Defence Science Journal, Vol 44, No 4, October 1994, pp 323-330

Hazard Assessment of a Nitration Plant using Fault Tree Analysis

C. Rajagopal and Col A.K. Jain
Centre for Environment & Explosives Safety, Delhi-110 054

ABSTRACT

Hazard assessment techniques, namely, fault tree analysis and safety analysis, have been applied to the nitration section of a plant producing explosives in the defence sector. Critical components and operations, the failure of which could lead to the occurrence of an unwanted event, have been identified and their effects quantitatively assessed. Some remedial measures have been suggested to minimise potential hazards and the effect of incorporating these measures on the system safety has been examined by means of specific case studies.

1. INTRODUCTION

Rapid growth of large and complex units processing explosives or flammable or otherwise hazardous chemicals under extreme temperature and pressure conditions, poses a threat to human life, property and the environment. Swift technological developments in untested areas with no opportunity for gradual evolution and learning by trial and error, as well as ever increasing sophistication in design, tend to make projects vulnerable to failure[1]. The failure of such hi-tech projects often leads to catastrophic conditions, and this makes it imperative to get the design and operating procedures right the first time.

The need for systematic analysis of the potential hazards and likely risks from the process plants producing sensitive explosives in the defence sector, thus becomes very critical. Therefore, the quantitative hazard assessment techniques[2,3] must be used for every sub-system of the plant being designed, to minimise the catastrophic accidents resulting from a combination of primary, secondary or command failures.

This paper describes the quantitative and qualitative assessment of a critical event, using a hazard assessment technique, fault tree analysis[4]. Identification of the critical event itself is a result of the systematic analysis using FETI (fire, explosion and toxicity index) and HAZOP (hazard and operatibility) studies techniques. A fault tree is a graphical representation of the logical relations between an undesired event (fire, explosion, etc.), called the 'top event' and the primary cause events[5]. A qualitative analysis systematically maps all possible combinations of causes for a defined top event. The quantitative analysis may also be performed if data on the frequencies or failure rates of the various basic causes are available and the risk of occurrence of the top event is to be evaluated.

2. CASE STUDY : NITRATION SECTION OF A CHEMICAL PLANT

A small chemical plant, designed to produce less than 40 kg of a specific high explosive per day per shift, has been taken up for study. This plant comprises mixing, nitration, simmering, dissolution and re-crystallization sections.

The HAZOP study has identified all possible deviations from the defined intention in each section of the plant and also listed out various probable causes and consequences of each such deviation. This study

Received 12 August 1993, revised 22 April 1994

has identified the nitration section as one of the most hazardous sections of this plant.

instrumentation/safety features are incorporated in this assembly:

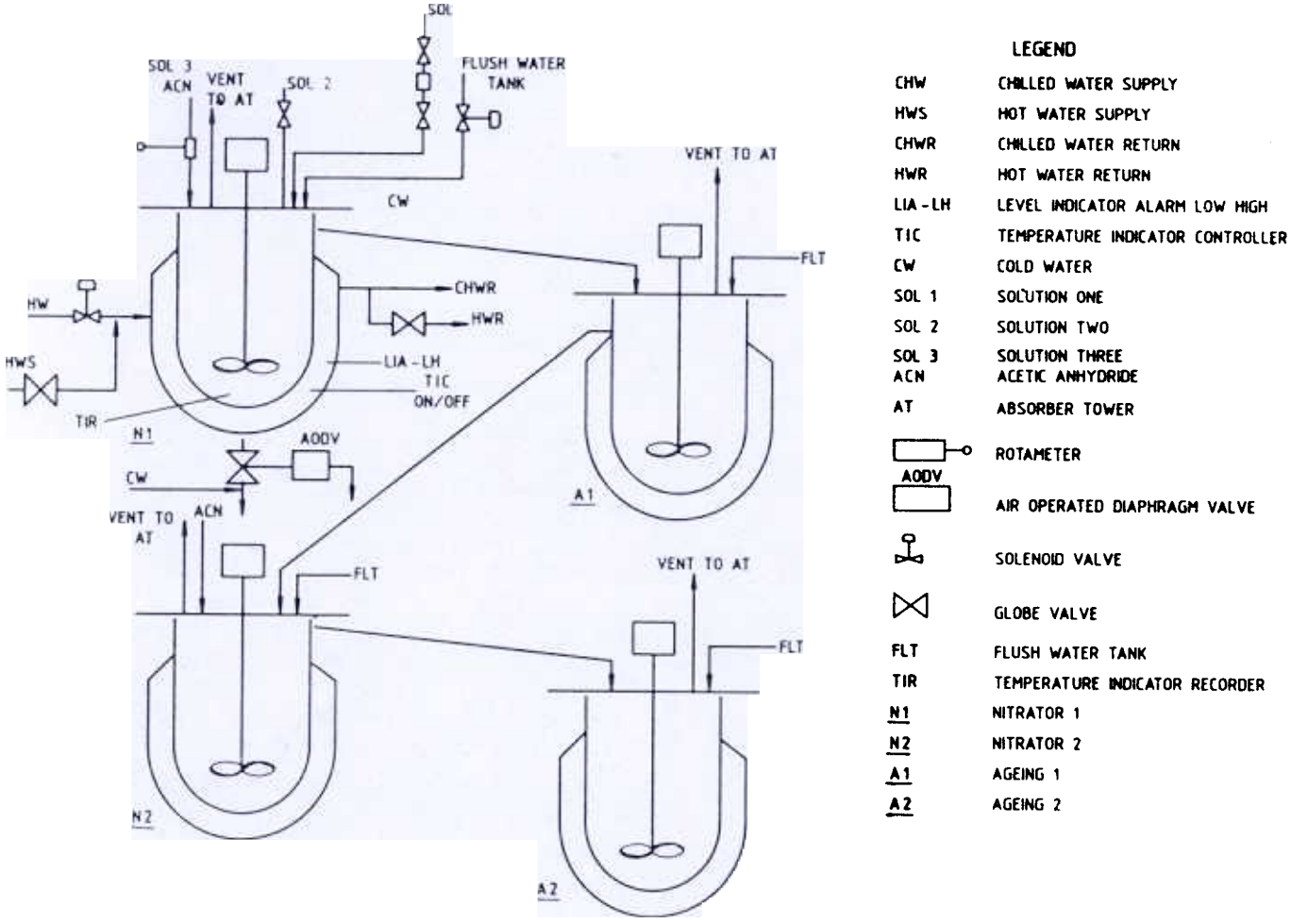

Figure 1. P&I diagram for nitrator section.

The nitration section consists of four vessels: two nitrators and two ageing vessels. Nitration takes place in two stages. In the first stage, nitration of solution 1 is carried out by its reaction with solution 2 in the presence of acetic anhydride and *p*-formaldehyde. This reaction starts in the first nitrator (N1) (Fig. 1) and proceeds to completion in the first ageing vessel (A1). The second stage involves reaction with more of solution 2 in the second nitrator (N2). This reaction is completed in the second ageing vessel (A2).

Being exothermic, the reactions occurring in stages I and II lead to an increase in the temperature of the reaction mixture. If this rise is not controlled, it could lead to a runaway reaction. Therefore, jacketed vessels with chilled water circulation are used for the nitrator (N) and ageing (A) vessels. The following

(a) The entry of the reactants to the nitrators is metered by means of rotameters.

(b) High-level alarms are provided in the control panel for all the N and A vessels.

(c) Temperature of the reaction mixture inside the N and A vessels is maintained at the design temperature by an ON/OFF temperature indicator controller (TIC). The sensing element is a thermocouple. The final control element is a solenoid valve in the inlet line of chilled water to the jackets.

(d) When the temperature reaches the first set point, the flow of chilled water supply to the jacket starts to prevent further rise in temperature. In case the chilled water supply

to the jacket fails and the temperature reaches the second (higher) set point which is set at 15 °C higher than the first set point, two additional safety features come into play.

The first safety feature is the provision of flush water to N and A vessels from an overhead tank. Inlet of the flush water to the N and A vessels is also controlled by the same TIC through another solenoid valve fitted in the inlet line of flush water. Water is used to flush the contents of the N and A vessels in case of a runaway reaction.

The second safety feature provides for the drainage of the contents of nitrator in case of a runaway reaction. An air operated diaphragm valve (AODV) fitted at the drain takes care of this contingency; the AODV gets activated by the TIC as soon as the second set point is reached and releases the contents of the nitrator into a drain.

3. FAULT TREE : NITRATION SECTION

The fault tree for 'critical conditions in the nitrator' leading to fire/explosion has been constructed (Fig. 2) Construction of fault tree is a deductive process and involves working backwards from effects towards causes[6]. The main elements of the tree are event definitions, such as RUNAWAY REACTION or NO FLUSH WATER and logic gates, such as AND and OR, which indicate the inter-relationship between various failure events. This tree has been analysed to find the minimal cut-sets, followed by the actual calculation of the top event probability.

As seen from Fig. 2, the top event could occur only if runaway reaction occurred in the nitrator with simultaneous failure of two safety features, viz., flush water to nitrator and drainage from nitrator. This is shown by an AND gate linking the top event to the three sub-events. Each of these contributory causes is then further broken down into more basic causes. The causes of failure may be primary, secondary or command.

(a) Primary failure is caused by inherent weakness in a component and is a basic failure such as faulty rotameter (9) or line fracture (6).

(b) Secondary failure is a sub-system failure and is caused when a component has been loaded beyond its limits such as when flow rate of solutions is more (69) or charge solution is faulty (65).

(c) Command failure is also a sub-system failure which occurs when a component is functional but fails because of incorrect control signals, energy supply, etc., such as when chilled water supply fails (67) or temperature control fails (60). Secondary and command failures are further developed to basic failures.

Following one of the branches of the fault tree, the *runaway reaction* (52) could occur as a result of any one of the following three possible causes:

(a) Reactants not added in correct proportion (55),

(b) Improper reaction conditions (56), and

(c) Agitator not functioning (57).

The relation among these three causes, therefore, is represented by an OR gate. Considering only the second cause, it could occur due to either rise in temperature or increased residence time within the nitrator. The rise in temperature itself could be due to failure of the solenoid valve (66), chilled water supply failure (67) or failure of the temperature control system (68). The temperature control could fail as a result of either thermocouple failure or controller failure.

Each branch of the tree, in turn, is likewise broken down into primary or basic failures. The analysis of this tree involves the identification of minimal cut-sets, following common mode failure resolution procedure (Table 1). Common cause failure is an important point which has significant bearing on the top event probability. These are basic failures which recur in various branches of the fault tree meeting at an AND gate. These failures occur when the components have some common susceptibility or a common location; two such examples are power failure and water supply failure. Wherever common cause failures are identified, they are to be eliminated as they greatly reduce the reliability of the system. By this procedure, each event is replaced by the inputs to its gates; AND gate-inputs being placed horizontally and OR gate-inputs inserted vertically in the table.

Since the identification of cut-sets and calculation of their probabilities in case of large trees is a laborious task, use of computers is helpful in obtaining the top-event probability. A computer program, developed at this Centre, has been used to obtain the minimal cut-sets and the corresponding failure rates.

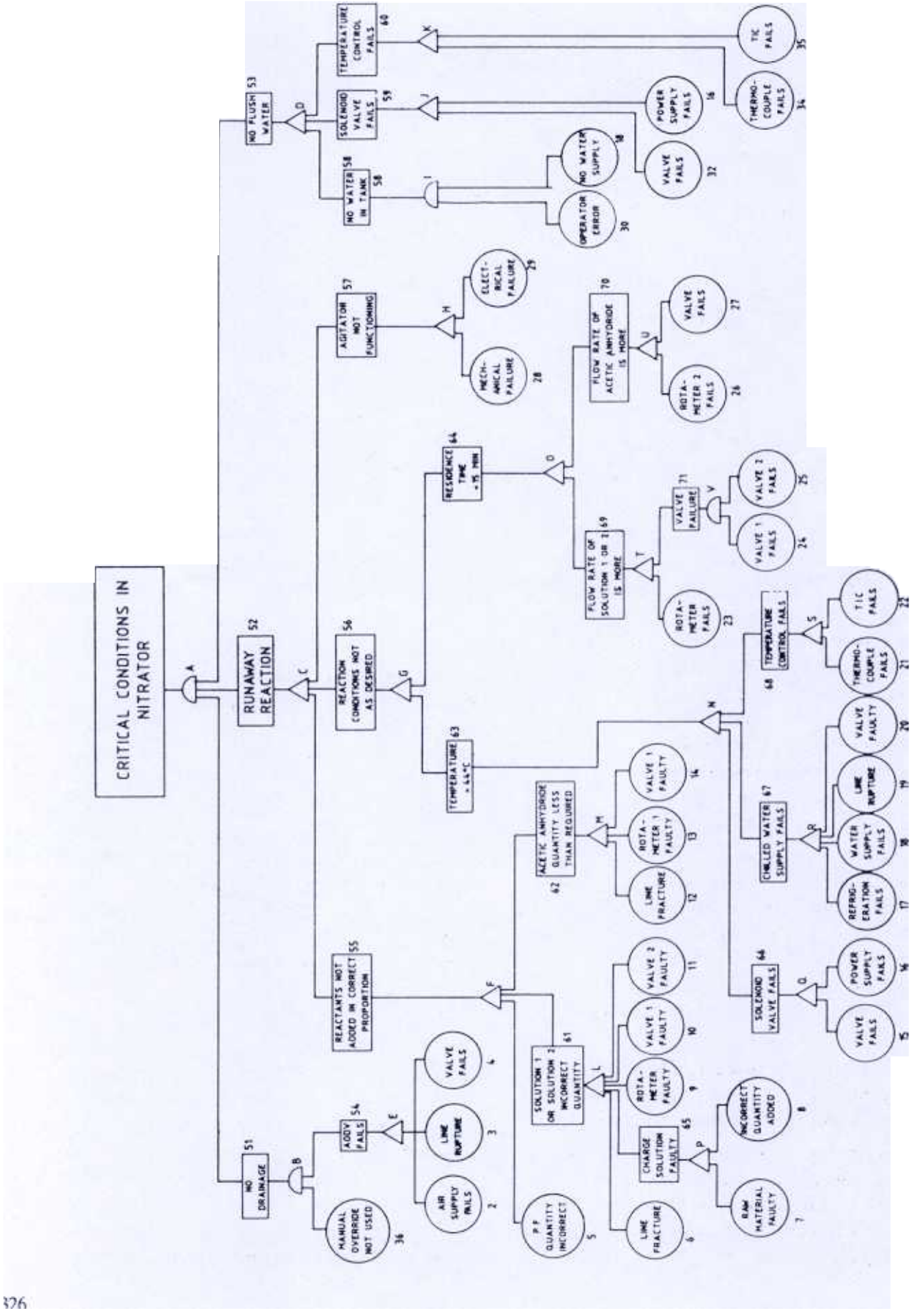

Figure 2. Fault tree for critical conditions in the nitrator

Table 1. Identification of minimal cut-sets

I	II	III	IV	V	VI	VII
A	BCD	(36)ECD	(36)2CD	(36)2FD	(36)25D	Contd→
			(36)3CD	(36)2GD	(36)2LD	↓
			(36)4CD	(36)2HD	(36)2MD	
				(36)3FD	(36)2ND	
				(36)3GD	(36)2OD	
				(36)3HD	(36)2(28)D	
				(36)4FD	(36)2(29)D	
				(36)4GD	(36)35D	
				(36)4HD	(36)3LD	
					(36)3MD	
					(36)3ND	
					(36)3OD	
					(36)3(28)D	
					(36)3(29)D	
					(36)45D	
					(36)4LD	
					(36)4MD	
					(36)4ND	
					(36)4OD	
					(36)4(28)D	
					(36)4(29)D	

The data to this program is input through a file which accepts five values in a sequence of main node (number), type of gate connecting it to next event (AND, OR, NOT), number of sub-nodes in that branch, numbers of these sub-nodes and probability of occurrence of the main node. The output is then consolidated through a data file.

The failure rates used in these calculations are based on the data compiled by UK Atomic Energy Authority, Atomic Energy Commission and Institute of Chemical Engineers[8].

From the results of this analysis, minimal cut-sets along with number of years between each failure have been listed in Table 2, in the decreasing order of criticality (refer Fig. 2). The highest probability of occurrence of critical condition in nitrator works out to about once in 5.2 years.

On examination of the list of 360 minimal cut-sets obtained for the fault tree for nitrator, it is evident that there are no single or double point failures. Table 2 also brings out those basic events which are critical by virtue of their relation to the top event and their high failure rates. Some of them are listed below :

Failure to use manual override	(36)
Air-operated diaphragm valve (AODV) failure	(4)
Incorrect addition of *p*-formaldehyde	(5)
Raw material impure	(7)
Incorrect quantity of raw material added	(8)
Power supply failure	(16)
Water supply failure	(18)
Failure to check water in flush water tank	(30)

Of these, events (36), (30), (5), (7) and (8) are operator errors; (36) being the most critical as it occurs in every cut-set of the fault tree. Human errors or failure rates are comparatively higher and vary unpredictably as compared to instrument and other component failure rates. In addition, humans do not fare well in making repetitive programmed responses to specific stimuli[7].

It would, therefore, be advisable, wherever possible, to replace operator control by instrumental controls for routine, programmable but critical actions. Wherever it is not possible, the following actions can be taken to aid the operator as well as to decrease the probability of failure:

Table 2. Criticality ranking of occurrence of top event

Minimal cut-sets	Years/Fault
(36: 4: 16: 30: 18:)	5.21
(36: 4: 5: 16:)	5.21
(36: 4: 7: 16:)	5.21
(36: 4: 8: 16:)	5.21
(36: 4: 17: 16:)	5.21
(36: 2: 16: 30: 18:)	6.25
(36: 2: 5: 16:)	6.25
(36: 2: 7: 16:)	6.25
(36: 2: 8: 16:)	6.25
(36: 2: 17: 16:)	6.25
(36: 4: 5: 30: 18:)	10.42
(36: 4: 7: 30: 18:)	10.42
(36: 4: 8: 30: 18:)	10.42
(36: 4: 17: 30: 18:)	10.42
(36: 4: 16:)	10.42
(36: 4: 18: 16:)	10.42
(36: 4: 22: 16:)	11.08
(36: 2: 7: 30: 18:)	12.5
(36: 2: 8: 30: 18:)	12.5
(36: 2: 17: 30: 18:)	12.5
(36: 2: 16:)	12.5
(36: 2: 18: 16:)	12.5
(36: 2: 22: 16:)	13.29
(36: 4: 9: 16:)	15.32
(36: 4: 13: 16:)	15.32
(36: 2: 9: 16:)	18.38

contd....

(a) Positioning of the override lever in a prominent location and marking it in fluorescent paint for easy identification, would reduce the response time in case of an emergency.

(b) Quality as well as quantity of the reactants added to the mixing tanks, and *p*-formaldehyde added to the nitrator, should be double checked.

(c) Events (16) and (18), i.e., power and water supply failures result in command failures. Therefore an alternative source of power supply, preferably a generator, could be considered. A water storage tank of sufficient capacity with level indicator and low-level alarm to meet both flush water and chilled water requirements could be provided.

SAFETY ANALYSIS

A logical fallout of the fault tree analysis is the safety ılysis. This analysis is based on a safety tree, which is the logical reverse of a fault tree. Resolution of this tree gives the number of possible ways by which a top unwanted event may be avoided.

Safety analysis basically involves the same steps as does a fault tree analysis, with the following differences :

(a) A safety tree is generally constructed for an event for which a fault tree already exists. The top event of the safety tree is the avoidance of the top event of the corresponding fault tree. The structure of safety tree is similar to that of the corresponding fault tree, except for the replacement of the logic gates, AND by OR and OR by AND, respectively.

(b) The safety tree is resolved in a similar manner as in the case of a fault tree. The minimal cut-sets obtained give the minimum combination of basic events required to avoid occurrence of the top unwanted event. From the cut-sets obtained, the lower order cut-sets, especially the single or one point cut-sets deserve special attention. They pinpoint those single, critical components and/or safety measures whose successful working or inclusion would ensure non-occurrence of a critical event.

(c) Basic events recurring in one or more branches of the safety tree deserve special consideration as the successful working of one such component would ensure that more than one branch of the tree is taken care of.

Cut-sets of the safety tree for 'critical conditions in the nitrator' are given in Table 3 in the order of increasing number of basic events per cut-set or in the decreasing order of importance.

Table 3. Minimal cut-sets for the safety tree for nitrator

(36)
(2)(3)(4)
(30)(32)(33)(34)(35)
(31)(32)(33)(34)(35)
(5)(6) .....(23)(24)(26)(27)
(5)(6) .....(23)(25)(26)(27)

It is seen that the safety tree for the top event in the nitrator has six cut-sets, which consist of one single point, one triple point, two five point and two 22 point

cut-sets. The 22 point cut-sets need not be considered for safety analysis as it would be practically impossible to ensure the non-occurrence of 22 events simultaneously. The other cut-sets are analysed, and the required actions to be taken to ensure the non-occurrence of the top event are suggested as follows :

(a) The only single point cut-set of the safety tree is event number (36), i.e., manual override to drain the nitrator. Therefore, if the use of the manual override is ascertained, it would also ensure non-occurrence of critical event in the nitrator.

(b) The next cut-set, (2)(3)(4), is of order three. The occurrence of all the three events, viz. uninterrupted air supply, failure-free operation of the diaphragm valve and crack/rupture-free operation of the air line, ensures the operation of the AODV valve and the drainage of the contents of the nitrator in the event of an emergency.

(c) The next two cut-sets are of order five and consist of the five basic events : (i) water should be available, (ii) solenoid valve should not fail, (iii) power supply to the valve should not fail, (iv) thermocouple should function accurately, and (v) the temperature controller should not fail.

Steps to obviate failures of sub-systems or components have already been enumerated in the preceding paragraphs.

5. IMPROVEMENT IN SYSTEM SAFETY – CASE STUDIES

To assess the improvement of safety standards in the nitration section due to inclusion of the various safety measures recommended in the previous sections, the following cases are considered :

Case 1 : Effect of Eliminating Common Cause Failures

In this case study, effects of eliminating the following common cause failures are considered :

Power supply failure (16), and

Water supply failure (18).

Results of the fault tree analysis obtained by this modification using the computer program show that the total number of cut-sets reduces from 360 to 225. Probability of occurrence of top event also reduces to 0.096 faults/year or 10.4 years between each fault.

Case 2: Effect of Change in Failure Rate

Use of manual override lever in case of a runaway reaction has been identified by both fault tree and safety analysis to be one sure way of preventing occurrence of top (unwanted) event. If the use of this lever can be ensured whenever required, i.e., the failure rate for this event is reduced from 0.4/year to say 0.001/year, the probability of occurrence of top event reduces to once in 208 years. Reduction in the failure rate of this event would perhaps involve positioning of an operator with adequate backup, solely for the purpose of operating this lever.

6. SUMMARY

Safe design of a plant involves eliminating potential hazards by modifications to design, operation or maintenance procedures and by inclusion of various safety devices. The need for such changes is specifically brought out by techniques like fault tree and safety analysis when applied to particular equipment/sub-systems.

In this paper, the application of fault tree and safety analysis techniques has highlighted the critical events which could lead to the occurrence of top event. The improvement in safety standards as a result of eliminating common cause failures or reducing the failure rate of an event, has also been quantitatively assessed through case studies.

ACKNOWLEDGEMENTS

The authors wish to record their thanks to the Director, Centre for Environment & Explosives Safety (CEES), Delhi, for his valuable suggestions and permission to publish the paper.

REFERENCES

1. Lees, F.P. Loss prevention in the process industries. Butterworths, London, 1986. pp. 1003-10.
2. Sayers, B. Safety and risk in a chemical plant (A case history). Proceedings of the Annual Reliability and Maintainability Symposium, 1979, Washington DC, USA. pp. 174-80.
3. Kletz, T.A. Practical applications of hazard analysis. *Chem. Engg. Progress,* October 1978, 47-53.

4. Browning, R.L. Use a fault tree to check safeguards. Proceedings of the Loss Prevention Symposium, Vol 14. AIChE. pp. 20-26.

Prugh, R.W. Application of fault tree analysis. Proceedings of the Loss Prevention Symposium, Vol 14. AIChE. pp. 1-10.

6. Methodologies for risk and safety assessment in chemical process industries – a manual. Commonwealth Science Council, London, 1990.

7. Browning, R.L. Human factors in the fault tree CEP, 1976. pp 72-75.