HOW TO AVOID FAILURES-(FMEA and/or FTA)

"*It is the responsibility of the practicing engineer and scientist to understand failures and their role in discovery, invention and design in order to minimize adverse effects to people and our environment.* "

Kuykendall's Fundamental Failure Theorem

"Drop-proof devices, bulletproof product and incorruptible metal" -It's engineered to last." Engineers like me giggle when we hear these assertion because we know that there is no superior system/product or infinitely successful systems in all conditions. Actually, whole system has failure modes and if exposed to enough physical energy, collision, loading cycles, or rough environment, everything can fail.

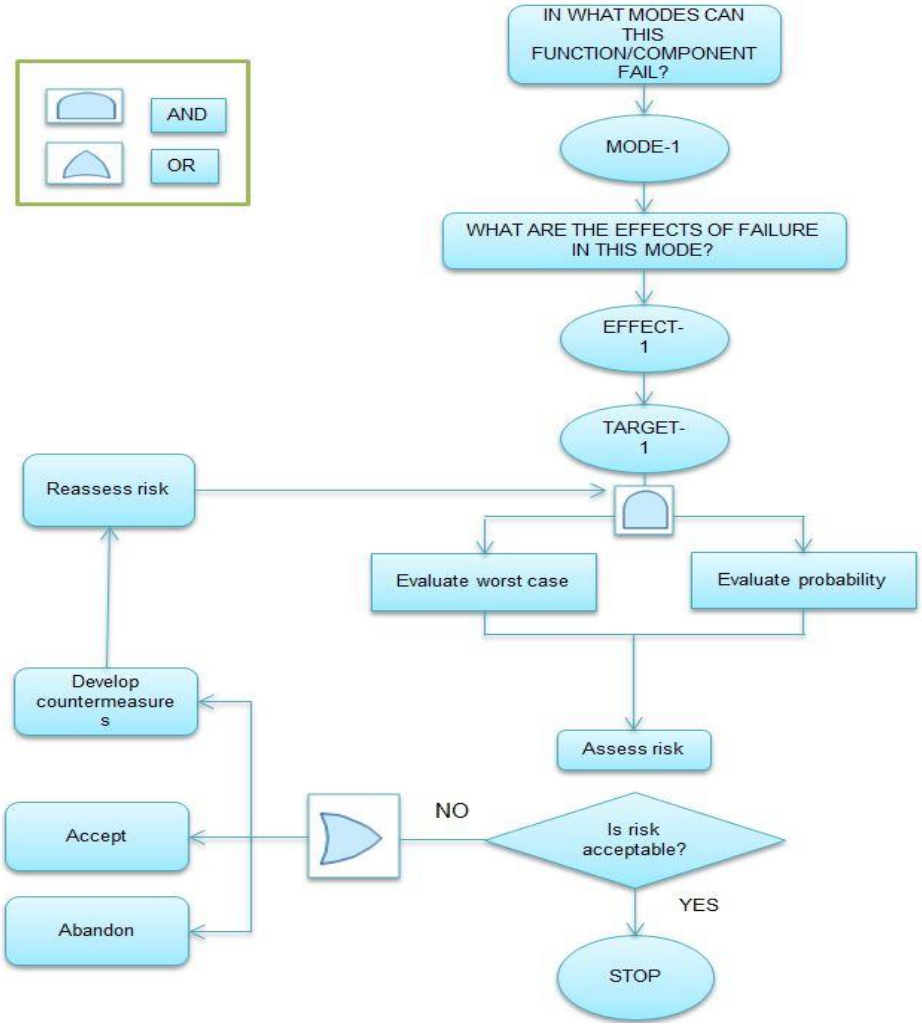
Potential failures of systems are focused on by safety assessments and an analysis of potential failures aids designers to effort on and comprehend the impact of potential process or product risks and failures. Modes, effects and impacts of failures have been determined and quantified by several systematic methodologies. Failure analysis is performed to prevent system malfunctions, insure system life and prevent safety hazards while using the system. On the other hand, system quality is insured, reliability of system is achieved and customer dissatisfaction is prevented by failure analysis.
There are several common failure analysis techniques such as;
Preliminary system safety analysis(PSSA), Even tree analysis, safety checklist& review, HAZOP(Hazard& operability) analysis, Cause and consequence analysis, fault tree analysis(FTA) and Failure modes and effects and criticality analysis(FMECA) etc. These techniques are utilized to obtain a better understanding of failure events and causative factors or to develop remedial actions for the prevention of failure recurrence and establish ownership of the failure and responsibility for remedial action.

FTA and FMEA are common but fundamentally different techniques;
"Fault Tree Analysis (FTA) is a deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, a Fault Tree Analysis is a "top-down" system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated." **SAE ARP4761**

"The Failure Mode, Effects and Criticality Analysis (FMECA) is a reliability evaluation/design technique which examines the potential failure modes within a system and its equipment, in order to determine the effects on equipment and system performance. Each potential failure mode is classified according to its impact on mission success and personnel/equipment safety." **MIL-STD-1629 REV.A**

FAILURE MODES AND EFFECTS ANALYSIS

Failure Modes and Effects Analysis (FMEA) is methodology for analyzing potential failures early in the development cycle where it is easier to take actions to overcome these issues, thereby enhancing reliability through design. FMEA is used to identify potential failure modes, determine their effect on the operation of the product, and identify actions to mitigate the failures. The Process flow of a FMEA is below;



A team approach and timeliness are particularly significant for FMEA. An effective Failure mode list can be prepared and consequences of failures can be evaluated by team approach. That is performed to preventive failures so timeliness is important. Design decisions can be steered between alternatives before failure modes are designed-in, rather than redesigning after the failure occurs. Main steps of a FMEA can be defined like as:

- ✓ Describe the system/sub-system/component
- ✓ Draw/review a block diagram of the product
- ✓ Break down the product into its components
- ✓ List all potential failure modes for each item
- ✓ Describe the consequences of each of the listed failure modes and assess the severity of each of these consequences on the system.
- ✓ Identify the possible cause(s) of each failure mode.
- ✓ Quantify the probability of occurrence of each of the causes of a failure mode.
- ✓ Identify all existing controls that contribute to the prevention of the occurrence of each of the causes of a failure mode.
- ✓ Determine the ability of each of the listed controls in preventing or detecting the failure mode or its cause.
- ✓ Calculate the Risk Priority Number (RPN) which is calculated via the formula;
- ✓ RPN= (Severity x Detection x Occurrence)
- ✓ Identify actions to address potential failure modes that have a high RPN
- ✓ Assign an individual responsible for implementation of the defined action(s) and a target date for completion.
- ✓ After the defined actions have been implemented the overall effect on the failure mode that the actions were supposed to address must be re-assessed and a new RPN calculated.
- ✓ The new RPN will help to determine if further action needs to be taken.
- ✓ Update the FMEA Table every time there is a significant change in the product design.

Although, FMEA has a lot of benefits, it has some weaknesses. Some of strengths and weaknesses are presented below.

Strengths	Weaknesses
The effect of various methods of mitigation/detection on risk can be modeled easily FMEA provide the designer with an indication of the predominant failures that should receive considerable attention while the product is being designed. Provides a well-documented record of improvements from corrective actions implemented. Provides information useful in developing test programs and in-line monitoring criteria. Provides historical information useful in analyzing potential product failures during the manufacturing process. Provides new ideas for improvements in similar designs or processes.	The relationship between different failure components is disregarded. Requires significant effort in establishing clearly defined terms. FMEA depends on subjective analysis and engineer's experience that are known by a small group of individuals, but fairly unknown and unmanaged at the enterprise level. Requires significant effort in assigning scores to each step

MIL-STD-1629 REV.A can be used for details about FMEA activities.

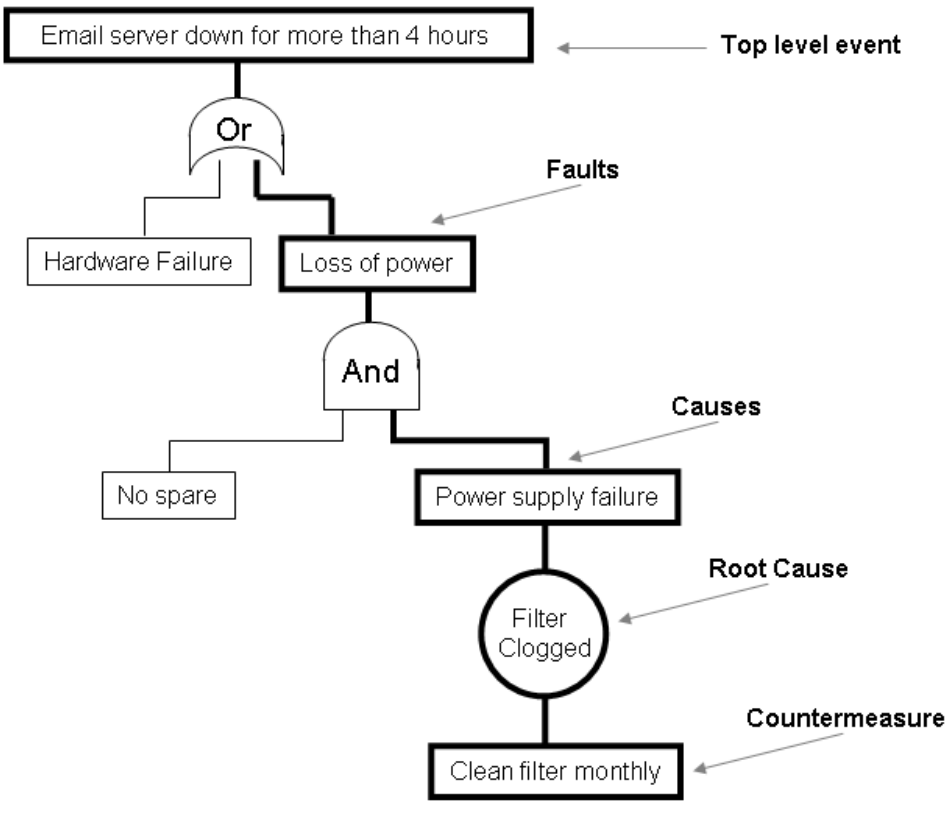
FAULT TREE ANALYSIS

Fault Tree Analysis (FTA) is a tool of failure analysis techniques. As a useful method it is applied in various industries, social and environmental problems for reconstruction, failure analysis, and failure frequency estimation. The Fault Tree process utilizes logic diagrams to portray and analyze potentially hazardous events. Steps to creating a Fault Tree Diagram are;

- ✓ Top event of the system shall be defined: Specify the problem on which the analysis will be made like open circuit, hose damage, leakage, engine stop etc.

- ✓ Tree top Structure shall be defined: Define the events and the conditions that lead to the top event. Explore each branch in successive level of details: Determine the events and conditions that lead to the intermediate event and keep repeating this process at different successive levels unless the fault tree is completed.
- ✓ Fault tree for the combination of events contributing to the top event shall be solved: Examine all the event and conditions that are necessary for the top event to occur and develop a minimal cut set.
- ✓ Significant dependent failure potentials shall be identified: Study the event and find the dependencies among the event that can cause a single or multiple events and conditions to occur simultaneously.
- ✓ Quantitative analysis shall be performed: Use the past statistical data to evaluate or predict the future performance of the system.
- ✓ The results in decision making shall be used: Find the conditions in which the system is at most potential hazard and place appropriate measure and recommendations to counter with such risk.

An example of FTA;



There are benefits and limitations in FTA as in FMEA. The most significant benefits and limitations are presented below:

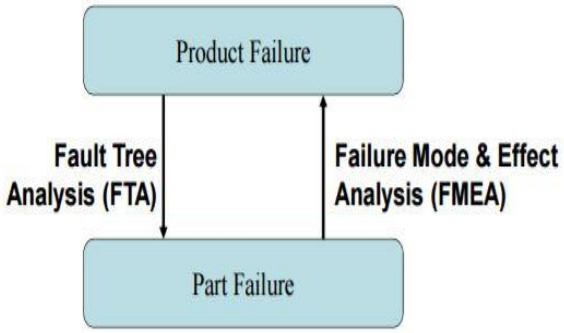
Benefits	**Limitations**
Deductive failure identification; all the different relationships that are necessary to result in the top event are showed by FTA. Full range of causes for a failure is included such as hardware, software and human factors. In constructing the fault tree, a thorough understanding is obtained of the logic and basic causes leading to the top event The fault tree is a tangible record of the systematic analysis of the logic and basic causes leading to the top event You can use a fault tree diagram to help you design quality tests and maintenance procedures. The fault tree provides a framework for thorough qualitative and quantitative evaluation of the top event In many ways, the fault tree diagram creates the foundation for any further analysis and evaluation. Critical elements related to system failure are highlighted. The FTA process may lead to a single component or material that causes many paths to failure, thus improving that one element may minimize the possibility of many failures. Graphics, and for complex systems it helps to focus the team on critical elements. Expose system behavior and possible interactions.	Fault tree analysis may lead to very large trees if the analysis is extended in depth. It depends on skill of analyst. Furthermore, it is difficult to apply to systems with partial success. Another shortcoming is that it can be costly in both time & effort.

Fault Tree Handbook with Aerospace Applications (Prepared for NASA Office of Safety and Mission Assurance NASA Headquarters/2002) can be used for details of FTA activities.

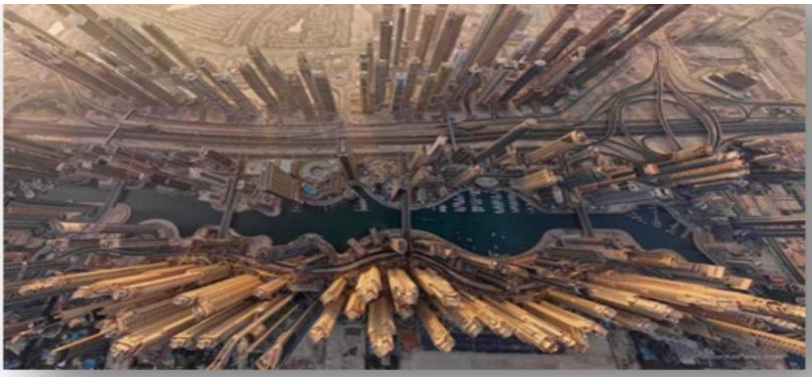
COMPARISON OF FTA AND FMEA

The main difference between FTA and FMEA is system approach. Even though FTA is a top-down approach, FMEA is a bottom-up approach.

FTA is a deductive method and it is not an FMEA which assesses different effects of single basic causes. “How resistant a system is to single or multiple initiating faults” can be showed by FTA well but FTA is not good at finding all possible initiating faults. FMEA is good at exhaustively cataloging initiating faults, and identifying their local effects. It is not good at examining multiple failures or their effects at a system level. FTA considers external events, FMEA does not. Both FTA and FMEA are usually performed in civil aerospace practices, with a Failure Mode Effects Summary as the interface between FMEA and FTA.



Top-down approach and bottom-up approach can be defined via the photographs which are below.



If we have similar failure more than once, maybe it is high time we become an investigator or hire one. If similar failure occurs again and again, it has to be a shame for us.

Be safe!