# USING FAULT TREES AND EVENT TREES TO MANAGE RISK

Dr Bill Danaher
Gibson Associates
P.O. Box 1010
Spring Hill 4000

## 1.0 INTRODUCTION

The ability to identify the causes of particular events or to be able to predict the likelihood of occurrence of certain events is a critical element in the risk management process. The purpose of this paper is to provide an introduction to fault tree and event tree analysis, and to provide guidance on their construction and use.

## 2.0 FAULT TREE ANALYSIS

### 2.1 Overview

Fault tree analysis(FTA) allows the frequency of a hazardous incident (Top Event) to be estimated from a logic model of the failure mechanisms of a system. The model is based upon various combinations of failures in more basic systems, safety systems and human reliability.

The underlying method involves the use of a combination of relatively simple logic gates (AND, OR gates) to construct a failure model. The Top Event frequency or probability, is calculated from data relating to simpler or more basic events.

A basic assumption in FTA is that all system failures are binary in nature, i.e. a component or operator either performs successfully or fails completely. In addition it is assumed that the system is capable of performing its task if all sub-components or sub-systems are operating. Fault trees do not treat degradation of a system or its components over a period of time. In addition, FTA addresses only instantaneous failures.

### 2.2 Aims of Fault Tree Analysis

The usual aims of FTA are one or more of the following:

- Estimation of the likelihood of the occurrence of a particular incident

- Determination of the combinations of equipment failures, operating conditions, and human errors that contribute to an incident

- Identification of remedial measures and their impact

FTA can be used in either a predictive or investigative manner. For example if an incident has occurred, then this incident can become the top event in a fault tree and an analysis can be undertaken to determine basic causes. On the other hand, if hazard analysis has indicated that a particular event might be possible, then fault tree analysis can be used to identify possible causes and the likelihood of occurrence.

## 2.3 Construction of Fault Trees

The procedure for undertaking FTA involves five steps:

- System description, including definition of system boundary

- Hazard identification and selection of the top event

- Construction of the fault tree

- Qualitative examination of the structure

- Quantitative evaluation of the fault tree

### Step One: System description

This is a key step in FTA because an understanding of the causes of undesirable events is possible only through a thorough knowledge of how the system functions. The description stage is basically open ended: it is the responsibility of the person developing the fault tree (the analyst) to determine boundaries and data needs. Some of the information that may be required includes description of the process, hazardous properties of materials, equipment specifications, operating and maintenance procedures, etc....

### Step Two: Hazard identification

A range of activities such as site inspections, check-lists, hazard and operability studies and accident investigation can be used to determine top events. Top events are usually major events such as fire, explosion, equipment failure or other accident/incident.

**Step Three: Fault tree construction**

There are no formal rules regarding fault tree construction or determination of what events and gates to use. Fault trees are logic diagrams that show how a particular top event may occur. Usually a fault tree is constructed from top down. A particular undesired event or outcome is chosen and this becomes the top event. Commencing with the top event the necessary and sufficient causes of the top event are identified together with their logical relationship. In order to do this, the analyst asks questions such as "How can this happen?" or "What will cause this event to occur?" This process of questioning is continued until the analyst is satisfied that sufficient resolution has been obtained to allow for subsequent assignment of probabilities or frequencies to the basic events, i.e. the questioning process continues until the analyst is satisfied that the failure model adequately describes the process under study. Although in principle the questioning process could continue indefinitely, problems arising outside the study boundary are not addressed. Therefore boundary definition is critical to successful fault tree analysis.

Manually constructed fault trees are inherently subjective and may be incomplete. However, the technique allows the fullest possible expression of the analysts understanding of the system. Some common mistakes which may occur in fault tree construction are:

- Rapid development of one branch of a fault tree without systematically proceeding level by level across the entire fault tree
- Omission of an important failure mechanism or cause, or a false assumption of negligible contribution
- Incorrect combinations of frequency and probability into logic gates
- Inappropriate balance between hardware type failures or causes and human errors
- Failure to recognise the dependence of events

**Step Four: Qualitative examination of structure**

Once a fault tree has been constructed, the structure of the fault tree can be examined qualitatively to understand the causation mechanisms. In particular, the effectiveness of safeguards, the qualitative importance of various sub-events, and the susceptibility to common-mode failures are highlighted. For more complex fault trees, inspection is too difficult and more formal means must be applied, such as Boolean analysis (see ref. 1). Fault trees can be converted into the equivalent Boolean expression defining the top events in terms of a combination of all lower events. This expression is

usually expanded using the laws of Boolean algebra, until it expresses the Top Event as the sum of all minimal cut sets.

Common-cause failures are due to a single event affecting the basic events assumed to be independent in the fault tree. A common cause might be a power failure disabling several electrical safety systems simultaneously, or a maintenance error miscalibrating all sensors. If, for example, a power failure appears in two branches of a fault tree joined by an AND gate, and the gate-by-gate method is followed, the final result will be incorrectly calculated. A Boolean analysis will identify and address this problem. However, there may be many elements that are not included in a fault tree that could result in common cause failure, e.g. common manufacturer, common location.

**Step Five: Quantitative evaluation of fault tree**

Once the final structure of a fault tree has been determined and a frequency or probability has been assigned to each of the basic events, it is possible to calculate the top event frequency or probability. The gate-by-gate technique starts with the basic events of the fault tree and proceeds upwards towards the top event. All inputs to a gate must be defined before calculating the gate output. All lower gates must be computed before proceeding to the next higher level. Note that addition occurs at OR gates, and that multiplication occurs at AND gates.

Once a fault tree has been fully calculated a number of additional studies are possible. These studies include sensitivity, uncertainty and importance analyses. Sensitivity analysis is used to determine the sensitivity of the top event frequency to possible errors in basic event data. Uncertainty analysis provides a measure of the error bounds of the top event. Importance analysis ranks the various minimal cut sets in order of their contribution to the overall failure frequency.

## 2.4 Example Fault Trees

Two sample fault trees are shown at the end of the paper. The first shows how fault tree analysis can be used to represent the outcomes of accident investigation. The example considered shows the basic elements of a fault tree relating to an incident involving a runaway vehicle. Each of the subelements could be developed in greater detail.

The second fault tree demonstrates the predictive value of fault tree analysis. A situation is considered where an underground conveyor fire has the potential to cause asphyxiation. Again each of the sub-elements could be developed in greater detail, and quantified. Such a fault tree could be used to assess the impact of different control options and operating strategies on the top event frequency. For example, location of conveyors in the ventilation outflow will reduce the likelihood of exposure of personnel to combustion products, but may also impact on the likelihood of other events. Therefore, there will be an overall impact on the top event frequency.

### 2.5 Strengths and Weaknesses of the Technique

FTA is a widely used technique. Its theory has been well developed and there are many published texts and papers describing its use. A particular advantage of the method is the complimentary information provided from the qualitative and quantitative analysis of the fault tree. The main weakness is that a great deal of effort is usually required to develop the fault tree and there is a potential for error if failure or causation paths are omitted, or manual calculation methods are incorrectly employed.

## 3.0 EVENT TREE ANALYSIS

### 3.1 Overview

An event tree is a graphical logic model that identifies and quantifies possible outcomes following an initiating event. The event tree provides systematic coverage of the time sequence of event propagation, either through a series of protective system actions, normal plant functions, operator interventions and incident consequences.

### 3.2 Aims of Event Tree Analysis

Event trees can be applied to either pre-incident or post-incident applications. In the case of pre-incident application the aim is to examine the systems in place that would prevent incident precursors from developing into incidents. For post-incident applications the aim is to identify the range and likelihood of potential outcomes.

### 3.3 Construction of Event Trees

The construction of an event tree is sequential and involves seven steps:

- Identification of the initiating event
- Identification of safety functions/hazard promoting factors and determination of outcomes
- Construction of the event tree
- Classification of the outcomes
- Estimation of probabilities
- Quantification of outcomes
- Testing of outcomes

**Step One: Identification of the initiating event**

Various hazard identification techniques can be used to determine the initiating event. In many instances the initiating event is the top event of a fault tree.

**Step Two: Identification of safety functions/hazard promoting factors and determination of outcomes**

A safety function is a device, action or barrier that can interrupt the sequence from an initiating event to a hazardous outcome. Examples are, automatic safety systems, alarms to alert operators, detection systems, barriers or containment. Hazard promoting factors may change the final outcome. They include ignition or non-ignition, containment or non-containment of release, etc.... Usually a heading is used to label a safety function or a hazard promoting factor on the event tree. Most event tree branches involve binary choices.

**Step Three: Event tree construction**

An event tree graphically displays the chronological development and progression of an incident. Commencing with the initiating event, the event tree is constructed from left to right. At each heading or node two or more alternatives are analysed until a final outcome is obtained for each node. Some branches may be more fully developed than others. In a pre-incident analysis the final sequence might correspond to successful termination of some initiating event, e.g. safe shutdown, or some specific hazardous outcome. The listing of the safe recovery and incident conditions is an important output of this analysis. For a post-incident analysis the final results typically correspond to a range of incident outcomes.

The various intermediate event headings should be indicated at the top of the page above the appropriate branch of the event tree. It is normal to have a "success" or "yes" branch upwards and a "failure" or "no" branch downwards. Starting with the initiating event, each heading is labelled with a letter identifier, e.g. A, B, C, D, etc... Every final event sequence can then be specified with a unique letter combination. Usually a horizontal bar over a letter indicates that the designated event did not occur.

**Step Four: Classification of the outcomes**

A completed event tree analysis yields a range of outcomes. Often these can be classified into groups of similar outcomes.

### Step Five: Estimation of outcome probabilities

In an event tree each heading other than the initiating event corresponds to a conditional probability of some outcome if the preceding event has occurred. Thus the probabilities associated with each heading must sum to 1.0. This is true for binary or multiple outcomes.

### Step Six: Quantification of outcomes

The frequency of each outcome may be determined by multiplying the initiating event frequency with the conditional probabilities along each path of the event tree leading to an outcome. Such a calculation assumes no dependency among events and either complete success or failure for each intermediate event.

### Step Seven: Testing of outcomes

As in the case of fault tree analysis, poor event tree analysis can generate inaccurate results. An important step in the analysis is to test results against common sense, expert opinion and the historical record.

## 3.4 Example of Event Tree

A sample event tree is shown at the end of the paper. The event tree considers a gas release and the range of events that might follow. Options considered include immediate ignition, dispersion of the gas and subsequent ignition, safe dispersion, occurrence of fire or explosion. The event tree summarises the range of outcomes that could result from the initial event.

## 3.5 Strengths and Weaknesses of the Technique

An important strength of the event tree is that it portrays the outcomes flowing from an initiating event in a manner that is systematic, logical and self documenting. The logical and arithmetic calculations are simple and the format is compact. Pre-incident event trees are valuable in highlighting the value and/or weaknesses of protective systems. Post-incident event trees highlight the range of outcomes that are possible from a given incident.

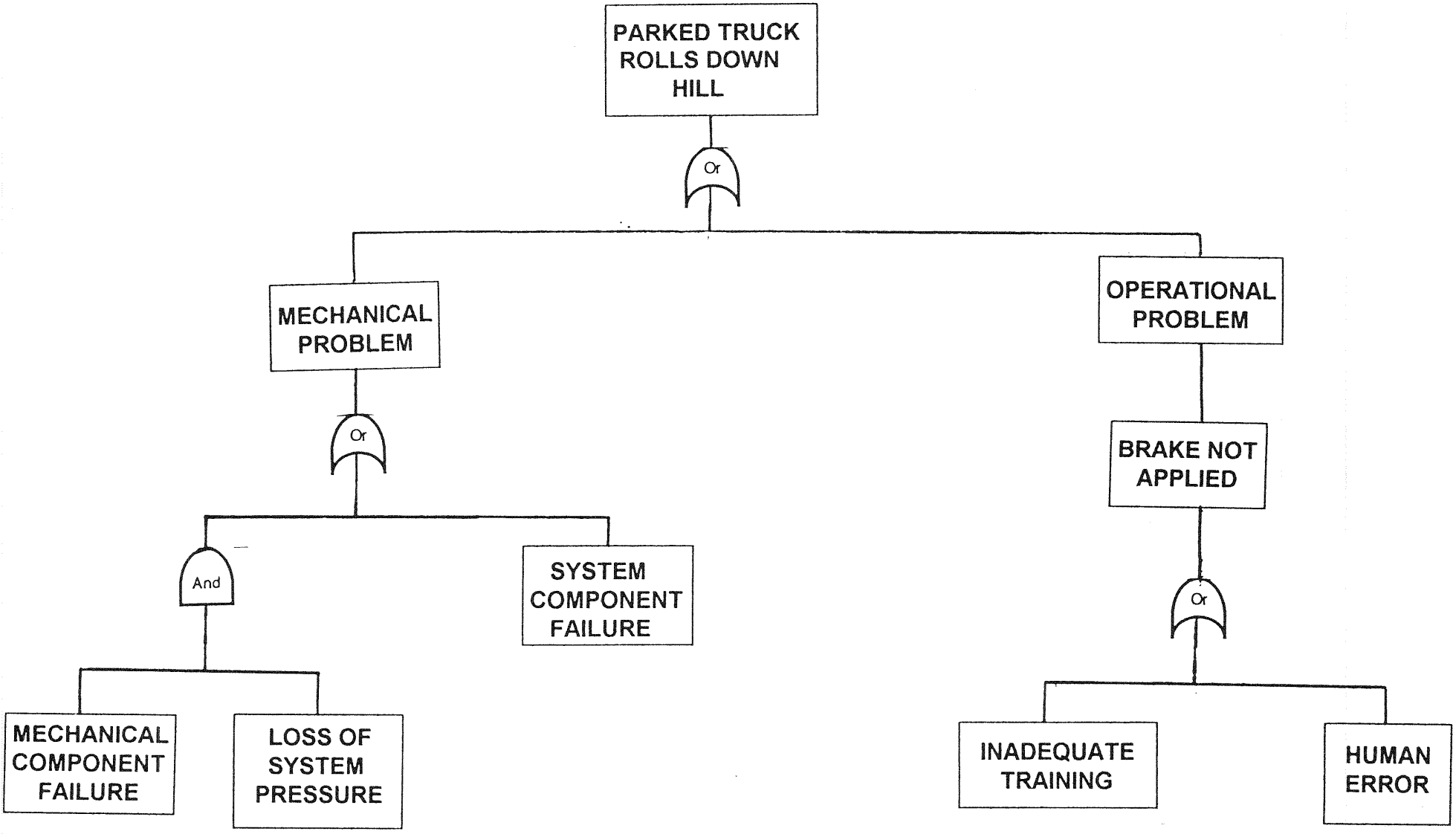
# 4.0 CONCLUDING REMARKS

The paper has aimed to provide details on fault tree analysis and event tree analysis, and to indicate how these techniques can be applied in either a predictive or investigative manner. As such they are useful techniques to assist in the management of risk.

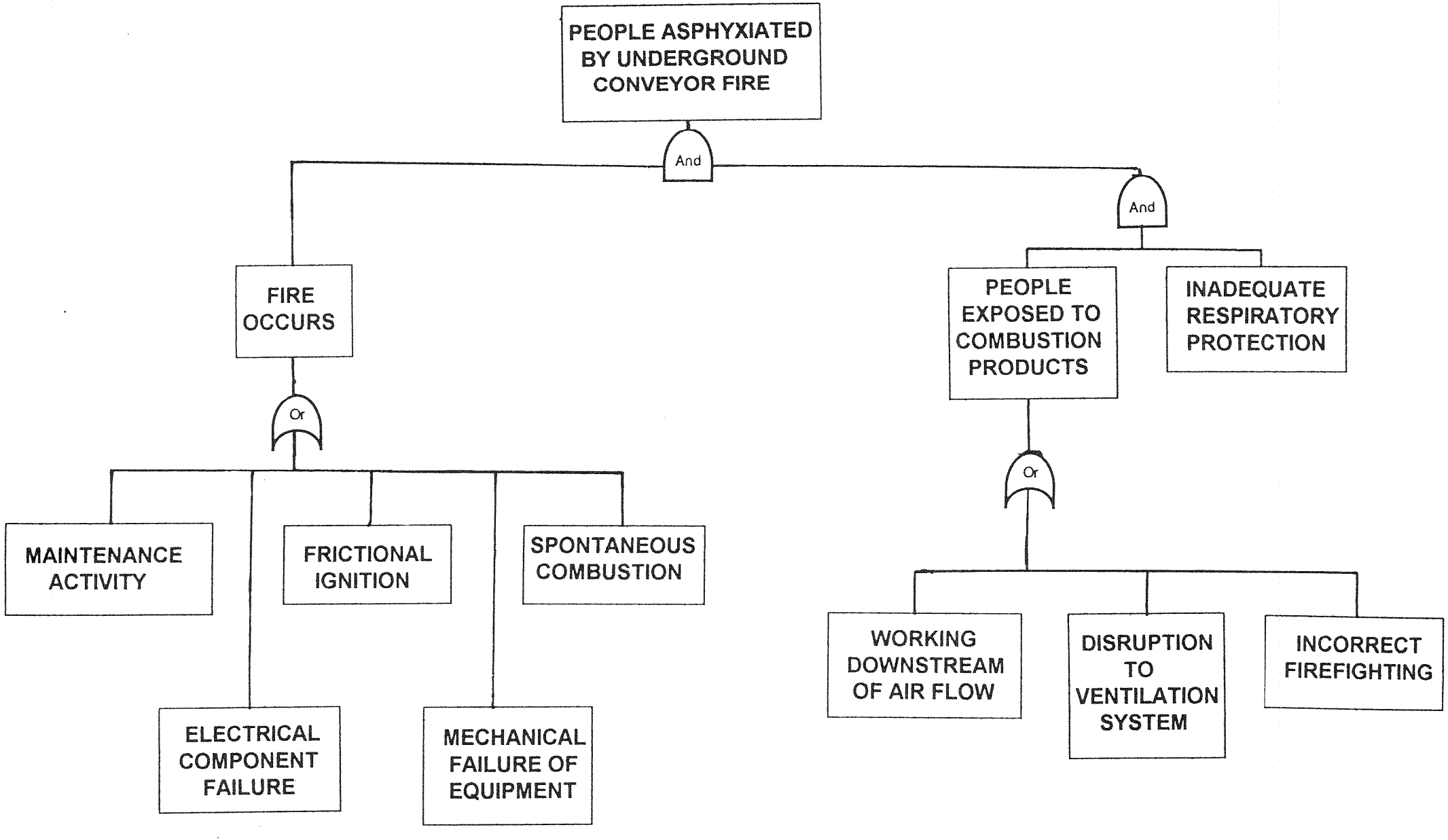
## 5.0 REFERENCE

American Institute of Chemical Engineers, "Guidlines for Chemical Process Quantitative Risk Analysis", 1989, pages. 185-221, Appendices D and E.

# FAULT TREE EXAMPLE : TRUCK RUNAWAY



# FAULT TREE EXAMPLE : UNDERGROUND FIRE



## EVENT TREE EXAMPLE : GAS RELEASE