RISK ASSESMENT: FAULT TREE ANALYSIS

Afzal Ahmed[+], Saghir Mehdi Rizvi*Zeshan Anwer Rana* Faheem Abbas*
[+]COMSAT Institute of Information and Technology, Sahiwal, Pakistan
*Navy Engineering College
National University of Sciences and Technology, Islamabad
drafzal@ciitsahiwal>edu.pk, 03452325972

ABSTRACT

The failure of engineering equipment causes loss of capital as well as human loss, injuries, and stoppage of production line. The hazards can be classified as safe, minor, major, critical and catastrophic Risk analysis or hazard analysis pin points the potential failures of engineering systems and or components when being used.. Failure mode and effects analysis is used to identify hazard and to make system safer. A system is broken down up to level of components and using reliability data the safety or probability of failure of assemblies and the system can be calculated. The failure mode and effects analysis is used with fault tree analysis to point the areas of a complex system where failure mode effect analysis is required. Fault tree analysis (FTA) is a technique which pinpoints any failure or severe accidents. It tells how things fail rather than emphasize on the design performance. It is a logic diagram connecting inputs an outputs using Boolean algebra. This paper shows how FTA can be applied to car carburetor failure and car brake failure.

Key words : Risk Management, Reliability, Fault tree, Failure mode

INTRODUCTION

The world is full risk. We are at risk of accident when crossing a road or driving. We are at risk living in an apartment not properly designed. An operator of machine is at risk while working on machine not designed with safety consideration. Engineering job is much dependent on involvement of risk. As the projects or products made by engineers are used by society and if not properly designed may cause accidents ranging from major to minor. A failure of an aircraft may cause death to passengers, while a machine may cause injury or death to an operator. The risk of accidents can be reduced by abiding ethics and acquiring in depth knowledge and experience by engineers. Avoidance of risk of accidents is also dependent upon: the use of appropriate materials of good quality, applying proper safety factor, accurate design analysis, ergonomic design, vetting of design, inspection

and quality control, clear easier and understandable operating procedures of machines, lighting arrangements to provide visibility, implementing the preventive maintenance schedule and in time replacement of worn out and damaged parts.

Regulations are made to protect the society from hazards of failure or emission of toxic gases. This puts pressure on the manufacturers because of increased cost incurred. Standards are made for maximum safety and performance. A mandatory standard is specified by government and its violation can result in fine or imprisonment. A voluntary standard is made by the interested parties to abide. It indicates the lowest safety level that an industry puts in the product it manufactures.

Risk is related to reliability in the sense that high risk of failure means less reliable. The reliability is the probability that a system, component, or device will perform without failure for a specified period of time under specified operating conditions [1]. The hazard rate or the instantaneous failure rate is the number of failures per unit of time per the number of items exposed for the same time.

CAUSES OF RISK OR UNRELIBILITY

An engineering system can experience malfunction [1] because of:

a. Design mistakes such as not including important operating factors, incomplete loading, poor selection of materials and mistakes in calculations.
b. Manufacturing defects such as poor surface finish and sharp edges which can lead to fatigue cracks. The defects can also result from poor workmanship, poor supervision and lack of training of workers.
c Engineering system are designed to have maintenance schedule which if not followed service life will be reduced. Since customers are lazy in maintenance of product to design a maintenance free product would be a good strategy.
d. The design limits being exceeded.
e. Subjecting equipment to environments for which it was not designed

HOW TO MINIMIZE RISK OF FAILURE

Following are some methods to minimize failure [1]:

a. Failure can be reduced by reducing the variability in strength of materials.
b. The reliability of equipment can be increased by using equipment at a de-rated value.
c. Using equipments in parallel will cause load sharing and equipments are de-rated and will work longer than its normal life.

d. The durability can be increased by protecting from corrosion, erosion and using high performance materials.
e. The cracks should not be allowed to grow beyond critical value and should be monitored by non-destructive testing equipments.
f. The simplification of assemblies and components reduces chances of failure.
g. Using standard items reduces risk of failure.

RISK ANALYSIS

A number of techniques have been developed to identify potential causes of failure [1, 2].

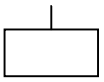
Failure Modes and Effects Analysis

Failure modes and effects analysis is the study of malfunctions of components of engineering systems. Here the system is broken into assemblies, subassemblies and the components it comprises of. From the operating and environmental conditions failure conditions of each component is determined and failure modes of all components are identified. Each failure mode is analyzed to determine whether it has an effect on next higher item or the entire system. The probability of failure of the entire system can be calculated from the reliability theory.

FAULT TREE ANALYSIS

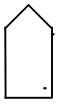
Fault tree analysis is a technique [1,2] that provides a combination of possible occurrences that can result in failure or severe accidents. FTA tells how things can fail to work. FTA is a logic diagram which uses logic gates to determine relations between input events and output events. In this paper two examples are presented for constructing a FTA of Carburetor failure and Car brake failure.

FTA is a top down approach that starts with top event and then determines the contributory events that would lead to top event. The top event could be hardware failure or human error. Events are described by symbols on FTA diagram and are stated in the following:

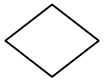


An output event should be developed further to determine how it can occur. This symbol will have logic gate and input events below it, except when it serves as an undesireable event at the top. A rectangle can also serve as an input event to another

An independent event that does not depend for its occurrence on other components within the system

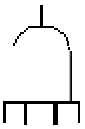


A normal event is an event that is expected to occur unless a failure occurs.

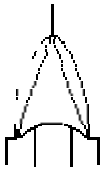


An undeveloped event that has not been developed because of lack of information or it has no sufficient consequences

A transfer symbol is a connection to another part of a fault tree within the same branch.



The AND gate is used to represent a logic condition in which all the inputs below the gate must be present for the output at the top of the gate to occur.



The OR gate is used to represent the situation in which any of the input events will lead to the output.

Figures 1 shows the Fault Tree for Carburetor failure. The top output event shows the Carburetor failure. Down the top event shows how failure can happen using the relevant symbols. A carburetor can fail because of any of three causes, lack of fuel, loss of adjustment of butterfly and spring assembly or malfunction in fuel flow. Similarly the lack of fuel could be because of any of the reasons that is fuel tank empty, fuel pump fault or fuel line choked. In the same way, loss of adjustment of butterfly, spring assembly could be because of failure of butterfly assembly, or spring fault or air leakage in butterfly valve. The carburetor failure could be because of fault in fuel flow such as dirt particles in fuel, or choking of tubes or malfunctioning of valves or accelerator cable disconnected.

Figure 2 shows the Fault Tree of Car brake failure. A car brake can fail because of any of the problem that is brake oil problem, brake paddle not properly engaging and brake shoes not functioning properly. The brake oil problem could be due to finishing of brake oil, or leakage of brake oil or brake oil line choked or infiltration of air in brake oil lines.

Similarly, brake paddle may not be engaging properly because the master cylinder kit is worn out or paddle needs adjustment.

The brake shoe may not be functioning properly.

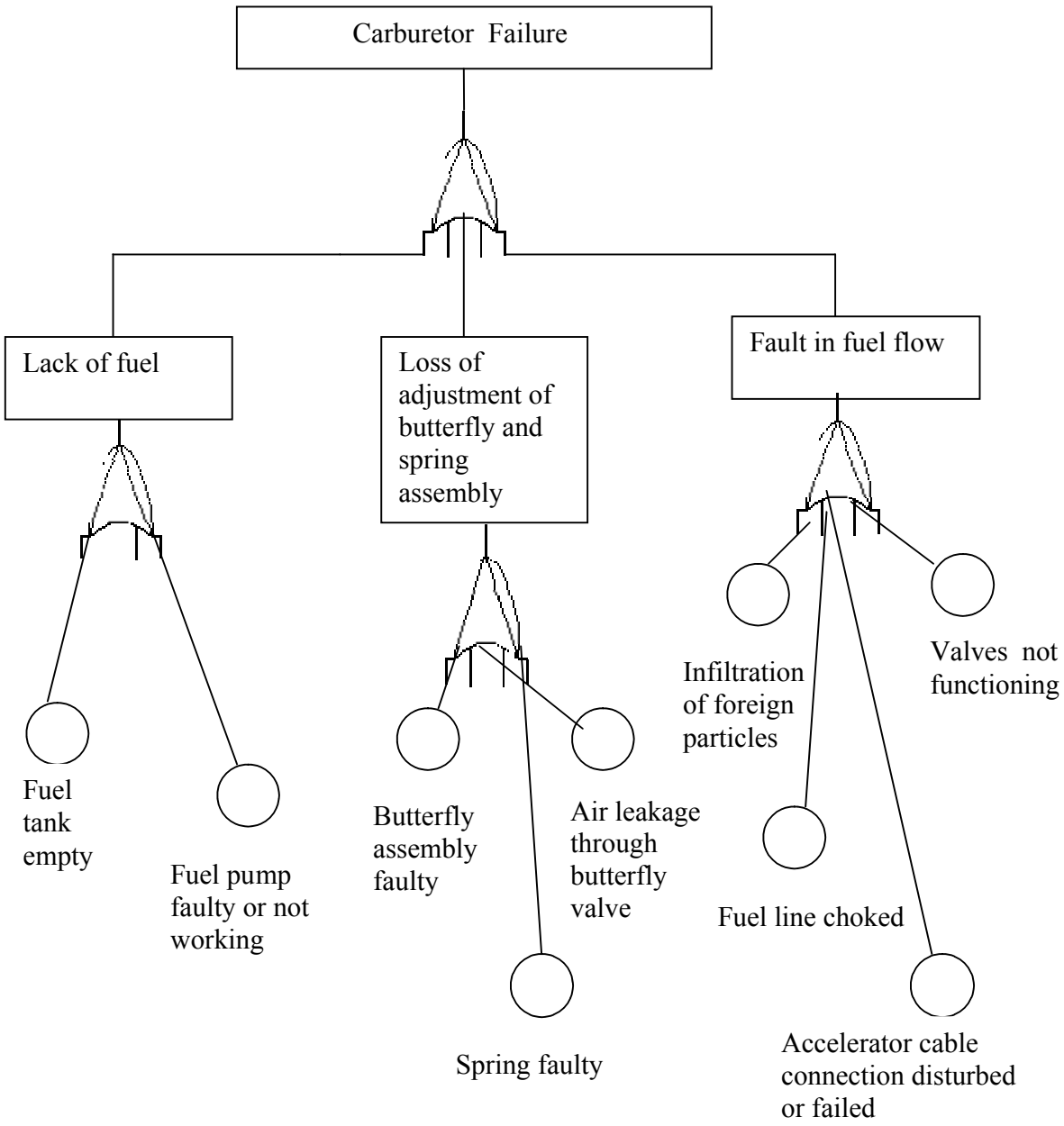


Figure 1: Fault tree analysis of carburetor failure

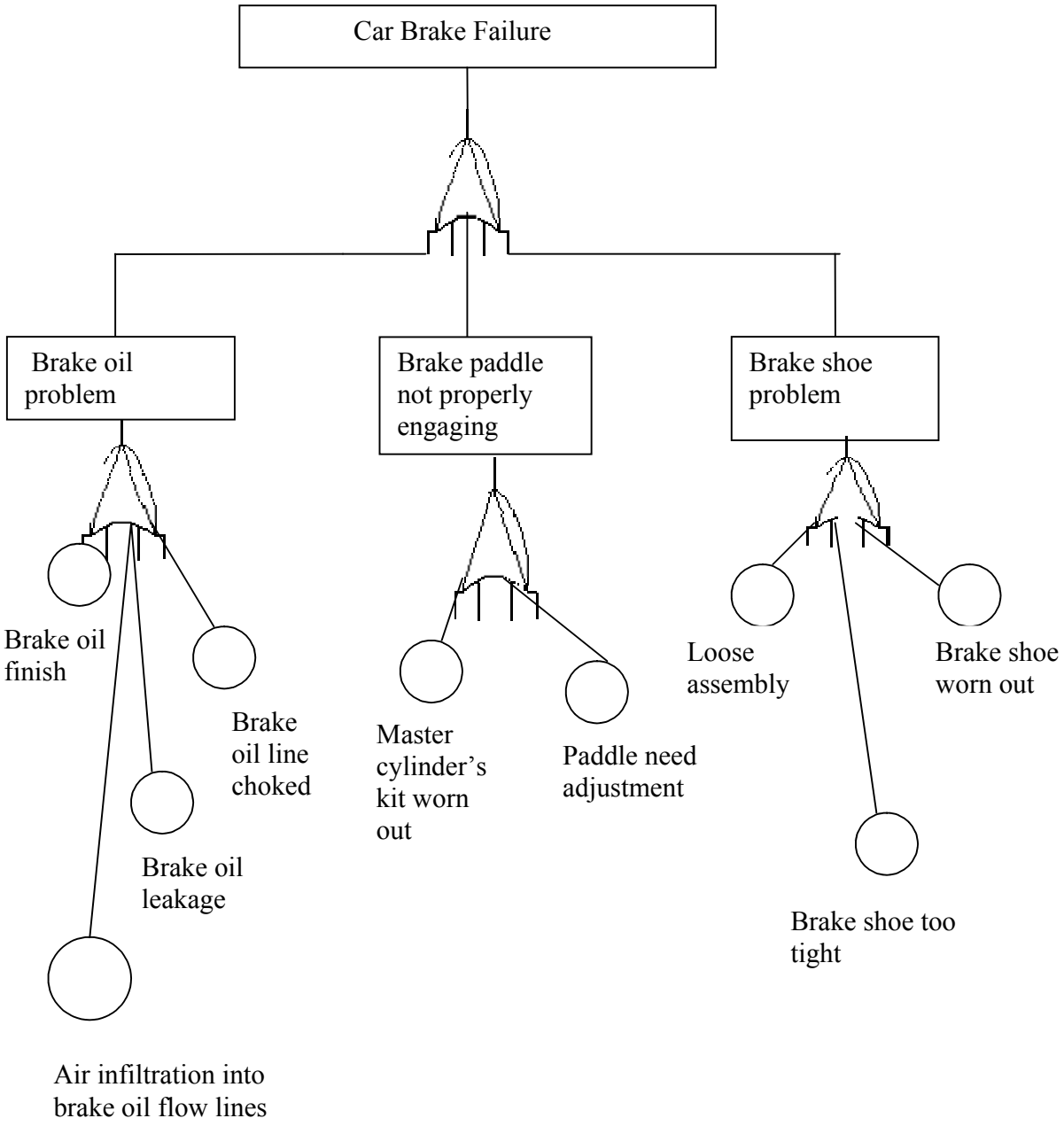


Figure 2 : Fault tree analysis of car brake failure

The car brake can also fail because the brake shoe is connected loosely or brake shoe is too tight or brake shoes are worn out.

CONCLUSION

To minimize the risk of failure it is imperative to increase the reliability of the system. For this Failure Modes and Effects Analysis is applied where the system is broken in assemblies and components. If the reliability of components are known the system reliability can be obtained using the established reliability methods. Fault tree analysis is of great help in this regard as here the causes of failure are clearly earmarked.

REFERENCES

[1] George E. Dieter, Engineering Design, McGraw Hill, 1991. pp 536-537, 547-551,553-556.

[2] Guide Lines for Failure Mode and Effect Analysis, Dydem Press, 2004