International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Fault Tree Analysis of LPG refuelling station

Maniram Kumar. A
Department of Mechanical Engineering,
Dr Sivanthi Aditanar College of Engineering,
Tiruchendur,India

Rajakarunakaran. S
Department of Mechanical Engineering,
Ramco Institute of Technology,
Rajapalayam, Virudhunagar District - 626117,
Tamilnadu, India.

***Abstract*— Fault tree analysis (FTA) is a top-down approach for analysis of the reliability and safety of technical systems. It starts with a possible failure event, called a TOP event, and then determining the ways it can happen. The analysis proceeds by determining how the TOP event is caused by lower level failure events. The primitive or basic failure events that ultimately cause the TOP event are connected through logical AND-gates and OR-gates. As an example of the practical application of methods, the lpg release accident of a LPG refueling station is analyzed, the estimation of the significance of certain events is done that have a greater or less influence on its reliability, and it is considered to be able to eliminate causes of failure or to minimize the consequences of failure.)**

Keywords—Fault tree analysis, reliability, risk assesment, LPG release

1. INTRODUCTION

The Fault Tree Analysis is one of the methods used for analysis of the technical system's reliability and safety. FTA is a deductive method, where at first, the so-called top event, which at the technical systems represents a failure, and then the possible causes of this failure inside the system are analyzed. Basis of the fault tree represents a transformation of physical systems to the structural logic diagrams.

The FTA method was invented and developed at Bell Telephone Laboratories in connection with a US Air Force contract to safety study of the Minuteman Launch Control System by H. A. Watson in 1961 [11]. The method was developed further by, D. F. Haasl of the Boeing Company by application to a wide variety of industrial safety and reliability problems [3]. Boeing in 1966 was the first commercial company that started to use the FTA for the development of commercial aircrafts [4]. In the seventies, the method was used in particular in the area of nuclear power techniques. From its beginnings until today, the FTA was used for failure analysis of different technical systems. This method is especially convenient for the reliability and safety analysis of the systems whose failures might cause catastrophic consequences for mankind and environment.

A fault tree is a tangible record of the systematic analysis of the logic and basic causes leading to the top event. It provides a framework for thorough qualitative and quantitative evaluation of the top event. It depicts a logical model of the relationship of the undesired event to more basic events. The top event of the fault tree is the undesired event. The middle events are intermediate events. The bottom of the fault tree is the causal basic events or primary events. The logical relationships of the events are shown by logical symbols or gates. Using data on the probability of the causes, the probability of system failure is determined. The probability of the accident scenario is thereby determined.

The data on the probability of the causes to determine the probability of system failure can be derived out from generic data, plant-specific operational data, equipment data, and event data. Generic failure data bases provide generic failure data collected from a variety of sources. This generic data needs to be screened for the applicable failure mode and environment. The generic data can also be updated using mission specific data. . In circumstances where a lack or incompleteness of data exists, there is a need to incorporate expert judgements into risk research. Sensitivity studies can be carried out to check the impact of the estimates.

In this paper, Section 2 introduces basic methodology of FTA. Section 3 describes a case study of a LPG refueling station and Section 4 gives the conclusion.

2. METHODOLOGY OF THE FAULT TREE ANALYSIS

The FTA methodology is described in several industry and government standards, including NRC NUREG–0492 [5] for the nuclear power industry, an aerospace-oriented revision to NUREG–0492 for use by NASA [6], SAE ARP4761 for civil aerospace, MIL–HDBK–338 for military systems [2] for military systems. Many different approaches can be used to model the FTA. Based on the analysis of implementation procedures of the FTA described in the above standards and references starting from [4], over [1] to modern literature references from the subject area [1,7], the FTA methodology is comprises the following steps:

A. Steps in Carrying Out a Fault Tree Analysis

A successful FTA requires the following steps be carried out:

1. Identify the objective for the FTA.
2. Define the top event of the FT.
3. Define the scope of the FTA.
4. Define the resolution of the FTA.
5. Define ground rules for the FTA.
6. Construct the FT.
7. Evaluate the FT.

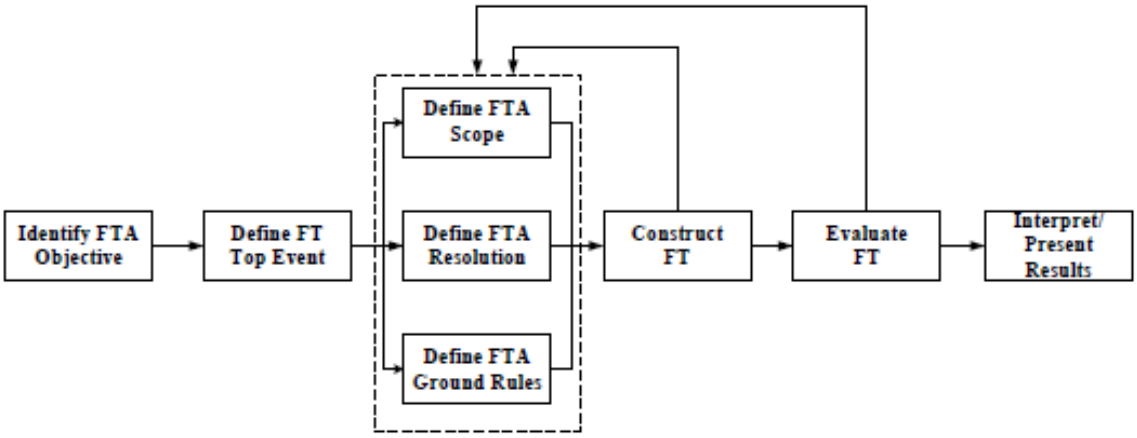


Fig 1. Fault Tree Analysis Steps

8. Interpret and present the results.

The first five steps involve the problem formulation for an FTA. The remaining steps involve the actual construction of the FT, the evaluation of the FT, and the interpretation of the FT results. While most of the steps are performed sequentially, steps 3-5 can proceed concurrently. It is not uncommon for steps 4 and 5 to be modified during steps 6 and 7. The interrelationship of the eight steps are shown in Figure 3-1. The feedback is indicated in the figure.

The **first step** for a successful FTA is to define the objective of the FTA. The analysis should satisfy the objective of the decision maker or manager who commissioned it. To be successful the objective should be phrased in terms of a failure of the system to be analyzed.

In **Step 2** the top event of the FT is defined once the objective is defined. The top event of the FT is the event for which the failure causes will be resolved and the failure probability determined. The top event defines the failure mode of the system that will be analyzed. Sometimes the objective may entail defining and analyzing more than one failure. In this case separate top events are then defined.

In **Step 3**, the scope of the analysis is defined. The scope of the FTA indicates which of the failures and contributors will be included and which will not be included. The scope of the FTA also includes the particular design version and historical time period relevant to the system that will be analyzed. Finally, the scope includes the boundary conditions for the analysis. The boundary conditions include the initial states of the components and the assumed inputs to the system. The FT represents a snapshot of the system at a given time for a given configuration and boundary.

In defining the scope, the version of the system to be analyzed is identified, the modes of operation defined, the component failures to be considered are indicated, and the interfaces to system (e.g., support systems, actuation signals) that will be modeled for their failures or that will be assumed to not fail are identified.

In **Step 4** of the process, the resolution of the FTA is defined. The resolution is the level of detail to which the failure causes for the top event will be developed. If the top event is a functional failure of the system, such as failure to operate or inadvertent shutdown, then the top event is generally resolved to the major components in the systems. Examples of major components are valves, pumps, and control modules. If the top event is a phenomenological failure such as a catastrophic explosion of an engine then the resolution is the level of detail to which the causes of the explosion will be modeled. The development of a quantitative model is based on the need to get the best possible estimate for the top event probability, considering the data and other information that are available. Fault trees are developed to a level of detail where the best failure probability data are available. Further resolution of the system is necessary when decisions about subcomponents or support systems are being made, or when an event cannot be shown to be independent of others in the analysis (e.g., a system that has actuation signals or power in common with other systems).

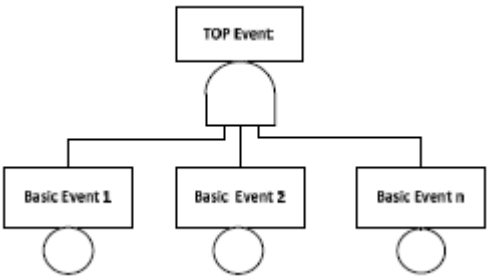
In **Step 5**, any ground rules for the FTA are defined. These ground rules include the procedure and nomenclature by which events and gates are named in the FT. The naming scheme used is very important in creating an understandable FT. Examples of naming schemes are given for the FTs that will be illustrated. Ground rules can also be given for the manner in which specific failures are modeled in the FT. These modeling ground rules are useful in providing consistency among different FTs especially when different individuals are developing them. The modeling ground rules can include the manner in which specific component failures, human errors and that can be used will be described. The FTs that will be presented will also illustrate some modeling ground rules that have been applied.

Step 6 involves the actual construction of the FT. A tangible record of the systematic analysis of the logic and basic causes leading to the top event is drawn. It provides a framework for thorough qualitative and quantitative evaluation of the top event.. The top event of the fault tree is the undesired event. The middle events are intermediate events. The bottom of the fault tree is the causal basic events or primary events. The logical model depicts the relationship of the undesired event to more basic events. The logical relationships of the events are shown by logical symbols or gates. Using data on the probability of the causes, the

probability of system failure is determined. The probability of the accident scenario is thereby determined

A fault tree can be modeled by a set of AND gates and OR gates connecting between basic events and intermediate events as shown in Fig. 2 and Fig. 3 respectively where:

AND gate with m basic event is given by:



$$Q\ \ (t) = \prod_{j=1}^{m} Q_j(t) \quad (1)$$

Fig.2 AND gate connecting *m* basic events

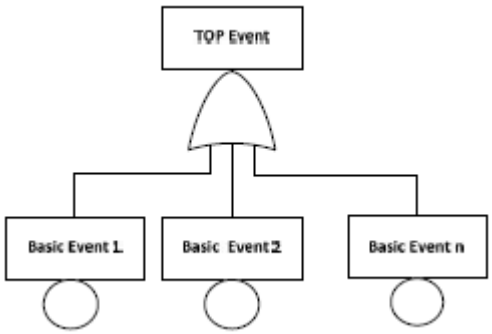


Fig.3 OR gate connecting m basic events

OR gate with m basic events is given by:

$$Q\ \ (t) = 1 - \prod_{j=1}^{m}(1 - Q_j(t)) \quad (2)$$

Step 7 involves the evaluation of the FT. The evaluation includes both a qualitative and quantitative evaluation. The qualitative evaluation provides information on the minimal cut sets for the top event. The nature of the basic events and the number of basic events in the combined sets give important information about the top event occurrence. Cut sets are usually sorted by cut set order (the number of events in a cut set) to provide information on the combinations of basic events that can result in the top event. The quantitative evaluation produces not only the probability of the top event but also the dominant cut sets that contribute to the top event probability, as well as quantitative importance of each basic event contributing to the top event. Cut sets in this case are sorted by probability, and low probability cut sets are truncated from the analysis. Different quantitative importance is determined for different applications. Sensitivity studies and uncertainty evaluations provide further key information.

A cut set in a FT is a set of basic events whose simultaneous occurrence ensures that the top event occurs. A minimal cut set fails if and only if the basic events in the set fail at the same time as shown in Fig. 4. It is assumed that all the r basic events in the minimal cut set j are independent.

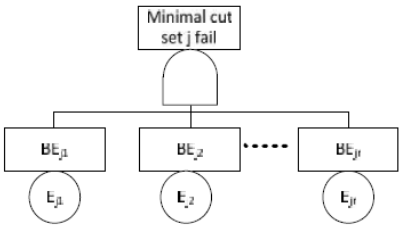


Fig. 4 Minimal cut set

The probability that the cut set j fails at time t is:

$$Q_o(t) = \prod_{r=1}^{i} Q_r(t) \quad (3)$$

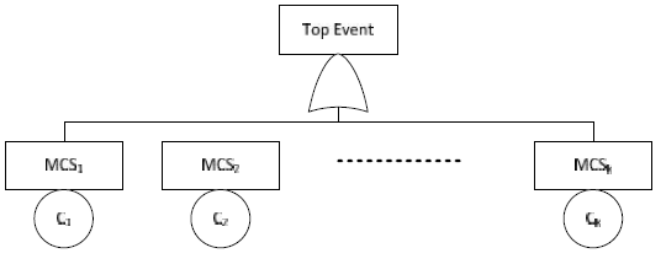


Fig 5. Fault tree represented by minimal cut sets

Any fault tree will consist of a finite number of MCs that are unique for that TE. By definition, an MCS is a combination (intersection) of BEs leading to the TE. The combination is a minimal combination in that all the failures are needed for the TE to occur; if one of the failures in the MCS does not occur, then the TE will not occur (by this combination). One-component MCSs, if there are any, represent those single failures that will cause the TE to occur. Two-component MCSs represent the double failures that together will cause the TE to occur. If the probabilities of all the basic events were given, the failure occurrence probability of the undesired top event would be achieved. By successive substitution, each gate event is express in terms of basic events. The resulting equations provide a basis for qualitative and quantitative evaluations. Using data on the probability of the causes, the probability of system failure is determined. The probability of the accident scenario is thereby determined.

An important objective of many reliability and risk analyses is to identify those components or MCSs that are the most important (critical) from a reliability or risk viewpoint so that they can be given priority with respect to improvements. Both intermediate events (gate events) as well as MCSs can be prioritized according to their importance.

Fussell-Vesely Importance Measure (F-VIM) is the contribution of the MCSs to the TE probability. F-VI measures are determinable for every MCSs modeled in the fault tree. This provides a numerical significance of all the fault tree elements and allows them to be prioritized. The F-VI is calculated by summing all the causes (MCSs) of the TE involving the particular event. This measure has been applied to MCSs to determine the importance of individual MCS. Where Q_i (t) is the contribution of MCS to failure of

the system, F-VI measure that can be calculated for each MC in the fault tree can be quantified as follows[10]:

$$Q_{TE}(t) = 1 - \prod_{o=1}^{k}(1 - Q_o(t)) \quad (4)$$

$Q_j(t)$ =Probability of failure of MCS i

$Q_S(t)$ = Probability of failure of TE due to all MCS

Top Event importance measure can be used for prioritization in FTA for different types of applications. Such importance measures establish the significance for all the MCSs in the fault tree in terms of their contributions to the TE probability.

In a sensitivity analysis, an input data parameter, such as a component failure probability is changed, and the resulting change in the TE probability is determined. This is repeated for a set of changes using either different values for the same parameter or changing different parameters, e.g., changing different failure probabilities. Usually for a given sensitivity evaluation, only one parameter is changed at a time. This is called a one-at-a-time sensitivity study. This method is employed here to validate the sensitivity of the proposed model. RRW is employed to perform sensitivity analysis. The RRW can be calculated by setting a MCS probability to 0. Risk Reduction Worth (RRW) measures the decrease in the probability of the TE if a given MCS is assured not to occur. This importance measure can also be called the Top Decrease Sensitivity (TDS). Therefore, the RRW can be calculated by re-quantifying the fault tree with the probability of the given MCS to 0. It thus measures the maximum reduction in the TE probability. An RRW value is determinable for every MCSs in the fault tree.

RRW = Top event probability - Top event probability with event probability set to zero

The ranking enables to identify which component mostly determine the overall system behaviour, trace system bottlenecks and provide guidelines for effective system improvement

Finally, **Step 8** involves the interpretation and presentation of the results. Emphasis is placed upon the interpretation to provide tangible implications, especially concerning the potential impact upon the objective. The FTA may be used to understand of the logic leading to the top event, to prioritize the contributors leading to the top event, to prevent the top event, to monitor the performance of the system, to minimize and optimize resources, to assist in designing a system, as a diagnostic tool to identify and correct causes of the top event.

3. CASE STUDY:

A case study of Fault Tree Analysis (FTA) in LPG refueling station is investigated in this paper. There are a number of possible hazardous scenarios which can occur with a LPG installation, irrespective of its size. These are well documented in the literature, with the most significant hazards being:

- Boiling Liquid Expanding Vapour Explosion BLEVE). Occurs in this case the escaping liquid expands very rapidly i.e. it `boils'), and, if ignited at or near the source of release, burns at a great rate.
- Unconfined Vapour Cloud Explosion UVCE). This occurs when a cloud of LPG, leaked from the tank with- out ignition taking place, is ignited at a later time at a source perhaps some considerable distance from the release point.
- Flash fire. This is a lesser form of UVCE, usually involving less gas and hence energy output.
- Jet fires. These are caused by the ignition of LPG escaping from a facility due to fracture of pipelines, valves and fittings, hoses etc. and minor leakage such as due to flange weep.
- Pool fires. These are caused by leakage and ignition of the liquid phase when it does not immediately drain away.

  Initiating events which can lead to the above consequences considered in the risk study are as follows
- Cold Catastrophic Failure: (CCF) is a catch-all term describing an apparently sudden failure of the tank. Postulated causes include metal fatigue and fracture, overfilling followed by excess pressure build-up and fracture, weakening of the vessel due to metal corrosion etc.
- Flame impingement: following rupture of pipe work or hoses and ignition of releasing LPG
- Impact e.g. from vehicles etc.: leading to rupture of hoses or pipe work
- Negligent action by operators, tanker drivers etc. : this include operator uncoupling hoses with valves open, attempts to disconnect hose with trigger activated, tanker driving away whilst still connected by hoses
- Poor maintenance: may include hose wear and tear, corrosion of springs etc., in relief valves, pump seal failure, foreign bodies in valve seats, connection seats etc., and
- Vandalism: including attempts to access liquid LPG via the drain valve.

The system studied is adopted from the work of Melchers RE and Feutrill WR (2005), an overview of the review process performed at Australian Standards level by subcommittee ME15/2 on behalf of Australian State planning and environmental authorities, sought after reviewing of the clearance distances for single occupancy low-rise domestic dwellings in the older version of Australian Standard AS1596-1997 to which the requirements of LPG storage tanks and dispensing facilities are subject to.

A typical above-ground facility as described in literature is shown in Fig.7. LPG tanks are designed to meet the requirements for wall thickness, material and welding to AS 1210 Class 2A. All pipework is constructed to AS 4041 and is traced with polyethylene tubing which is pressurised by air and is connected to an automatic shut down system. In addition, equipped with a emergency shutdown system which can be activated to cut off the electricity supply to the pump and release the automatic stop valves, thereby stopping the supply of LPG. On the purview of the authors, fatigue failure of the tank wall, corrosion is a negligible hazard, considered to be a result of good industry maintenance practices.

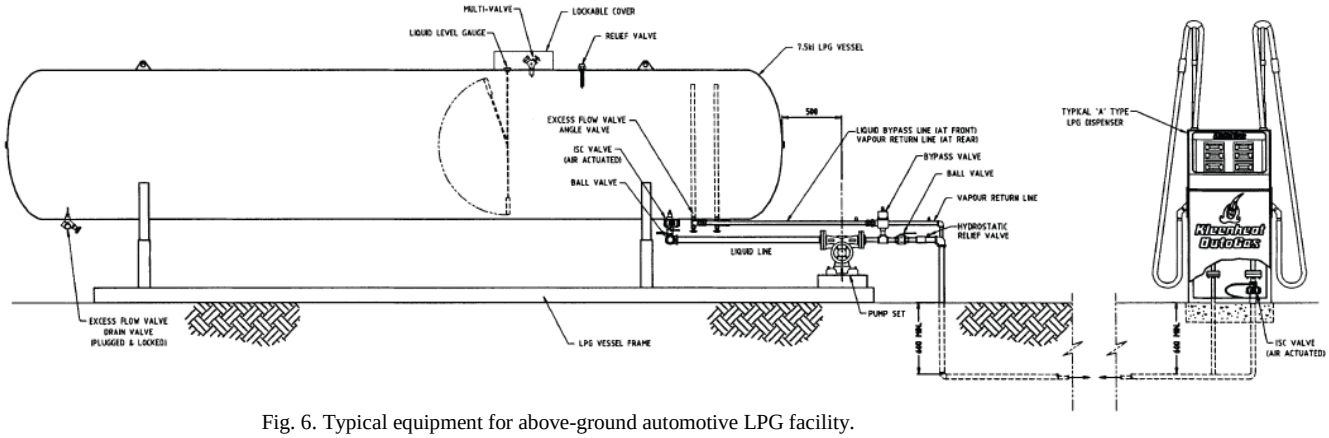


Fig. 6. Typical equipment for above-ground automotive LPG facility.

The tanks are refilled from LPG road tankers using high-grade rubber hoses. There is a recognised but small risk involved with this operation, associated with making and maintaining the coupling, disengaging the pumps and uncoupling in an appropriate sequence. To prevent the tanker driving away with the fill hoses still connected, drive-away locks are fitted as standard equipment to road tankers. The presence and location of a road tanker on the site of a service station can constitute a hazard, both in terms of impact of other vehicles on the tanker, its equipment and the refilling hoses, and its disruptive nature generally.

3.1. Fault Tree Development

The objective of the fault tree is to model a top event of LPG release in a LPG refuelling facility. All major components like the over ground tank, piping shown in the system schematic and the major process of decanting form tanker and filling operations carried out normally are considered as the boundary to be studied. The common cause failures are not considered under the scope of the tree. The fault tree resolves the basic causes to above mentioned boundary with the prospective causes available in the work. The fault tree assumes the initial state of the system to be normal working refuelling pump station. The logical relationships of the events are shown by logical symbols or gates. The basic events are assumed to be independent. The failure probabilities are assumed to be fixed probabilities.

The customised fault tree developed consists of 15 basic events which covers the various failures in transfer hose coupling, hose reel medium, storage tank, drain valve, safety relief valve, vapour return line, liquid outlet line, dispenser nozzle and damages due to vehicle impact, and negligent action due to drivers, operators, etc. is made for expert evaluation. The basic event failure probabilities are enlisted from the work of Melchers RE and Feutrill WR (2005),

Table 1: Basic events and failure probabilities (from literature)

Basic events	Description (Failure of components)	Failure rate (x 10^{-6}/year)
B1	Transfer hose coupling (small)	24,600
B2	Hose reel (medium)	3.46
B3	Tanker SRV	0.19
B4	Cold catastrophic failure	0.12
B5	Drain valve (small)	120
B6	Safety relief valve of storage tank	0.53
B7	Vapour return line (small)	1000
B8	Liquid outlet line (small)	5
B9	Liquid outlet line (medium)	2.3
B10	Liquid outlet line (large)	0.56
B11	Vehicle impact (small)	4.5
B12	vehicle impact (large)	2.43
B13	Dispenser nozzle (small)	200
B14	Vehicle drive-away (small)	667
B15	Vehicle impact (hose or dispenser)	667

3.2 Failure Probability of Top Event:

The fault tree developed generated 15 basic events which are connected by OR gates by the scope mentioned earlier. The failure combinations resulted in 15 one-component MCs which contribute to the occurrence of the TE. With the probabilities of all the basic events derived out from literature, the failure occurrence probability of the undesired top event is achieved.

Table 2**:** Top Event Probability

Top Event probability	Failure probability
	2.720480E-02

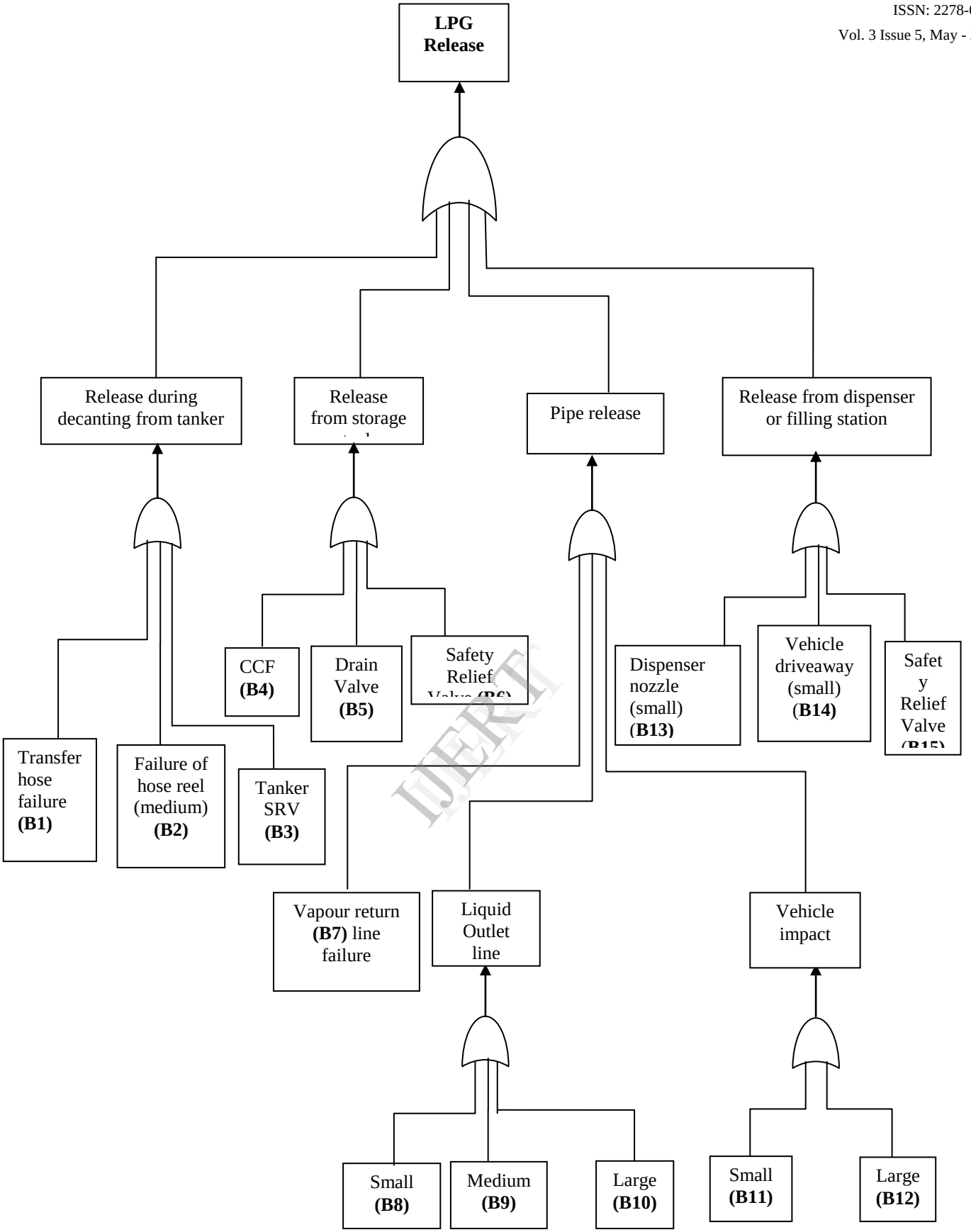
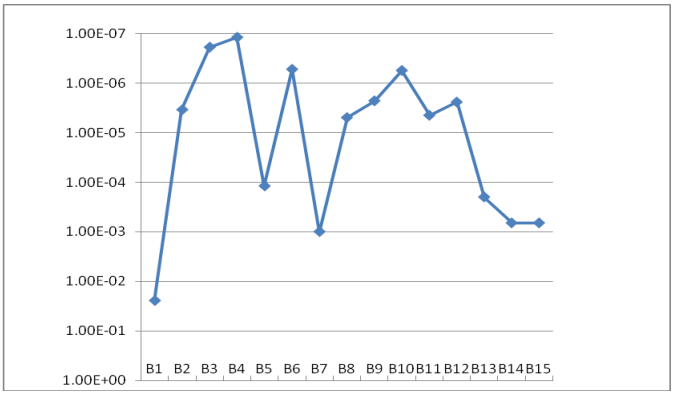


Fig 7. Fault tree of LPG release



Graph 1: Failure probability comparison for basic events B1-B15
(Lograthmic variation of probability values)

3.3 IMPORTANCE RANKING:

One of the most important outputs of an FTA is the set of importance measures that are calculated for the TE. The Importance ranking analysis is applied to identify a component which has greatest contribution to the occurrence of the Top-event. Importance measures establish the significance for all the MCSs in the fault tree in terms of their contributions to the TE probability. Fussell -Vesely Importance Measures (F-VIM) are determinable for every MCSs modeled in the fault tree. This provides a numerical significance of all the fault tree elements and allows them to be prioritized. The results are enlisted in the table below.

3.4 SENSITIVITY ANALYSIS

Risk Reduction worth (RRW) is employed to perform sensitivity analysis. RRW are calculated to give the sensitivity of the TE probability to an increase or decrease in the probability of any event in the fault tree and they were also compared with conventional fault tree values from literature. It is expected that elimination of the MCS that has the highest contribution to the occurrence of TE should result in reducing the occurrence rate of TE more than other MCSs. Therefore, ranking of RRW values is expected to be the same as the ranking result of MCSs.

The Importance and Sensitivity Analysis is applied to identify the weakest parts of the system, i.e. those components whose failure modes give the greatest contribution to the likelihood of occurrence of the Top-event. Importance measures establish the significance for all the MCSs in the fault tree in terms of their contributions to the TE probability. Fussell-Vesely Importance Measure (F-VIM) and Risk Reduction Worth (RRW) importance measures are calculated give the sensitivity of the TE probability to an increase or decrease in the probability of any event in the fault tree. Transfer hose coupling is found to be the weakest part of the system, which requires shorter maintenance intervals or replacement to ensure safe working of the system. It is followed by drain valve failure and transfer lines which are potential sources of failure.

3.5 RESULTS AND DISCUSSION

Basic events 5,8,9,11,12 show an appreciable variation in the value of the failure probabilities derived. These events are related with failures of drain valve, liquid outlet line, vehicle impact. The sensitivity analysis of probability of failure of basic events pin-point the areas where more attention is required for preventing LPG release. The RRW ranking of cutsets shows a similar trend in ranking(FVIM) among the cut sets.

4. CONCLUSION:

The FTA is used to make detailed analysis of technical systems from the aspects of failure understanding the logic leading to the top event, to prioritize the contributors leading to the top event, to prevent the top event, to monitor the performance of the system, to minimize and optimize resources, to assist in designing a system by finding weak spots with harming potential, as a diagnostic tool to identify and correct causes of the top event.Obtained data makes possible a complex recognizing of causes and modes of failures and also mutual dependence between particular potential modes of elements' failures. The fault tree analysis applied to a LPG refueling station shows the various aspects of failure and it literally derives a probability of 2.720480E-02/ year for a LPG release accident. The preventive methods and maintenance may be planned to avert the situation. Fault tree presents convenient means for illustration of possible solutions. Further future works may be adopting the general top events in the fault tree sufficiently and by its development to the basic events, the majority of the potential modes of failure of components can be recorded, which can be used as one of the best Failure Modes and Effects Analysis model for analyses of causes and consequences of faults

REFERENCES

[1] Dhillon, B. S. (1985). *Quality Control, Reliability, and Engineering Design*, Marcel Dekker, Inc., New York.

[2] Ericson, C.A. (2005).*"Fault tree analysis", Chapter 11 in: Hazard Analysis Techniques for System Safety*. John Wiley & Sons, Inc.

[3] U.S. Department of Defense, B.. MIL–HDBK–338B. "Fault tree analysis" (pdf), electronic reliability design handbook (1998). http://www.everyspec.com/MIL-HDBK/MIL-HDBK+(0300+-+0499), Retrieved from:/download.php?spec=MIL-HDBK-338B.015041. pdf. Retrieved 2010-01-17.

[4] Haasl, D.F. (1965). "Advanced concepts in fault tree analysis". System Safety Symposium, University of Washington Library, Seattle.

[5] Hixenbaugh, A.F. (1968)." Fault Tree for Safety". The Boeing Company, D6-53604, Seattle, Washington.

[6] Roberts, N. H., Vesely, W.E.,Haasl, D.F., & Goldberg, F.F. (1981)".Fault tree handbook", Nuclear Regulatory Commission, U.S. Government Printing Office, Washington, D.C.

[7] Vesely, W. (2002). "Fault tree handbook with aerospace applications". National Aeronautics and Space Administration. Retrieved 17 January 2010 from: http://www.hq.nasa.gov/office/codeq /doctree /fthb.pdf

[8] Yang, G. (2007). "Life cycle reliability engineering", John Wiley & Sons.

[9] Melchers RE, Feutrill WR., (2001) "Risk assessment of lpg automotive refuelling facilities", Reliability Engineering and System Safety 74 283-290.

[10] Modarres, M., (2006). Risk analysis in engineering: probabilistic techniques, 1st. Ed. CRC publishing, USA

[11] Watson, H.A. (1961).Launch Control Safety Study, Bell Labs, Murray Hill, NJ,1(4).