fault tree evaluates the probability of occurrence of the root event, in terms of the status of the leaves (faulty/non faulty)

- Applicable both at design phase and operational phase

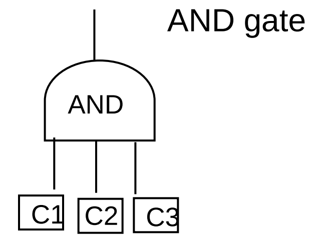
Fault Trees



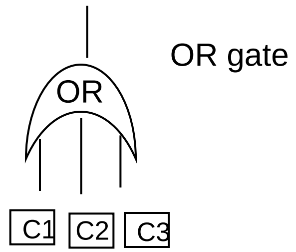
Describes the Top Event (status of the system) in terms of the status (faulty/non faulty) of the Basic events (system's components)

Fault Trees

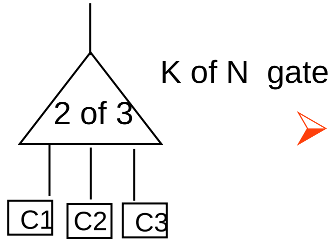
- Components are leaves in the tree
- Component faulty corresponds to logical value **true**, otherwise **false**
- Nodes in the tree are boolen AND, OR and k of N gates
- The system fails if the root is true



- True if all the components are true (faulty)

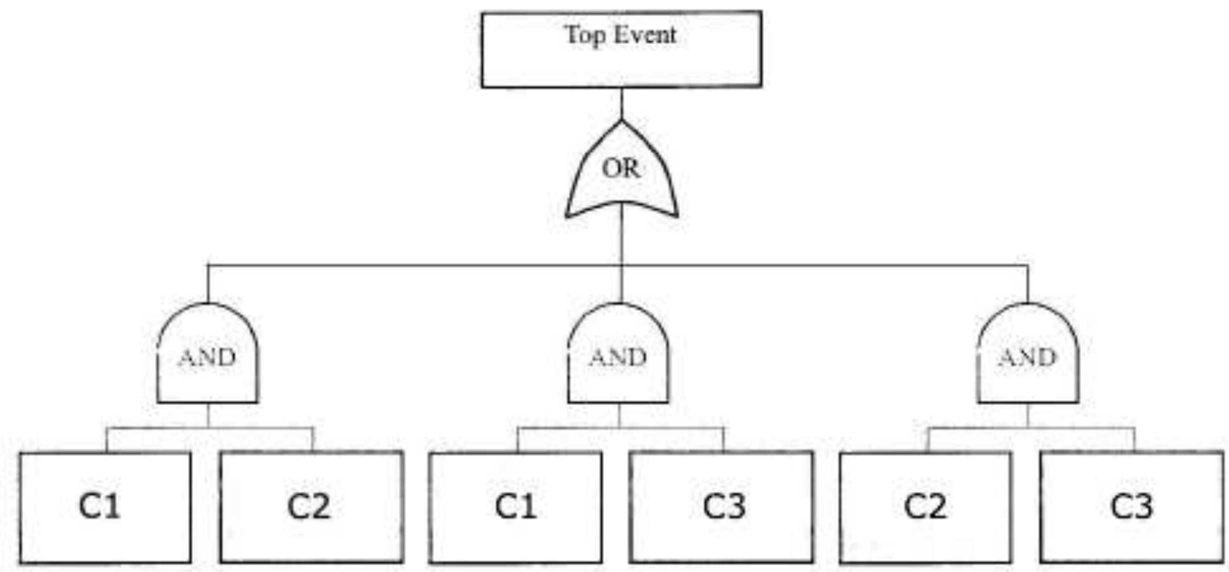


- True if at least one of the components is true (faulty)



- True if at least k of the components are true (two or three components) (faulty)

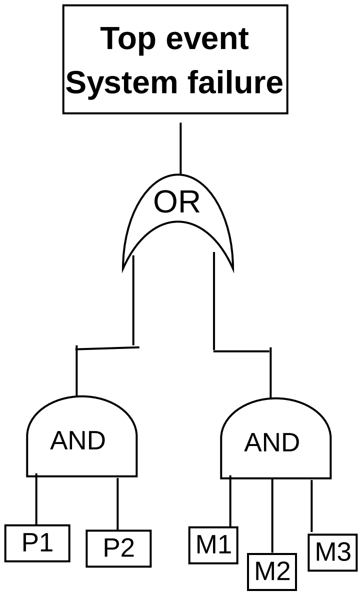
2of3



Example:

Multiprocessor with 2 processors and three shared memories

-> the computer fail if all the memories fail or all the processors fail



A cut is defined as a set of elementary events that, according to the logic expressed by the FT, leads to the occurrence of the root event.

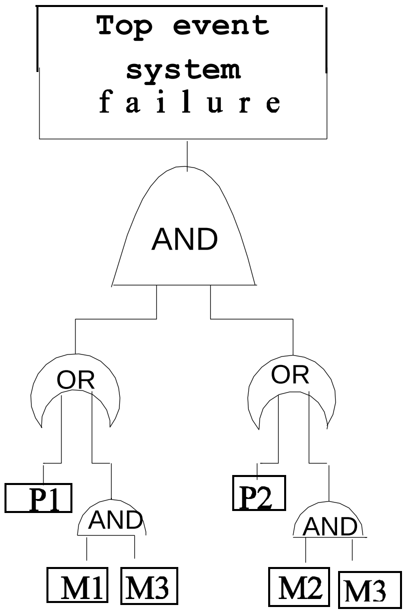
To estimate the probability of the root event, compute the probability of occurrence for each of the cuts and combine these probabilities

Conditioning Fault Trees

- If the same component appears more than once in a fault tree, it violates the independent failure assumption (conditioned fault tree)

- Example

  Multiprocessor with 2 processors and three memories: M1 private memory of P1 M2 private memory of P2, M3 shared memory.



- Assume every process has its own private memory plus a shared memory.
- Operational condition: at least one processor is active and can access to its private or shared memory.
- **repeat** instruction:given a component C whether or not the component is input to more than one gate, the component is unique

  M3 is a shared memory

Conditioning Fault Trees

If a component C appears multiple times in the FT

$$Q_s(t) = Q_{S|C\ Fails}(t)\ Q_C(t) + Q_{S|C\ not\ Fails}(t)\ (1-Q_C(t))$$

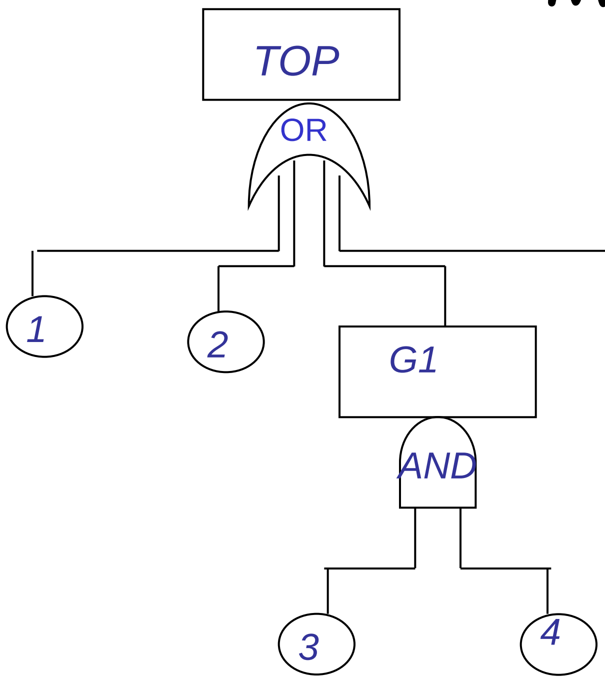
where

S|C Fails is the system given that C fails

and

S|C not Fails is the system given that C has not failed

Minimal cut sets



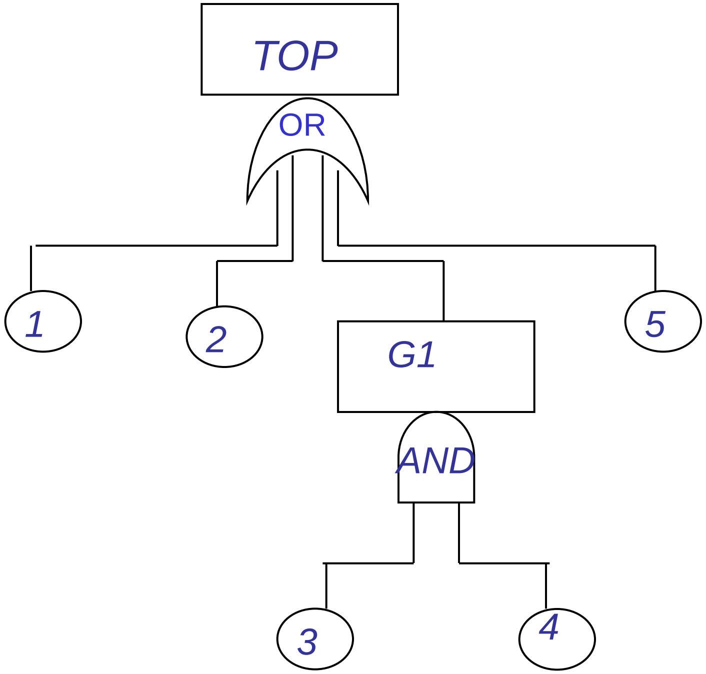
A cut is defined as a set of elementary events that, according to the logic expressed by the FT, leads to the occurrence of the root event.

Cut Sets

Top = {1}, {2} , {G1} , {5} = {1}, {2} , {3, 4} , {5}

Minimal Cut Sets

Top = {1}, {2} , {3, 4} , {5}



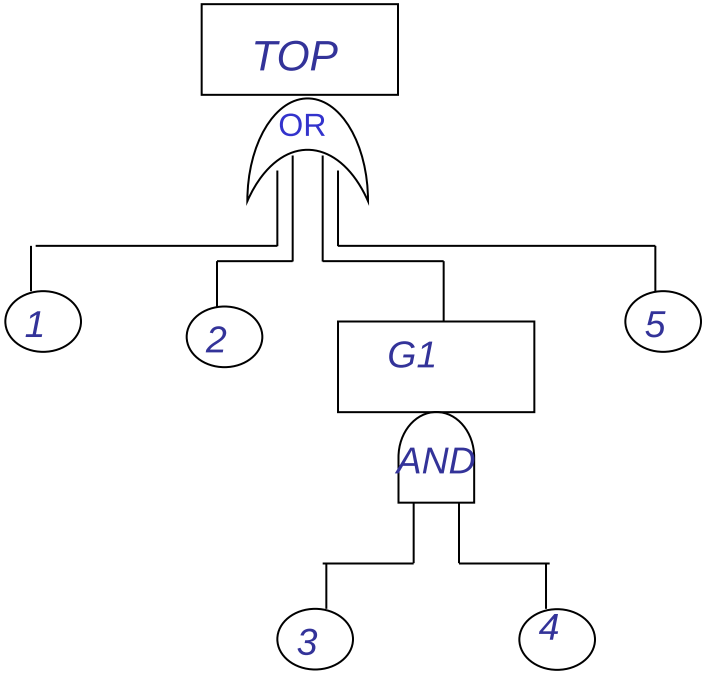
Minimal Cut Sets
Top = {1}, {2} , {3, 4} , {5}

independent faults of the components

Q_i (t) = probability that all components in the minimal cut set *i* are faulty

Qi (t) = q_1(t) q_2(t) … q_{ni}(t)
where ni is the number of components of the minimal cut i

The numerical solution of the FT is performed by computing the probability of occurrence for each of the cuts, and by combining those probabilities to estimate the probability of the root event



Minimal Cut Sets

Top = {1}, {2} , {3, 4} , {5}

Q_{Top} (t) = Q1 (t) + … + QN (t)

N number of mininal cut sets (MCS)

Fault Trees

- Definition of the Top event
- Analysis of failure models of components
- Minimal cut set

  minimal set of events that leads to the top event

  -> critical path of the system

  (#MCS =1 or #MCS = n)

Analysis:

- Failure probability of Basic events
- Failure probability of minimal cut sets
- Failure probability of Top event
- Single point of failure of the system: minimal cuts with one event

Failure Mode Effect Analysis

FMEA

Failure Mode Effect Analysis (FMEA):
is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.

FMEA

vulnerability to single failures is analysed
(FMEA does not consider multiple failures)

FMEA

FMEA is used during design to prevent failures. Later it's used for control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the life of the product or service.

Begun in the 1940s by the U.S. military, FMEA was further developed by the aerospace and automotive industries. Several industries maintain formal FMEA standards

FMEA: current knowledge and actions about the risks of failures

Example

FMEA performed by a Bank on ATM (Automated Teller machine) system

Function	Potential Failure Mode	Potential Effects(s) of Failure	S	Potential Cause(s) of Failure	O	Current Process Controls	D	RPN
Dispense amount of cash requested by customer	Does not dispense cash	Customer very dissatisfied Incorrect entry to demand deposit system Discrepancy in cash balancing	8	Out of cash	5	Internal low-cash alert	5	200
				Machine jams	3	Internal jam alert	10	240
				Power failure during transaction	2	None	10	160
	Dispenses too much cash	Bank loses money Discrepancy in cash balancing	6	Bills stuck together	2	Loading pro-cedure (riffle ends of stack)	7	84
				Denominations in wrong trays	3	Two-person visual verification	4	72
	Takes too long to dispense cash	Customer somewhat annoyed	3	Heavy computer network traffic	7	None	10	210
				Power interruption during transaction	2	None	10	60

From: http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html

FMEA tables

- Identify the functionality of the system
- Identify all the ways a failure could happen. These are potential **failure modes.**

FMEA is applied to the system and to any component.

Define a Table with the following information :

1) **potential effects of failure**

for each failure mode, identify all the consequences on the component and on the system.

determine how serious each effect is. This is the severity rating, or S. Severity is usually rated on a scale from 1 to 10, where 1 is insignificant and 10 is catastrophic.

FMEA tables

2) List all possible causes for each failure mode.

For each cause, determine the occurrence rating, or O. This rating estimates the probability of failure occurring for that reason during the lifetime of your scope. Occurrence is usually rated on a scale from 1 to 10, where 1 is extremely unlikely and 10 is inevitable.

3)For each cause, identify current process controls.

These are tests, procedures or mechanisms that you have in place to keep failures from reaching the customer.
These controls might prevent the cause from happening, reduce the likelihood that it will happen or detect failure after the cause has already happened but before the customer is affected.

FMEA tables

For each control, determine the detection rating, or D. This rating estimates how well the controls can detect either the cause or its failure mode after they have happened but before the customer is affected. Detection is usually rated on a scale from 1 to 10, where 1 means the control is absolutely certain to detect the problem and 10 means the control is certain not to detect the problem (or no control exists).

Calculate the risk priority number, or RPN, which equals S × O × D. Also calculate Criticality by multiplying severity by occurrence, S × O.

FMEA tables

FMEA table numbers provide guidance for ranking potential failures in the order they should be addressed.

Identify recommended actions. These actions may be additional controls to improve detection.

Note that:

FMEA allows to associate a cause, i.e., the failure mode of a simple component, to the system failure event.

FT/FMEA

Fault-trees often used in conjunction with FMEA

FMEA

vulnerability to single failures is analysed
(FMEA does not consider multiple failures)

FT

allows to describe the case in which the occurrence of an event depends on multiple failures