Reliability Engineering

Notes 8

Failure and Fault

- **Failure:** The termination of the ability of an item to perform a required function.
- A failure is always related to a required function. The function is often specified together with a performance requirement.
- A failure occurs when the function cannot be performed or has a performance that falls outside the performance requirement

Failure and Fault

- **Fault** : It is a condition that causes the system to fail to perform its required function.
- **Fault:** The state of an item characterized by inability to perform a required function.
- **Failure cause:** The circumstances during design, manufacture, or use which have led to a failure.

Fault Tree Analysis (FTA)

- Fault Tree Analysis (FTA) is the most commonly used technique for risk and reliability analysis.
- It was developed by Bell Telephone Laboratories to evaluate safety of the Minuteman Launch Control System in 1962.
- It was improved then by Boeing Company.
- It is widely used in aerospace, automobile, chemical, nuclear and software industries.

Fault Tree Analysis (FTA)

- Fault tree analysis (FTA) is a graphical tool to explore the causes of system level failures.
- Fault tree analysis consists of two elements “events” and “logic gates” which connect the events to identify the cause of the top undesired event.
- Fault tree analysis can be used to perform for all types of system level risk assessment process. The purpose of FTA is to effectively identify cause(s) of system failure and mitigate the risks before it occurs.

Fault Tree Analysis (FTA)

- FTA is a deductive (general to the specific) approach.
- FTA identifies events that can cause an undesired event.
- FTA utilizes Boolean logic.

Fault Tree Analysis (FTA)

- Fault tree analysis is the qualitative and quantitative analyses that can be carried out.
- This method is frequently used as a qualitative evaluation method in order to assist the designer, planner or operator in deciding how a system may fail and what remedies may be used to overcome the causes of failure.

Fault Tree Analysis (FTA)

- The method can also be used for quantitative evaluation, in which case the causes of system failure are gradually broken down into an increasing number of hierarchical levels until a level is reached at which reliability data is sufficient or precise enough for a quantitative assessment to be made. The appropriate data is then inserted into the tree at this hierarchical level and combined together using the logic of the tree to give the reliability assessment of the complete system being studied.

Fault Tree Analysis (FTA)

- Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential undesirable event called a TOP event, and then determining all the ways it can happen.
- The analysis proceeds by determining how the top event can be caused by individual or combined lower level failures or events.
- The causes of the top event are “connected” through logic gates (AND, OR) into basic failures (causes), and called “primary events.”

Fault Tree Analysis (FTA)

- The main elements of a fault tree are:
- TOP event, which is the description of the critical system event
- Basic events, the are the lowest level of identified causes
- Logic gates, such as OR or AND gates, which gives the logical relationship between the TOP event and the basic events

Fault Tree Analysis (FTA)

- Top event is represented with rectangle.
- Basic Events : An event that cannot be developed any further. (circle symbol)

Fault Tree Analysis (FTA)

- *Qualitative Analysis*
- used for identifying
- critical events
- potential system weaknesses
- best ways to reduce the risk associated with the top event
- conducted using minimal cut sets

Fault Tree Analysis (FTA)

- *Quantitative Analysis*
- calculate the probability of occurrence of the top event, given the fault
- tree and the probability of occurrence of the basic events
- common approaches include assume all basic events are independent

Cut-set

- Cut-set: combination of basic events to cause the top level event
- Minimum cut-set: A cut-set with the minimum number of events that can still cause the top event. It is a cut-set that does not contain another cut-set. It is a cut set that cannot be reduced without losing its status as a cut set.
- The top event occurs if one or more of the minimal cut sets occur.

Usage

- to understand of the logic leading to the top event
- prioritize the contributors leading to the top event
- a proactive tool to prevent the top event
- to monitor the performance of the system
- diagnostic tool to identify and correct causes of the top event

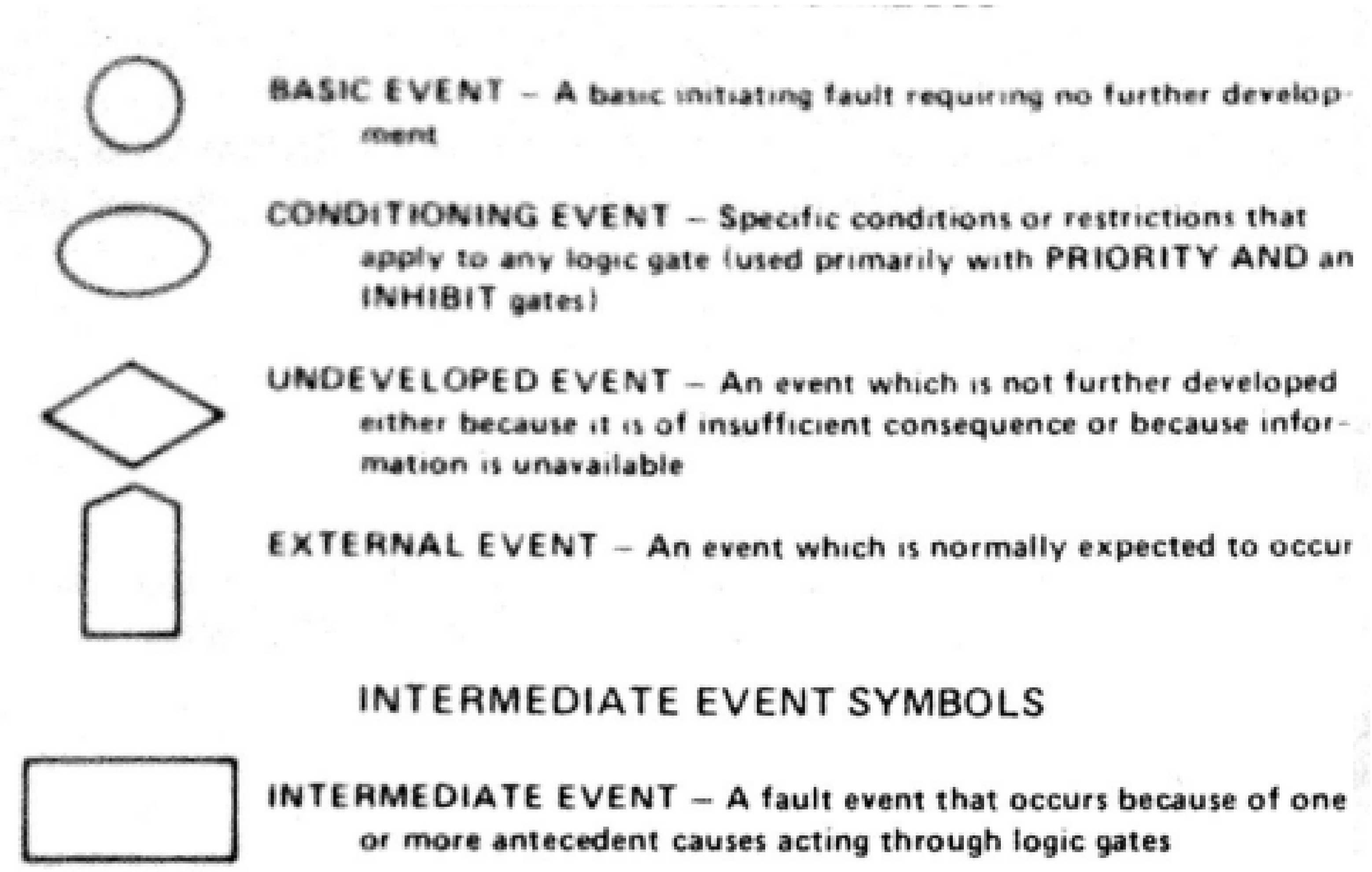
Benefits

- Fault tree can help to
- Quantify probability of top event occurence
- Evaluating proposed system architecture attributes
- Developing to minimize the probability of the undesired event
- Determining the mitigation measures
- Complying with qualitative and quantitative reliability objectives
- Establishing maintenance tasks and intervals from reliability assessments.

Limitations

- Events is often assumed as independent.
- Common-cause failures not always obvious
- Difficult to capture delays and other temporal factors
- Can be labor intensive
- Can become very complex very quickly, can be difficult to review
- difficult to conceive all possible scenarios leading to the top event
- construction of fault trees for large systems can be tedious
- correlations between basic events (e.g. failure of components belonging to the same batch) are difficult to model and exact solutions to correlated events do not exist

Symbols



BASIC EVENT – A basic initiating fault requiring no further development

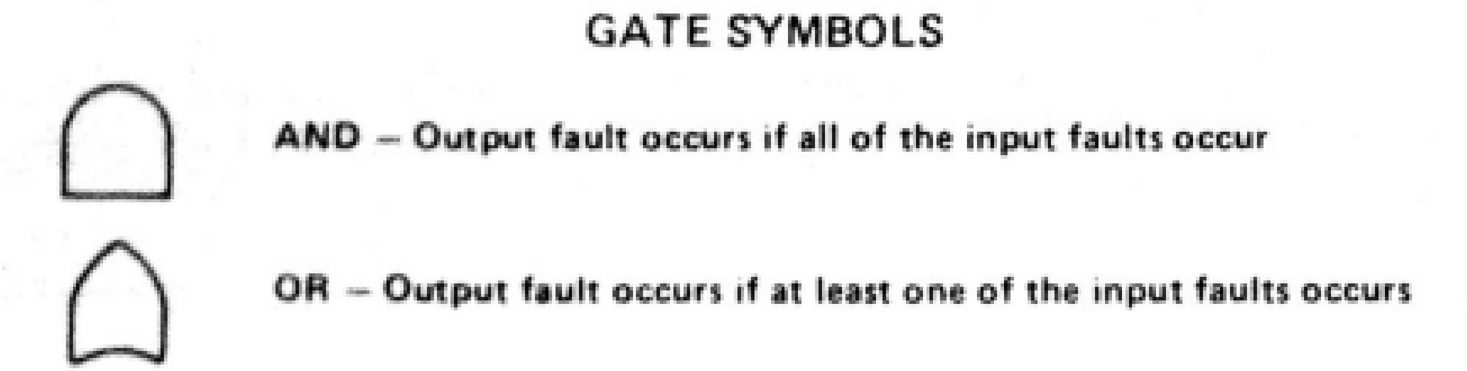
CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND an INHIBIT gates)

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

EXTERNAL EVENT – An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS

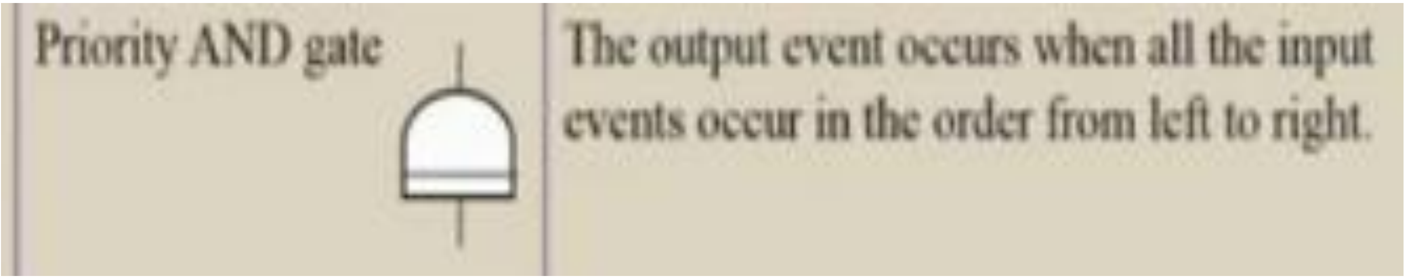
INTERMEDIATE EVENT – A fault event that occurs because of one or more antecedent causes acting through logic gates



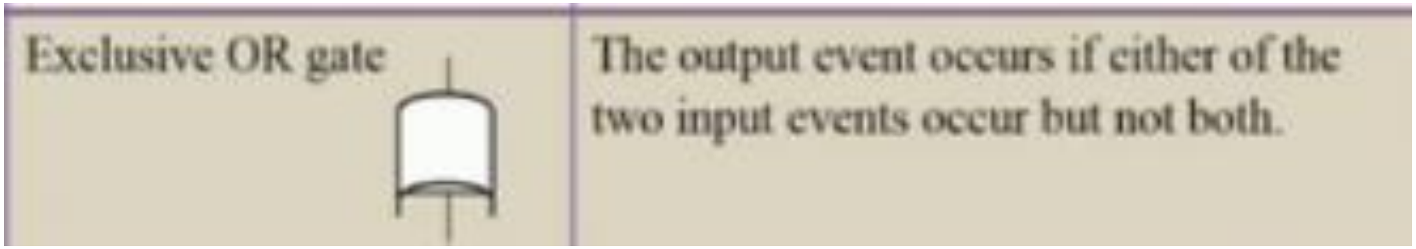
GATE SYMBOLS

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

OR – Output fault occurs if at least one of the input faults occurs

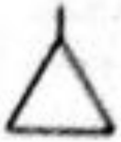


Priority AND gate	The output event occurs when all the input events occur in the order from left to right.

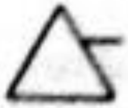


Exclusive OR gate	The output event occurs if either of the two input events occur but not both.

TRANSFER SYMBOLS



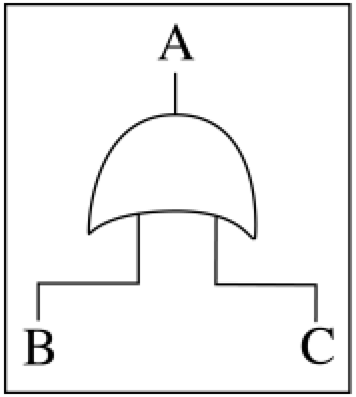
TRANSFER IN – Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)



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

Fault Tree Analysis (FTA)

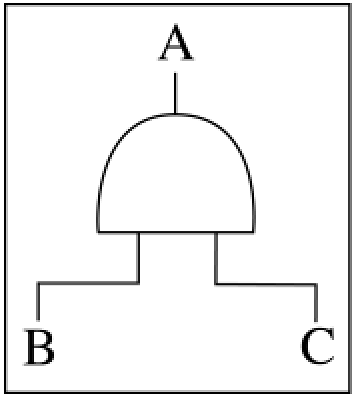
Operation, OR



Meaning:

Event A occurs when either event B or C occurs

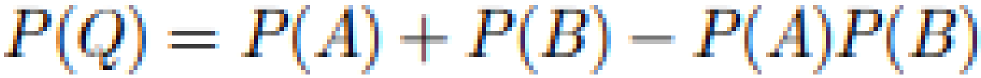
Operation, AND



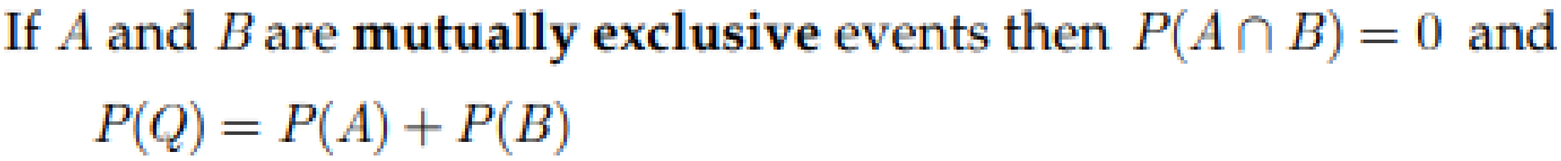
Meaning:

Event A occurs when both event B and C occur

- OR GATE
- If A and B are independent events



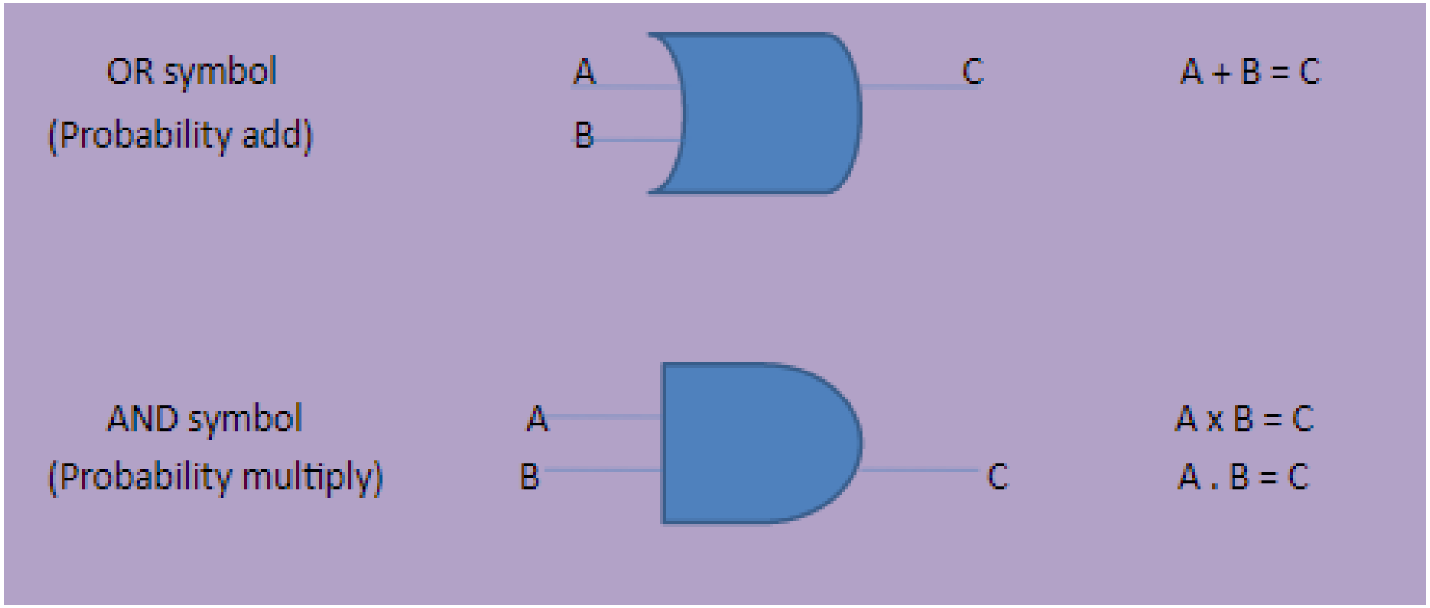
$$P(Q) = P(A) + P(B) - P(A)P(B)$$



If A and B are **mutually exclusive** events then $P(A \cap B) = 0$ and

$$P(Q) = P(A) + P(B)$$

- P(Q)= P(A)+P(B) is an estimate for the probability of event Q (because P(A ∩B) is small compared with P(A)+ P(B)for very low probability events)



OR symbol

(Probability add)

A + B = C

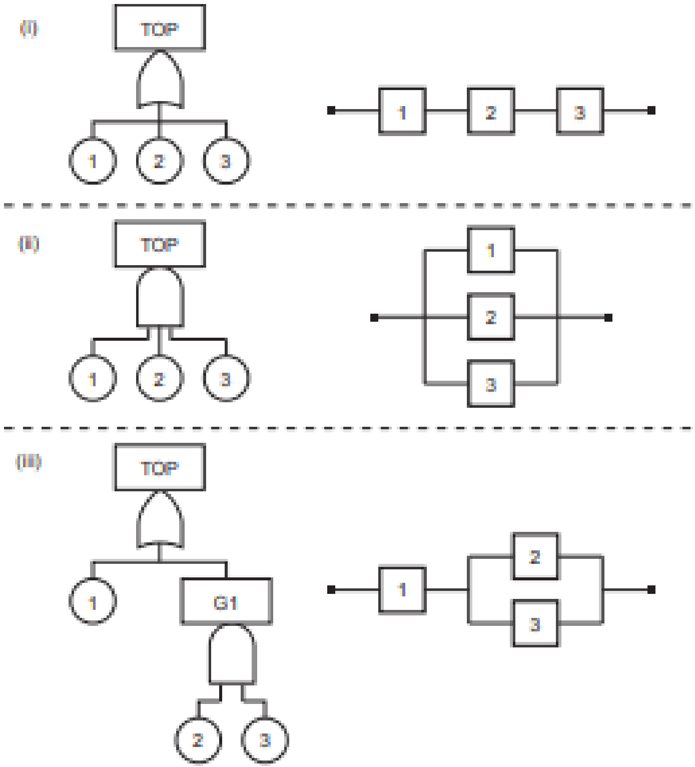
AND symbol

(Probability multiply)

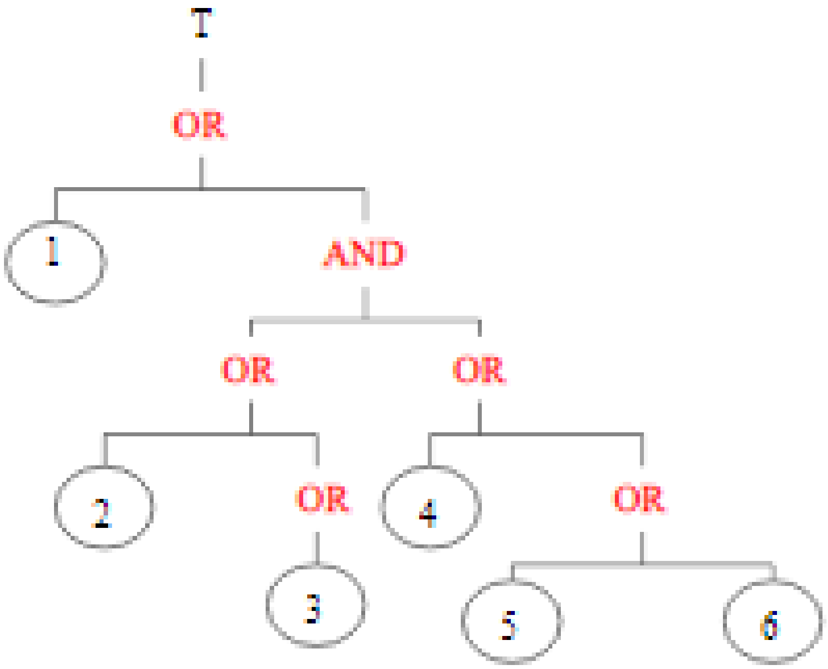
A x B = C

A . B = C

A fault tree may be converted into a reliability block diagram and vice verse, as illustrated below.



-



Minimum Cut Sets

{1}, {2,4}, {2,5}, {2,6}, {3,4}, {3,5}, {3,6}

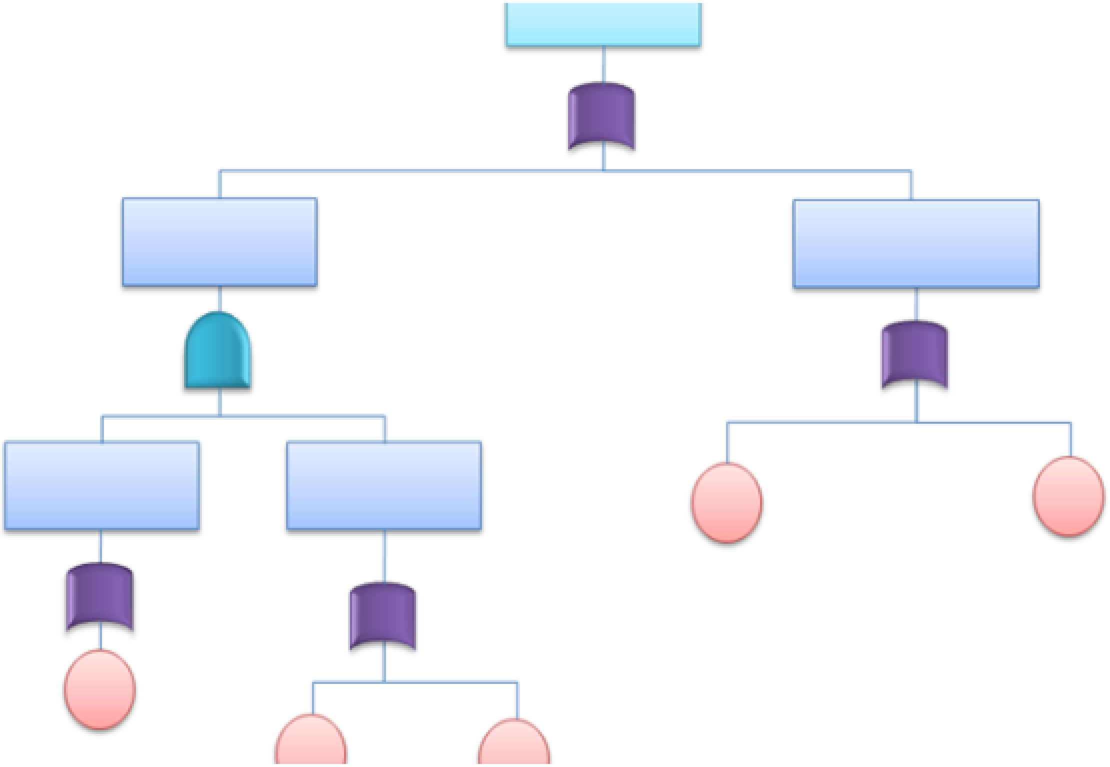
- Event symbols described the events that lead to system level failure, system level failure is top event and gate symbols are that connect the event symbol as per their causal relations.

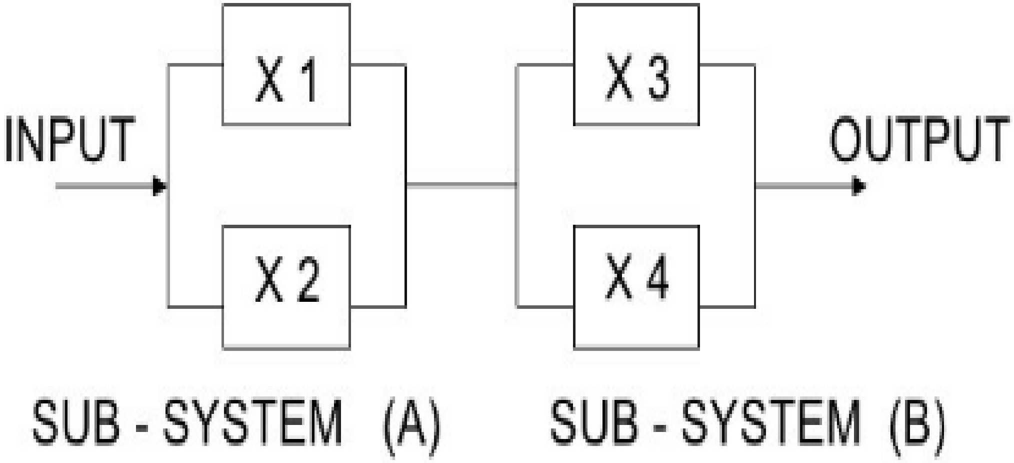
Steps of FTA

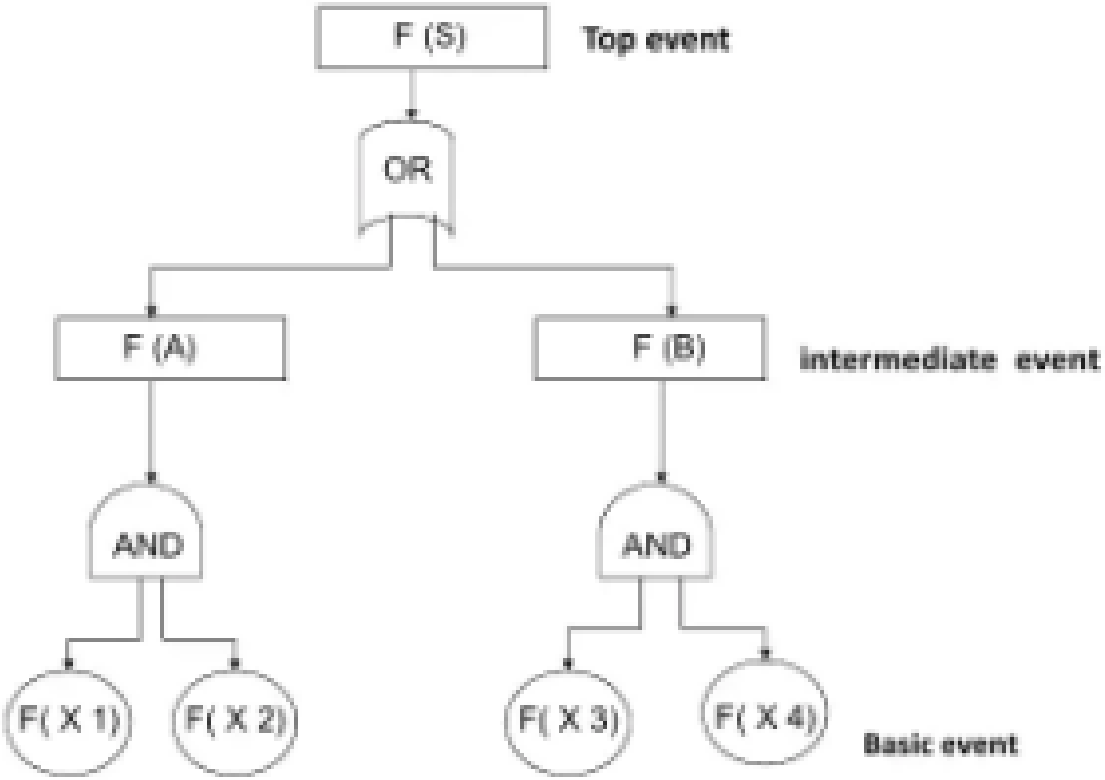
- 1. Definition of the problem, system, and boundary conditions of the analysis
- 2. Construction of the fault tree
- 3. Identification of minimal cut sets
- 4. Qualitative analysis of the fault tree
- 5. Quantitative analysis of the fault tree

Steps of FTA

- The following basic steps are involved in performing fault tree analysis:
- i Establishing system definition.
- ii Constructing the fault tree.
- iii Evaluating the fault tree qualitatively.
- iv Collecting basic data such as components' failure rates, repair rates, and failure occurrence
- probability.
- v Evaluating fault tree quantitatively.
- vi Recommending corrective measures.




INPUT
X 1
X 2
X 3
X 4
OUTPUT
SUB - SYSTEM (A)
SUB - SYSTEM (B)


F (S)
Top event
OR
F (A)
F (B)
intermediate event
AND
AND
F(X 1)
F(X 2)
F(X 3)
F(X 4)
Basic event

Here F(x1) , F(x2) , F(x3), F(x4) Are Events Fail…

F (A) = SUB – SYSTEM (A) FAILS

F(B) = SUB – SYSTEM (B) FAILS

THEN F(A) = F(X1) AND F(X2)

AND F(B) = F(X3) AND F(X4)

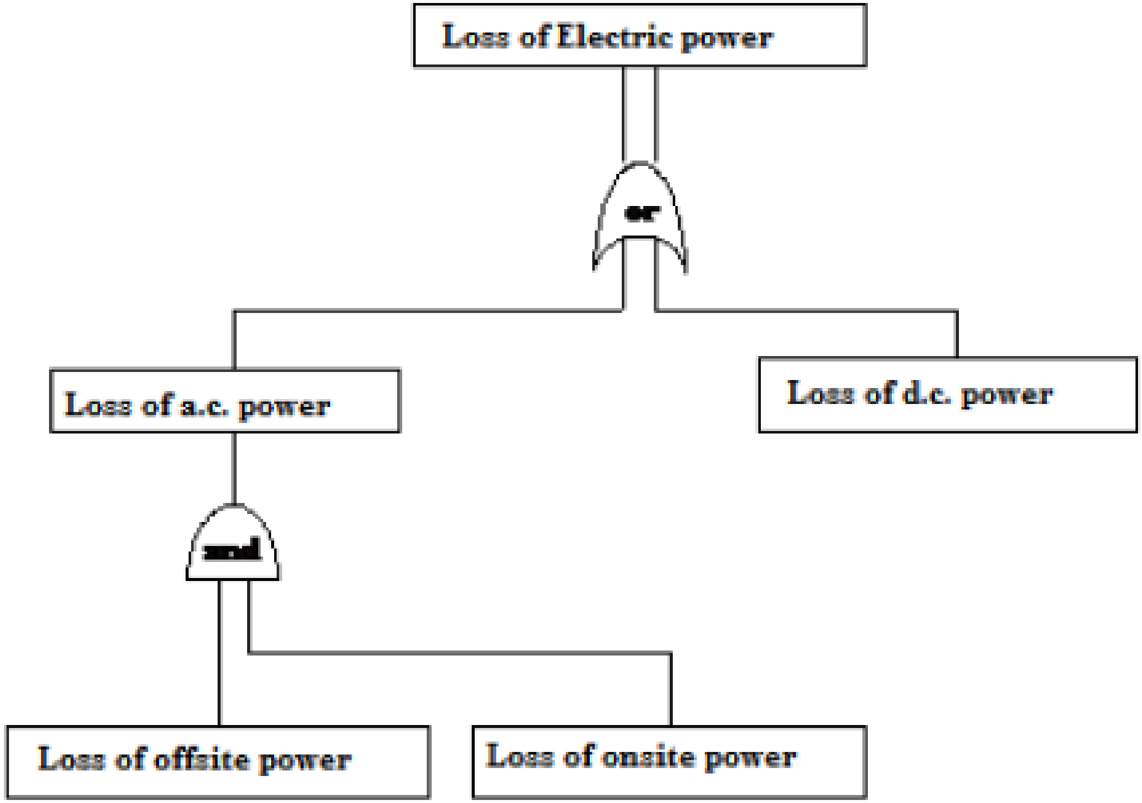
FINALLY THE FAILURE OF THE SYSTEM

F(S) = F(A) OR F(B)

Example

- In this example, the failure event being considered is loss of the electric power. In practice the electric power requirements are both a.c. power, to supply energy for prime movers, and d.c. power, to operate relays and contractors, both of which are required to
- ensure the successful operation of the electric power. Consequently the event 'loss of electric
- power' can be divided into two sub-events 'loss of a.c. power' and 'loss of d.c. power'. Failure of either, or both, causes the system to fail.

- Sub-events can be divided further. The event 'loss of a.c. power' may be caused by 'loss of offsite power' (the grid supply) and by 'loss of onsite power' . They both have to fail for the a.c. power to fail.
- The events are mutually exclusive for the OR gate(i.e. they don’t overlap).
- In the present example, suppose the probabilities of the events at the bottom of the tree are:
- Prob (Loss of offsite power) = 0.067
- Prob (Loss of onsite power) = 0.075
- Prob (Loss of dc power) = 0.005


Loss of Electric power
or
Loss of a.c. power
Loss of d.c. power
and
Loss of offsite power
Loss of onsite power

- For the AND gate at the bottom we multiply the probabilities to work out
- Prob (Loss of a.c. power) =
- Prob(Loss of offsite power) x Prob (Loss of onsite power)
- = 0.067 x 0.075 = 0.005025
- For the OR gate we add the probabilities to get the probability of the top event:
- Prob (Loss of electric power) =
- Prob (Loss of a.c. power) + Prob (Loss of d..c power)
- = 0.005025 + 0.005 = 0.010025.

Resources

- RISK-INFORMED OPERATIONAL DECISION MANAGEMENT (RIODM): RISK, EVENT TREES AND FAULT TREES, Fall 2005, Lecture 1, Michael W. Golay Professor of Nuclear Engineering Massachusetts Institute of Technology, https://ocw.mit.edu/courses/nuclear-engineering/22-38-probability-and-its-applications-to-reliability-quality-control-and-risk-assessment-fall-2005/lecture-notes/sec1_1.pdf
- Fault Tree Analysis Chapter 3 and 4, Marvin Rausand,
- RAMS Group Department of Production and Quality Engineering, NTNU Trondheim Norwegian University of Science and Technology, Slides related to the book System Reliability Theory Models, Statistical Methods, and Applications Wiley, 2004 , Marvin Rausand and Arnljot Hoyland
- System Safety : Traditional Hazard Analysis Lecture Notes , https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-863j-system-safety-spring-2016/lecture-notes/MIT16_863JS16_LecNotes4.pdf
- https://sixsigmastudyguide.com/fault-tree-analysis/
- Industrial Safety Engineering, Prof. Jhareswar Maiti, Department of Industrial and Systems Engineering Indian Institute of Technology, Kharagpur, Lecture – 12, Fault Tree Analysis (FTA) - Construction

Resources

- Chapter 5 Fault Tree Analysis (FTA) , Mary Ann Lundteigen and Marvin Rausand, RAMS Group Department of Mechanical and Industrial Engineering, NTNU Trondheim Norwegian University of Science and Technology
- Introduction to reliability Lecture Notes (Portsmouth Business School, April 2012)
- Fault&Event Tree Analysis, NITESH M. DONGARE https://www.slideshare.net/NiteshDongare/fault-event-tree-analysis
- Fault Tree Analysis, Part 6 Solution of Fault Trees http://slideplayer.com/slide/4613302/
- http://web.rec.org/documents/ECENA/training_programmes/2008_03_bristol/seveso_presentations/06_overview_of_ra1.ppt
- https://slideplayer.com/slide/7854255/
- https://softwaretestingtimes.com/2010/04/fault-error-failure.html
- https://risk-engineering.org/static/PDF/slides-reliability-engineering.pdf

Resources

- Chapter 3 Failures and Failure Classification, Marvin Rausand, RAMS Group Department of Production and Quality Engineering, NTNU Trondheim Norwegian University of Science and Technology, Slides related to the book System Reliability Theory Models, Statistical Methods, and Applications Wiley, 2004 , Marvin Rausand and Arnljot Hoyland
- Fault Tree Analysis, M. Pandey, University of Waterloo CIVE 240 – Engineering and Sustainable Development, http://www.civil.uwaterloo.ca/maknight/courses/CIVE240-05/Week%2011/Fault%20Tree%20Analysis.pdf
- Fault Tree Analysis, Clifton A. Ericson II, September 2000.
- Reliability Engineering, Kailash C. Kapur , Michael Pecht, 2014 , John Wiley & Sons, Inc
- Fault Tree Construction in Reliability Engineering, Chelliah Sundararajan, PhD, CED Engineering , Continuing Education and Development, Inc.