Root causes analysis: Literature review

Prepared by
WS Atkins Consultants Ltd
for the Health and Safety Executive

CONTRACT RESEARCH REPORT
325/2001

HSE
Health & Safety Executive

Root causes analysis: Literature review

A D Livingston, G Jackson & K Priestley
WS Atkins Consultants Ltd
Science & Technology
WS Atkins House
Birchwood Boulevard
Birchwood
Warrington
WA3 7WA

Typically an incident report will place emphasis on developing a description of the consequences rather than causes of the incident, explaining what happened, but not why it happened. It is only by adopting investigation techniques that explicitly identify root causes, ie the reasons why an incident occurred, that organisations may learn from past failures and avoid similar incidents in the future. Root causes analysis is simply a tool designed to help incident investigators determine what, how and most importantly, why an incident occurred.

Based on this literature review it is apparent that there are three key components that need to be applied to ensure effective root causes analysis incident investigation. These are a method of describing and schematically representing the incident sequence and its contributing conditions; a method of identifying the critical events or active failures and conditions in the incident sequence, and based on this identification; a method for systematically investigating the management and organisational factors that allowed the active failures to occur, ie a method for root causes analysis. In selecting or developing a root causes analysis method, the analyst needs to consider whether the method specifically facilitates the identification of safety management and organisational inadequacies and oversights which relate to their own operations. The method needs to identify those factors that exert control over the design, development, maintenance and review of their risk control systems and procedures.

This report and the work it describes were funded by the Health and Safety Executive (HSE) Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

HSE BOOKS

First published 2001

ISBN 0 7176 1966 4

Foreword

In 1991 HSE published *Successful Health and Safety Management, HSG65*, ISBN 0 7176 1276 7, which described a model for health and safety management. This was followed in1993 by *The Costs of Accidents at Work, HSG96,* ISBN 0 7176 1343 7, which both analysed the costs of individual accidents at 5 sites over a 3 month period and discussed the background to the economic argument for good health and safety using loss control principles. The analysis confirmed earlier work by Heinrich and others on building accident pyramids, whereby a small number of fatal/serious accidents is underpinned by a much larger number of minor injuries and non injury damage occurrences.

HSE subsequently commissioned WS Atkins to investigate if the work in these two publications could be linked – could the costs of accidents be clearly identified and linked back to specific management failures? If it could this would enable organisations to target improvement effort in a cost effective way by concentrating on well defined areas of failure. This should reduce both overall costs and accident numbers.

The work involved developing and trialling two major methodologies – one for capturing data on costs of accidents, which was simpler and more user friendly than the one in the original *HSG96* publication, while the other was to develop a root causes analysis tool from first principles. It was for this purpose that the present literature review was undertaken – something which had never been done comprehensively before. It is considered of sufficient interest in its own right to publish separately as a Contract Research Report. The original work was completed in 1995 but has been updated to cover new products up to the end of 1998.

Contents

1.0 INTRODUCTION 1

2.0 METHOD 3

3.0 SUMMARY OF INCIDENT INVESTIGATION TECHNIQUES 4

4.0 SEQUENCE DIAGRAMS 6
4.1 Principles of Sequence Diagrams 6
4.2 Conducting an Analysis 6
4.3 Events and Causal Factors Charting 7
4.4 Multilinear Events Sequencing 9
4.5 Sequentially Timed Events Plotting Procedure 10
4.6 Schematic Report Analysis Diagram 10
4.7 Summary 11

5.0 IDENTIFICATION OF CRITICAL EVENTS 13
5.1 Introduction 13
5.2 Barrier Analysis 13
5.3 Change Analysis 14
5.4 Fault Tree Analysis 16
5.5 Summary 18

6.0 ROOT CAUSES IDENTIFICATION - 'TREE TECHNIQUES' 20
6.1 Management Oversight and Risk Tree 20
6.2 Savannah River Plant (SRP) Root Cause Analysis System 22
6.3 TapRooT™ 24
6.4 Human Performance Investigation Process (HPIP) 26
6.5 Causal Tree Method 28
6.6 REASON® Root Cause Analysis 29
6.7 Event Root Cause Analysis Procedure 30
6.8 Summary 31

7.0 ROOT CAUSES ANALYSIS - CHECKLIST METHODS 33
7.1 Human Performance Evaluation System 33
7.2 Systematic Cause Analysis Technique 34
7.3 Technique of Operations Review 36
7.4 Systematic Accident Cause Analysis (SACA) 38
7.5 Summary 39

8.0 ROOT CAUSES ANALYSIS - OTHER METHODOLOGIES 40
8.1 Introduction 40
8.2 American Institute of Chemical Engineers' Review 40
8.3 HSYS 42
8.4 Checklists 42
8.5 Assessment of Safety Significant Teams (ASSET) 43
8.6 Safety Through Organisational Learning (SOL) 43
8.7 PROACT™ 45

9.0 CONCLUSIONS 46

10.0 REFERENCES 49
10.1 References Included in the Text 49
10.2 Papers Reviewed, but not Mentioned in the Text 51
10.3 References not Obtained 52

GLOSSARY 53

1.0 INTRODUCTION

Typically an incident report will provide an organisation with a description of events which principally focus on the status of the system at discrete moments along a timeline. Reports also usually place the emphasis on developing a description of the consequences rather than causes of the incident, explaining what happened, but not why it happened. Such analyses are almost invariably technically orientated involving detailed descriptions of plant, equipment, reactions and their governing logic systems. It is only by adopting investigation techniques which explicitly identify root causes, i.e. the reasons why an incident occurred, that organisations may learn from past failures and avoid similar incidents in the future.

Root causes analysis is simply a tool designed to help incident investigators describe what happened during a particular incident, to determine how it happened and to understand why it happened.

The definition of a root cause varies between authors and root causes methodologies, with different 'levels' of causation being adopted by different systems. Figure 1 illustrates the different levels of cause that can be ascribed to an incident. The root causes lie at level 1 which inevitably influence the effectiveness of all the risk control systems and workplace precautions that exist at levels 2 and 3.

The most useful definition identified to date is the definition used by Paradies and Busch (1988), that is:

the most basic cause that can be reasonably identified
and that management has control to fix

This definition, will be used for this review. It contains three key elements:

Basic Cause	Specific reasons as to why an incident occurred that enable recommendations to be made which will prevent recurrence of the events leading up to the incident.
Reasonably Identified	Incident investigation must be completed in a reasonable time frame. Root causes analysis, to be effective, must help investigators to get the most out of the time allotted for investigation.
Control to Fix	General cause classifications such as 'operator error' should be avoided. Such causes are not specific enough to allow those in charge to rectify the situation.

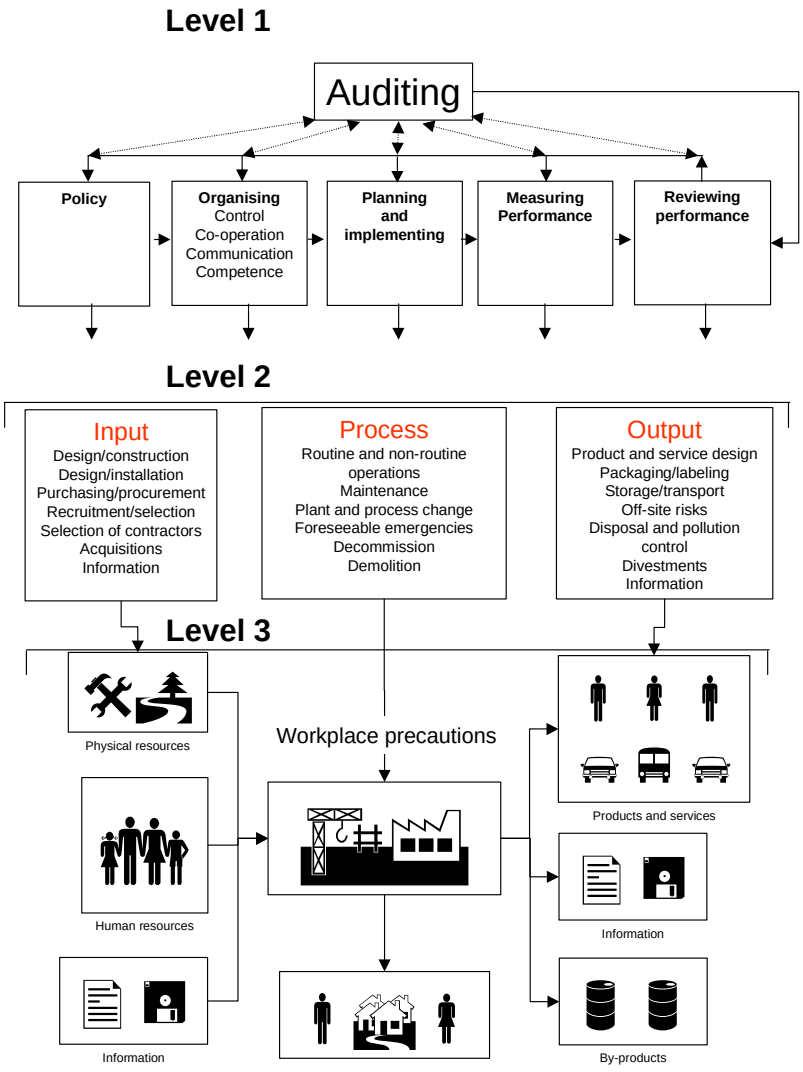
Management needs to know exactly why a failure occurred before action can be taken to prevent recurrence. If the investigators arrive at vague recommendations such as 'Remind operator to be alert at all times', then they have probably not found a basic enough cause and need to expend more effort in the investigation process. Also, if causes at level 2 and 3 are identified without investigating why the level 1 systems allowed such failures to occur, then similar or repeat incidents may occur.

This definition, by default, also recognises that there will be instances where incidents happen that are beyond management control. Waldram (1988) suggests that, under UK law, the extent of the control to be expected should be judged according to the test of 'reasonable practicability'.

In the majority of cases, root causes analysis methodologies have to be used by busy personnel working within the organisation where the incident occurred. Therefore, techniques need to be practical and easily applied. The application of the technique should also be prescriptive to minimise variations in user interpretations, and should encourage multiple causes to be identified, where appropriate.

This report contains the findings of a literature search, outlining the principles, structure and method of application of each identified root causes analysis technique.

Figure 1: Levels of Causation



2.0 METHOD

The following libraries/database systems were consulted:

- WS Atkins Central Information Services (Access to the British Library and Dialog series of databases)
- HSE Library in Sheffield (HSELINE)
- Ergonomics Information Analysis Centre (Ergonomics Databases)
- RoSPA Information Service
- Internet searches

Initially the general terms ‘root causes analysis’, ‘incident investigation’ and ‘accident investigation’ were used to initiate the search. As specific techniques were identified, the respective titles were researched further.

In some instances publications have been unobtainable. In these cases reviews have been undertaken via commentaries/reviews by other authors.

3.0 SUMMARY OF INCIDENT INVESTIGATION TECHNIQUES

The principles of root causes analysis have long been recognised in fields such as engineering, quality control and environmental management, as well as in safety management. Techniques have been successfully borrowed from other disciplines and adapted to meet the requirements of the safety field, most notably the development of the 'tree' structure from Fault Tree Analysis, which was originally an engineering technique.

The overall process of incident investigation within the safety field is similar across many of the methodologies reviewed. Differences arise however, in the particular emphasis of the techniques. Some focus on management and organisational oversights and omissions while others consider human performance/error problems in more depth. A generic representation of the incident investigation process is shown in Figure 3.1.

The first stage of the incident investigation involves obtaining a full description of the sequence of events which led to the failure. This will require interviews with key personnel and examination of the physical evidence in order to piece together the circumstances of the incident.

The use of techniques such as Events and Causal Factors Charting, Multiple Events Sequencing (MES) and the Sequentially Timed Events Plotting Procedure (STEP), will provide a systematic and structured framework to aid the collection of information by identifying where gaps in the understanding of event chains lie. These techniques are described in Section 4.

These sequencing techniques can also be used in conjunction with methods such as Barrier Analysis, Change Analysis and Fault Tree Analysis to ascertain the critical events and actions, and thus the direct causes of the incident. The concepts of incident causation encompassed in both Barrier Analysis and Change Analysis are fundamental to the majority of root causes analysis methodologies and are frequently included in an array of tools to be applied as appropriate by the investigator. As stated earlier, the logic tree principles behind Fault Tree Analysis have been developed and adapted to produce generic causal trees to guide the analyst in the identification of the appropriate root causes. These three techniques have been termed the 'building blocks', because of their wide application, and are discussed in Section 5.

Having identified the direct causes of the critical actions/events of the incident, the next stage is concerned with determining their underlying or root causes. Often a tree structure is used to organise root causes. Investigators are required to work through the tree identifying the appropriate branches at each level until the root causes are arrived at. Tree Techniques are described in Section 6. Section 7 goes on to describe other systems that support the decision process for the investigator by providing checklists with cross referencing systems.

By identifying the root causes of the incident, the remedial actions proposed are more likely to be effective in the long term. In addition, it is possible to develop a database of root causes that address human, equipment, technical and quality failures. This approach enables the identification of root cause trends and, from these, the development of effective preventative recommendations which not only prevent repeat failures but will also circumvent many related incidents.

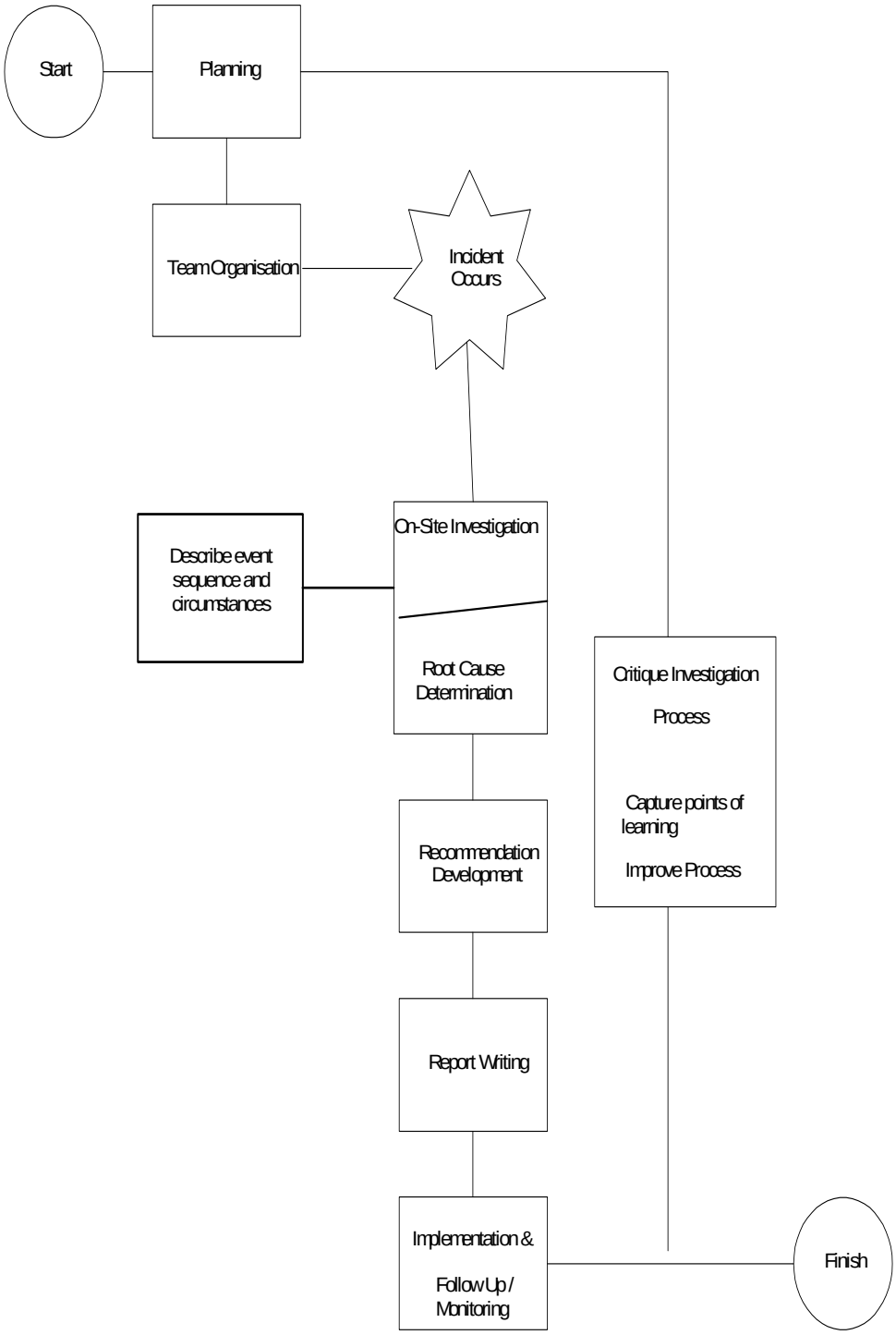


Figure 3.1 : Overview Of The Incident Investigation Process

4.0 SEQUENCE DIAGRAMS

Although diagrams and charts had previously been used in incident investigation, the National Transportation Safety Board (NTSB) are regarded as pioneers in the use of sequence diagrams as analytical tools in incident investigations. Much of the work in the development of the techniques used at NTSB was undertaken by Ludwig Benner Jr and colleagues, in the early 1970s.

There are many fundamental principles that are encompassed by all of these techniques. These will be discussed in the section below, followed by a brief explanation of each method.

4.1 PRINCIPLES OF SEQUENCE DIAGRAMS

4.1.1 Structure

Before starting the sequencing diagram it is necessary to define the end of the incident sequence. It is also be necessary to define the start point of the incident, but this may not become apparent until the investigation is underway. Typically, the diagrams start at the end point and work backwards identifying the most immediate contributing events first. Basic construction principles for sequence diagrams are suggested by Johnson (1980):

Chart Format

- All events are enclosed in rectangles, and conditions in ovals
- All events are connected by solid arrows
- All conditions are connected to other conditions and/or events by dotted arrows
- Each event or condition should be based upon valid evidence or, if presumptive, shown by dotted rectangles or ovals
- The primary sequence of events is depicted in a straight horizontal line (bold arrows are suggested)
- Secondary event sequences are presented at different levels
- Relative time sequence is from left to right

Criteria for Events Description

- Events must describe an occurrence, not a condition
- Events must be described with one noun or verb
- Occurrence must be precisely described
- Events must describe one discrete action
- Events should be quantified when possible
- Events should range from beginning to end of the accident sequence
- Each event should be derived from the one preceding it

4.2 CONDUCTING AN ANALYSIS

The diagram should be started as soon as facts about the incident begin to be collected. The construction of this ‘diagram’ will only be a skeleton of the final product, but it will ensure that valuable information is not forgotten or lost during the investigation.

Events and conditions will not necessarily emerge in the sequence in which they occurred during the incident. Initially, there will be unresolved gaps. The effort of the analyst and/or investigation team should focus on identifying information to resolve these gaps.

The diagram will frequently need to be updated as more information is gathered. It is therefore important to choose a format that can easily be modified. An effective technique involves the use of the yellow self-adhesive stickers and a large sheet of paper (e.g. flipchart paper). A single event is written on each sticker and affixed to the paper. As a more complete picture of the incident emerges, the stickers can be added, removed or rearranged. Using the large sheet of paper as a base allows the investigators to take the chart with them if they need to move between conference rooms, offices or locations involved in the incident.

4.3 EVENTS AND CAUSAL FACTORS CHARTING

4.3.1 Overview

The principle of using sequence diagrams was adopted by the U.S. Atomic Energy Commission, (developers of MORT see Section 6.1). Events and Causal Factor diagrams are now an integral part of the MORT root cause analysis system. Subsequently, many other root cause analysis programmes have included Events and Causal Factor diagrams in their armoury of methods, including HPES, SRP, TapRooT™ and HPIP. The TapRooT™ software for Event and Causal Factors Charting is reviewed with the other TapRooT™ software in section 6.3.

The purpose of Events and Causal Factors Charting is to identify and document the sequence of events from the beginning to the end of the incident, and to identify the factors, conditions, failed barriers, energy flows etc. that contributed to the incident.

4.3.2 Structure

The generic structure of the Events and Causal Factors chart is shown in Figure 4.1, while Figure 4.2 shows a simple example of an Events and Causal Factors chart. It should be noted that for major accidents such charts become very involved and complex, yet once completed allow a clear understanding of the event sequence and conditions underlying it.

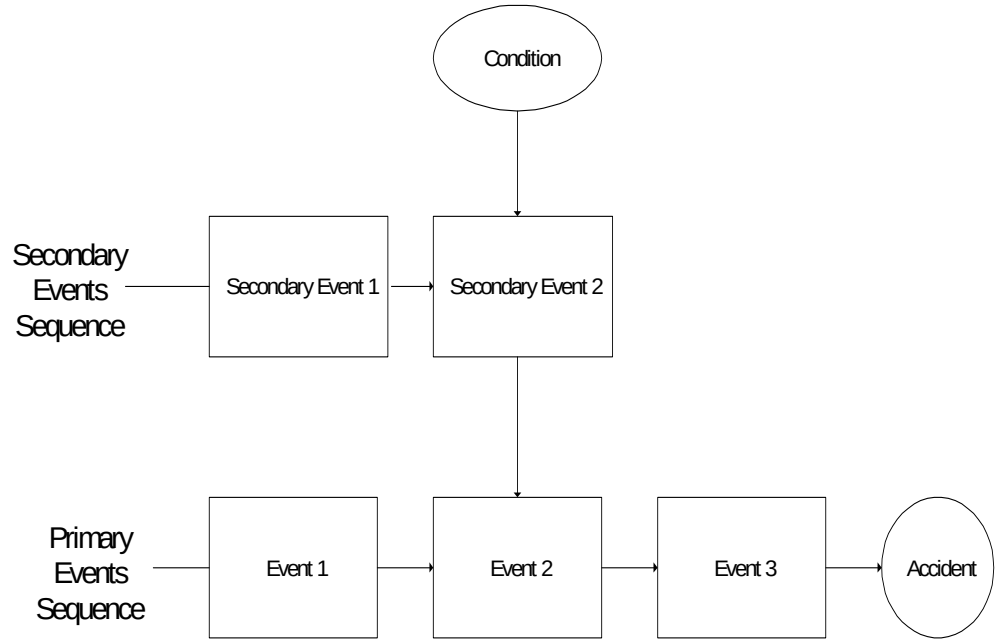


Figure 4.1 : Generic Structure of an Events and Causal Factors Chart

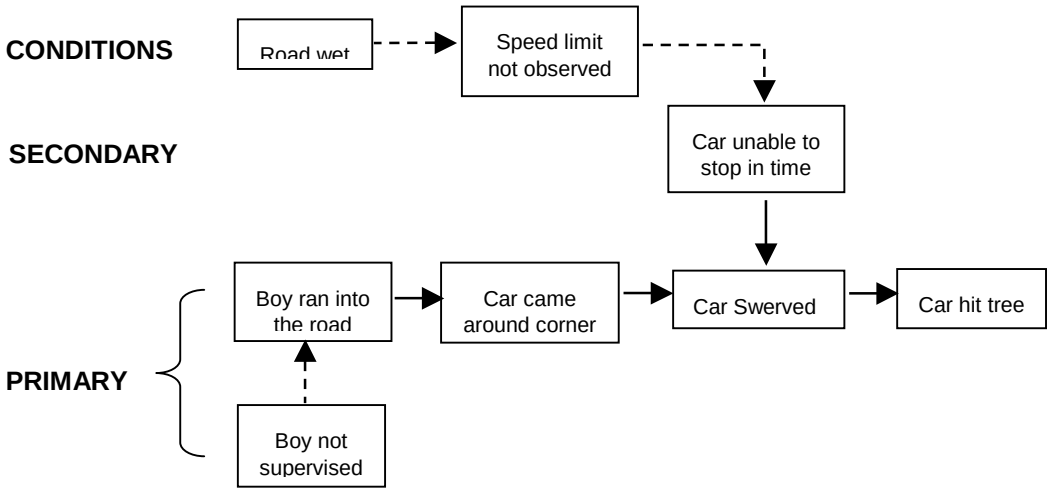


Figure 4.2 Example of an Events and Causal Factors Chart

4.4 MULTILINEAR EVENTS SEQUENCING

4.4.1 Overview

Benner (1975) is responsible for the principles and concepts used in Multilinear Events Sequencing (MES) diagrams. The introduction of MES incorporated timelines into sequential diagrams, providing a scale that parallels the sequences of events to show the time relationships between events and the incident.

The method distinguishes between actors, actions and events. Actors can be people, equipment, substances etc., while actions are anything that is carried out by an actor. Events are the unique combination of one actor plus one action during the incident process. The primary aim of the method is to help the analyst to identify the main actors and their actions and map the relations between these events along a flexible timeline.

4.4.2 Structure

The timeline is drawn horizontally across the page, with time progressing from left to right. The boundaries of the time scale must be carefully defined. The onset of the incident, T_o, is defined as the first event that disrupted the stable situation. The end point is defined as the last consecutive harmful event connected directly with the incident, and is denoted as T_n .

MES requires all the 'actors' to be identified. An actor is defined as something that brings about an event and may be a person, a piece of equipment, a substance etc. These are listed vertically down the left hand side of the page.

To the right of each actor's entry on the chart will be found the specific events that involved the particular actor. These events are arranged horizontally in sequence, and are spread out according to the time intervals at which they occurred. Each event represents a single action undertaken by a specific actor. Figure 4.3 shows a schematic version of an MES diagram.

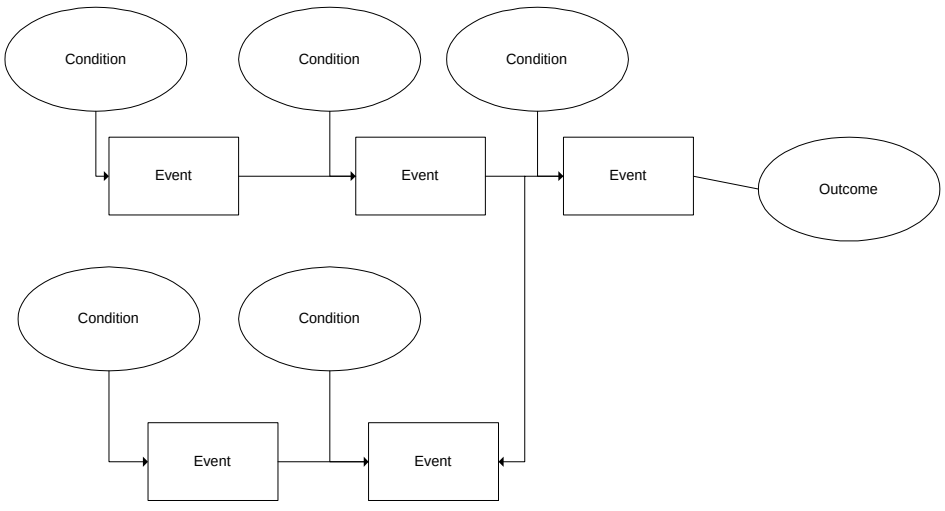


Figure 4.3 : Schematic of an MES DIagram

4.5 SEQUENTIALLY TIMED EVENTS PLOTTING PROCEDURE

4.5.1 Overview

The Sequentially Timed Events Plotting Procedure (STEP), developed by Hendrick and Benner (1987), is essentially a refinement of the MES technique, see Section 4.4. However, a whole volume has been written to support the technique which provides guidance on the complete investigation process.

A STEP worksheet is provided to structure the analysis; this is essentially a pair of axes. Actors involved in the incident are listed down the vertical axis and a timeline is established on the horizontal axis. A conceptual representation of the STEP diagram is presented in Figure 4.4.

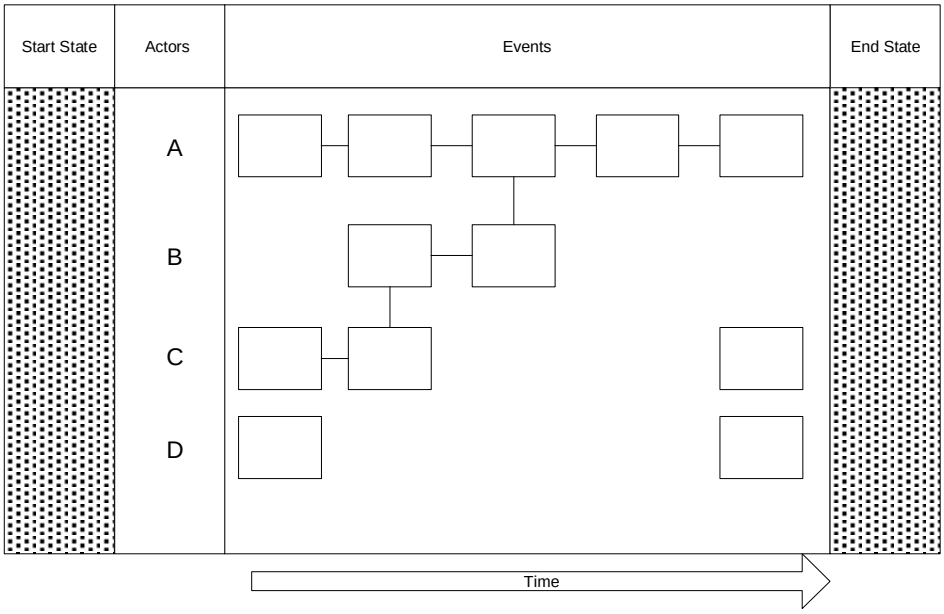


Figure 4.4 : Schematic Representation of a STEP

4.5.2 Structure

Each actor's actions are traced from the start of the incident to the finish. Events are positioned relative to one another along the timeline and causal links are represented through arrows connecting various boxes on the timeline.

One-to-many and many-to-one relations can be represented in the diagram. If data cannot be found to verify the relation between an event pair, then a technique called backSTEP can be used to explore gaps in understanding. Essentially backSTEP is a fault tree which uses the event with no arrows leading to it as the top node. The analyst then develops possible event flows that could describe what happened during the gap in events in order to cause the top node.

4.6 SCHEMATIC REPORT ANALYSIS DIAGRAM

4.6.1 Overview

The Schematic Report Analysis Diagram (SRAD) approach, described by Toft and Turner (1987) uses a slightly different approach and means of presentation to the three techniques previously described. The distinction between events, conditions and actors is not so clear with this technique

4.6.2 Structure

The convention in these diagrams is to enclose conditions in solid boxes that were fully appreciated before the incident and use broken lines to identify conditions that were hidden or only partially understood before the incident. With SRAD the final event is positioned at the bottom of the page with the preceding events arranged vertically in chronological order, the earliest events appearing at the top of the page. Arrows are used to show sequence and the interrelationships between events.

4.6.3 Conducting an Analysis

The paper by Toft and Turner (1987), states that the diagram is constructed from the draft report of the incident. Events which the analyst feels have had a bearing on the development of the incident should be extracted from this text. These should then be assembled in chronological order and in a manner which illustrates causal links. They emphasise that the development of the final diagram will probably be an iterative process as information is examined more closely and the interaction between events is established.

4.7 SUMMARY

These methods are relatively easy to learn and do not necessarily require the analyst to have knowledge of the system under investigation, providing they understand the principles of the method and can consult with 'experts'.

The production of a diagram depicting the sequence of events leading to an incident provides a number of advantages. These are summarised by Ferry (1988) into three main areas: Investigation, Identifying Actions and Reporting.

Investigation

- Summarising the events in the form of a diagram provides an aid to developing evidence, identifying causal factors and identifying gaps in knowledge
- The multiple causes leading to an incident are clearly illustrated
- Diagrams enable all involved in the investigation to visualise the sequence of events in time, and the relationships of conditions and events
- A good diagram will serve to communicate the incident more clearly than pages of text, and ensure more accurate interpretation

Identifying Actions

- The diagram will provide a cause orientated explanation of the incident
- Areas of responsibility will be clearly defined

Reporting

- Summary diagrams can be used in reports to provide a concise, easy-to-follow-representation of the incident for readers.
- Diagrams should help to prevent inaccurate conclusions by revealing any gaps in the logical sequence of events
- Where gaps are identified, the requirement for further analysis / investigation can be raised

- Diagrams provide a means of checking the conclusions with the facts uncovered
- Recommendations can be evaluated against the events and causal factors identified in the diagrams.

Except in the case of STEP, little guidance is given on how to collect the information required to construct the diagrams. There is a reliance on the knowledge and experience of the analyst or investigation team. Care must therefore be taken to prevent an investigation team 'locking' into a preconceived scenario of the incident.

Furthermore, it will be evident that sequence diagrams alone do not identify the root causes of the incidents, and that they should be used in conjunction with other techniques.

5.0 IDENTIFICATION OF CRITICAL EVENTS

5.1 INTRODUCTION

The techniques of Barrier, Change and Fault Tree Analysis do not tend to be used to identify the root causes of incidents per se. However, the principles and concepts they employ have provided the foundation for almost every root causes analysis technique. These methods are incorporated into some root causes methodologies to identify the direct causes of incidents or the 'critical events'. Thus, they act as a filter to reduce the number of direct causes to which further analysis methodologies will be applied.

Although the three methodologies are quite different, there are some common advantages and disadvantages discussed below:

5.2 BARRIER ANALYSIS

5.2.1 Overview

The concepts utilised in barrier analysis were originally developed in Hienrich's domino theory back in the 1930s. Johnson (1980), the author of the Management Oversight and Risk Tree (MORT) system, cites Haddon (1966) and Gibson (1961) as developers of the concept of an accident as an abnormal or unexpected release of energy. Barrier analysis utilises this idea in its approach to accident prevention by suggesting that to prevent an accident a barrier must be erected between the energy source and the item or person to be protected, see Figure 5.1, taken from Dew (1991).

Barrier analysis provides a structured way to consider the events related to a system failure. The ideas behind barrier analysis were taken up by Johnson and form the basis upon which the MORT tree has been developed. An accident within the MORT framework is represented as an unwanted energy flow that comes into contact with people. Three conditions are therefore required for an accident to occur, namely;

- an unwanted flow of energy
- failure or omission of a barrier
- presence of people

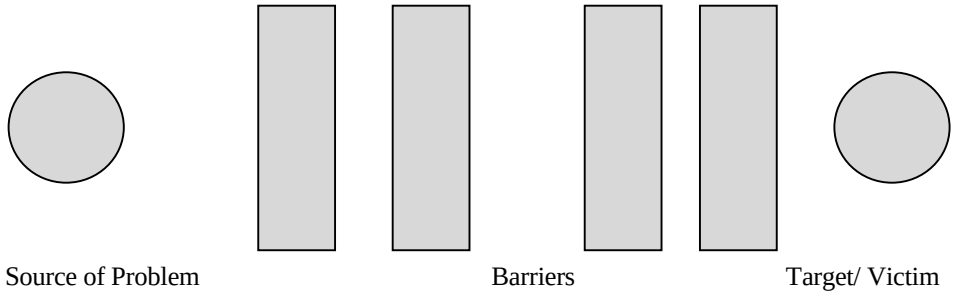


Figure 5.1: Representation of the Barrier Analysis Concept

In the event of an accident occurring, MORT requires the investigation of failures in each of these three elements. Given that accidents typically have more than one cause, it will usually be necessary to repeat the analysis for multiple energy transfers, and barrier failures that led to the final failure resulting in the accident.

The term barrier encompasses a wide range of preventative measures such as guards, personal protective equipment and failsafe systems on large pieces of equipment or plant. However, barriers need not be physical objects but could include preventative measures such as working procedures, training, supervision, space, time, emergency plans and management and organisational controls such as design and safety reviews and risk assessments.

Since the publication of the MORT system other root causes analysis systems have been developed that have utilised the barrier analysis technique described by Johnson.

5.2.2 Structure

No real structure is given for the conduct of a barrier analysis. Essentially the model is that given in Figure 5.1, and the analyst seeks to identify the barriers through asking questions and conducting initial investigations .

MORT has used the barrier analysis technique and incorporated it into a tree structure, making the process more systematic and formalised. This is discussed in more detail in Section 6.1.

5.2.3 Conducting an Analysis

Paradies et al (1993b) state that the following five questions must be answered to complete a barrier analysis:

- What physical, natural, human action, and/or administrative controls are in place as barriers to prevent this accident?
- Where in the sequence of events would these barriers prevent this accident?
- Which barriers failed?
- Which barriers succeeded?
- Are there any other physical, natural, human action, and/or administrative controls that might have prevented this accident if they had been in place?

5.3 CHANGE ANALYSIS

5.3.1 Overview

The concept of change-based analysis was refined by the Rand Corporation for the US Air Force in the early 1960s. The method was widely used in quality control, but took longer to become established as a safety tool.

As with barrier analysis, the principles of change analysis are widely recognised as a systematic framework for examining incident causation. Change analysis has now been adopted as an investigative tool in a number of incident investigation procedures including MORT and HPIP and is described by Johnson (1980). It is regarded as a complementary technique to support root causes analysis.

The basic premise of change analysis, is that if a system performs to a given standard for a period of time and then suddenly fails, the failure will be due to a change or changes in the system. By identifying these changes it should then be possible to discover the factors that led to the failure arising.

Two other concepts that come in to play here are the directional and exponential characteristics of change. That is, if a change is made the system will continue to follow that direction unless another change is made towards a new direction or back to the original status. Furthermore, if a number of changes are made their combined effect is said to interact exponentially rather than additively.

The change analysis technique requires a comparison between the period before the incident occurred and the incident situation. Having established the differences, their contributions are then evaluated. This is shown diagrammatically in Figure 5.2.

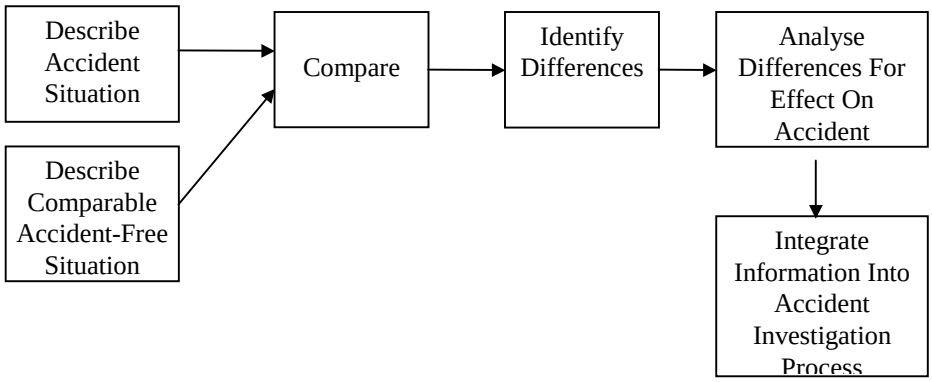


Figure 5.2: Overview of the Change Analysis Process

5.3.2 Structure

Worksheets can be used to structure investigations using change analysis. The basis of these worksheets is an assessment of eight event factors; What, Where, When, Who, Task Nature, Working Conditions, Presence of a Trigger Event, and the Prevalence of Managerial Controls. Through application of these structured worksheets the analyst is able to examine the influence of each factor upon the incident in terms of; the present situation, the prior comparable situation, the differences that exist between the two and the affective changes that have taken place, if any. The eight factors cited on the worksheet form the structure of the change analysis. They are not cast in stone and other factors should be added as required by those conducting the analysis.

5.3.3 Conducting an Analysis

The process identified by Kepner and Tregoe (1976) is cited in many other texts and involves six basic steps:

- Examine the incident situation
- Consider comparable incident-free situations
- Compare the two situations
- Write down all the differences between the two situations, whether they appear relevant or not
- Analyse the differences for effect on the incident
- Integrate the differences into incident causal factors

The technique leaves the analyst to assess the causes of the incident based on the differences identified.

5.4 FAULT TREE ANALYSIS

5.4.1 Overview

The concept of fault tree analysis (FTA) has been around since at least 1961. It is a deductive methodology, that is it involves reasoning from the general to the specific, working backwards through time to examine preceding events leading to failure. FTA is used for determining the potential causes of incidents, or for system failures more generally. The safety engineering discipline uses this method to determine failure probabilities in quantitative risk assessments.

A fault tree is a graphic model that displays the various logical combinations of failures that can result in an incident, as shown in Figure 5.3. These combinations may include equipment failures, human errors and management system failures. The tree starts with a 'top event' which is a specific undesired event (accident) or system condition. This top event is then broken down into a series of contributory events that are structured according to certain rules, and logic. This process of breaking down the events to identify contributory causes and their interaction continues until the root causes are identified.

Once the fault tree is completed it can be analysed to determine what combinations of failures or other faults may cause the 'top event'.

The aim of the fault tree is to find the minimal cut set (MCS). This is a group of basic events whose occurrence will cause the top event to occur. A first order cut set consists of one base event that will cause the top event to occur on its own. A second order cut set consists of two events which, in combination, will lead to the top event; a third order cut set consists of three base events and so on. Clearly, a first order cut set identifies the most serious failures that could affect the system, a second order cut set identifies the next most serious combination of failures, etc. By examining the cut sets the analyst can prioritise actions to prevent the top event from occurring.

There are a number of rules that govern the construction of a fault tree. The 'top event' appears at the top of the page and is linked to the basic failure events by logic gates and event statements. A gate symbol can have one or more inputs, but only one output. There are two basic logic gates, the AND gate and the OR gate. An AND gate signifies that all the inputs must be present for an output to occur whilst an OR gate will only require one input for an output to be generated.

The fault tree works back through time. Each level of the fault tree should represent a discrete period of time, and the events should be presented in chronological order with the earliest events at the bottom.

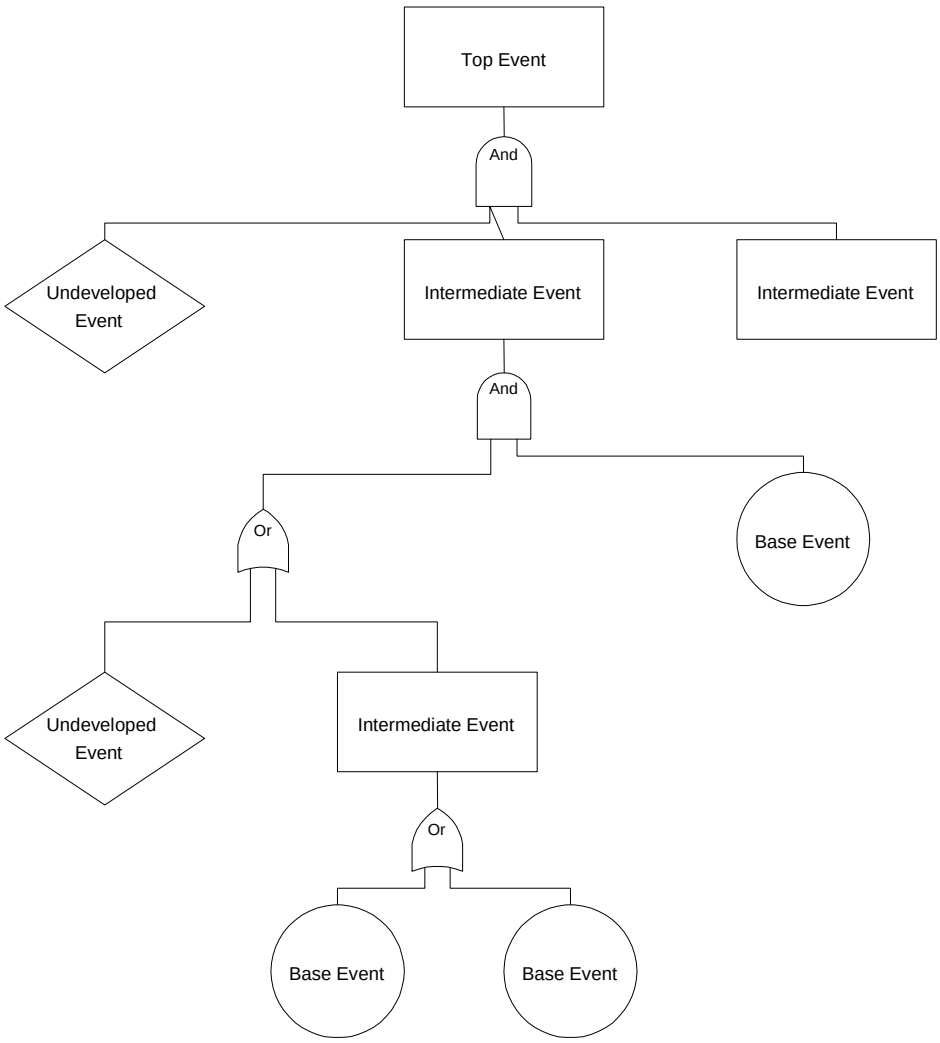


Figure 5.3:Structure of a Simple FTA

5.4.2 Structure

A number of fairly standard symbols are used in the construction of fault trees. These are divided into symbols that depict different classes of event, and those that represent different logic ‘gates’ that hold the events together. These symbols are shown in Figure 5.4.

If the fault tree has been developed to a sufficient level of detail each element of the minimum cut set will represent a root cause.

5.4.3 Conducting an Analysis

The first step in conducting a FTA is to define the ‘top event’, or undesired failure. This is one of the most important steps in the process if the analysis is going to be meaningful. The definition must not be vague or ambiguous.

The top event is broken down by the analyst who identifies the failures and events that contributed to the top event. In addition, the logic behind the combination of the contributory failures must be developed and incorporated into the fault tree diagram. Clearly, the analyst needs to have a thorough knowledge of the system under review, in order to ensure that the fault tree is constructed correctly.

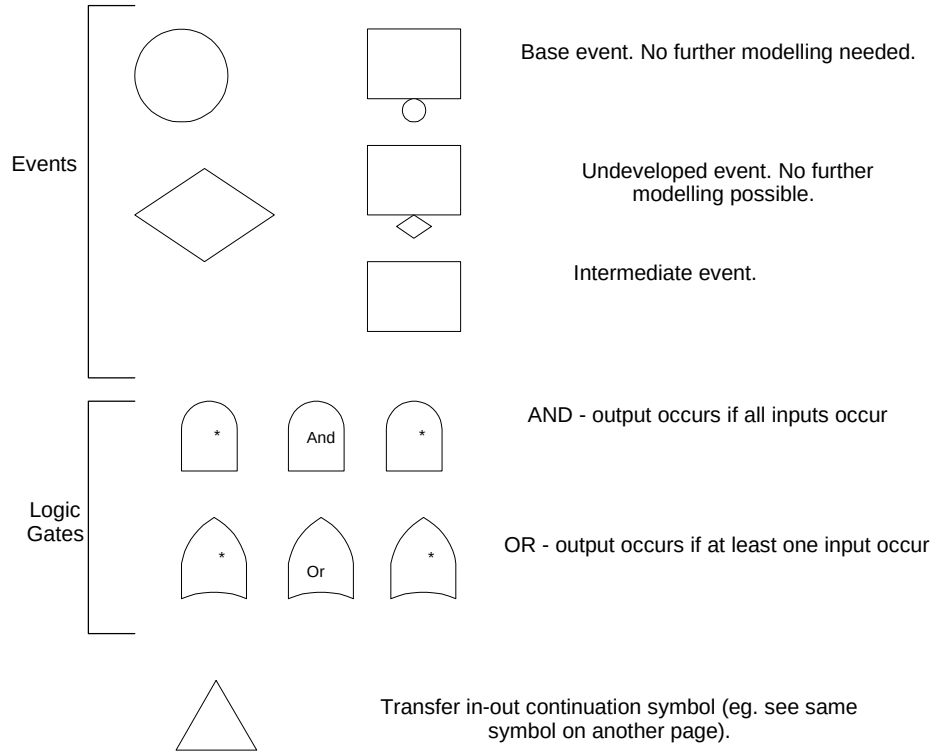


Figure 5.4 : Very Basic Fault Tree Symbols

The process of breaking down the events in the tree and evaluating the logic continues until the base events are reached. Typically, where fault trees are used in quantitative analysis, the base event will be defined by the available reliability data. If data is available the analysis will stop, if not the analysis will continue. In the context of root causes analysis, the definition provided by Paradies and Busch (1988) could be used to define the base events, i.e. events that management have the control to fix.

The analyst should check the output to make sure that the cut sets make sense, by working through the logic and verifying that the base events will in fact lead to the top event.

5.5 SUMMARY

All three of these critical event identification techniques are flexible and may be applied to any type of problem, both simple and complex, to identify potential causes for further investigation

The concept of energy transfer presented in Barrier Analysis has formed the basis of the majority of root causes analysis techniques discussed in this report. Similarly the principles of Change Analysis have been heavily utilised.

It will be seen in Section 6 that the principles of Fault Tree Analysis have been adapted in a number of forms in the development of root causes analysis techniques. The simplest methods adopt the tree format for the presentation of different levels of cause, while others attempt to incorporate the principles of logic in a simplified format. As with FTA, each of these systems will examine one particular failure at a time.

The use of logic allows the thinking of the analyst to be scrutinised easily, and assists with identifying gaps in understanding or knowledge during the investigation process. The graphic representation used in FTA, assists understanding for easier interpretation of events.

The methods reviewed in this section do not actually suggest the root causes, but provide a structure to aid diagnosis. The limitation of using such methods as stand alone investigation techniques is that the causes identified by the analyst may only represent failures at level 2 and 3 (see Figure 1), of the system, thereby not representing root causes. Thus, true root causes analysis is totally dependant on the expertise of the analyst.

All of the methods are dependent upon the knowledge the analyst has of the failed system, and their experience in applying the technique. If an analyst is not totally familiar with a process or is not systematic then the quality of the output will be limited. If the analyst lacks system specific knowledge then the support of a systems expert should be sought. The role of the analyst then is to focus on ensuring a systematic and structured investigation is conducted. Extensive training is required in the application of the FTA technique.

6.0 ROOT CAUSES IDENTIFICATION - 'TREE TECHNIQUES'

6.1 MANAGEMENT OVERSIGHT AND RISK TREE (MORT)

6.1.1 Overview

The development of MORT was initiated by William Johnson and sponsored by the U.S. Atomic Energy Commission (AEC). MORT is a comprehensive, analytical procedure that provides a disciplined method for determining the causes and contributing factors of major incidents. It can also be utilised as a tool to evaluate the quality of an existing safety programme.

In the middle and late 1960s, there were few methods available for the investigation of accidents. Within the AEC attempts had been made to apply fault tree analysis (FTA) logic to existing accident reports, and this technique was found to be of value. It was noted that for a variety of accidents studied using FTA, similar patterns of causal factors were being uncovered. This observation of commonality eventually led to the development of a tree, based loosely on fault tree conventions, that represented an 'ideal safety management system'. The principles incorporated into this model were identified from a thorough review of best practices and 'state-of-the art' safety management system concepts.

MORT therefore uses similar symbols and logic to that used in FTA. However, there are two main differences between the techniques that should be noted. Firstly, MORT represents a fault tree that has already been constructed. The analyst is not required to build the tree, but to work through the existing model and discard those branches which are not relevant to the incident under review. Secondly, MORT not only looks at what happened during an incident, but traces causal factors back to management systems to identify why events happened, thereby departing from strict FTA logic.

6.1.2 Structure

MORT consists of eight interconnecting trees, through which 98 generic problems and 200 basic causes can be identified. The number of basic causes can be increased to 1500 in some instances through the transfer of parts of the tree to other relevant areas. Generic problems are represented by text in rectangular boxes, while circles are used to identify basic causes.

As with FTA, the MORT chart starts with a top event that represents some kind of loss e.g. an injury, property damage, loss of production etc. Once the extent of the incident is established, the user arrives at the first logic gate which is an OR gate. The model states that the loss will have arisen from either an 'Assumed Risk' or 'Management Oversights and Omissions'. Only those risks which have been identified, analysed and accepted at the appropriate management level can be Assumed Risks; unanalysed or unknown risks are Oversight and Omissions by default. Mistakes could have been made when initially accepting a risk, therefore the assessment should still be applied.

The next major sub-division separates what happened from why. The 'what happened' considers the specific control factors that should have been in operation while the 'why' considers general management system factors. It is the 'what happened' branch of the tree which forms the major assessment route during incident analysis.

The MORT chart continues to break down each of these factors until the basic causes are reached. In some instances this amounts to 13 levels. At certain points triangles are used to show where portions of the tree might be repeated.

The MORT chart has been constructed to incorporate time into the model, although this is not too explicit. Those factors found to the bottom and to the left of the chart occurred earlier than those to the right and the top. Thus, with the 'Specific Control Factors' occurring at the top of the chart, the analyst is required to work backwards in time through the incident.

6.1.3 Conducting An Analysis

MORT is not a technique that would be used in the field. The analysis would therefore start with an accident report and possibly a sequence diagram. Events and Causal Factors Charting is described by Johnson (1980). The analyst must first establish the facts regarding the top event, for example:

- What happened?
- Why?
- What were the losses?

The MORT User's Manual states that the MORT chart should be used as a working paper. That is, a copy should be used so that notes can be made in appropriate places on the page. Furthermore, the use of coloured pens is advocated in order to allow the progression of the analysis to be assessed at a glance.

The aim of the analysis is to work through the entire chart and identify those basic causes that have contributed to the top event. The analyst achieves this by asking a number of questions at each juncture on the chart. The first requirement is to establish whether the elements are applicable to the incident. If not, these items should be crossed out in black. For those elements that remain, the question 'was this item adequate?' is asked. If the analyst does not know the answer to the question, this indicates that more information needs to be sought on the incident and the element should be marked blue. Where it is judged that elements are less than adequate, they should be marked in red, and those that are found to be acceptable should be indicated in green. The analysis ends when all the elements marked in blue have been addressed and subsequently judged as either adequate or less than adequate.

To assist the analyst in judging whether the basic causes are 'adequate' or 'less than adequate' (LTA), there is a supporting text to accompany the MORT chart outlining the criteria which should be met.

A software tool based on the MORT tree, the Intelligent Safety Assistant (ISA), has been developed by Koornneef and Hale, of Delft University of Technology. ISA is a method of applying MORT methods for registration of incidents at work in order to ensure consistent data collection and the generation of diagnostic messages about critical or failing safety management factors underlying a single accident, near miss or Safety Management System (SMS) failure event. The software tool has been tested in field trials in Poland in a wide range of industries and in the Netherlands in a university hospital. The system is currently being transformed into an operational prototype.

6.2 SAVANNAH RIVER PLANT (SRP) ROOT CAUSES ANALYSIS SYSTEM

6.2.1 Overview

The SRP approach to root cause analysis was developed under contract from the US Department of Energy in the late 1980s, and is described by Paradies and Busch (1988).

Essentially the SRP system follows a similar structure to MORT, starting with a description of the incident using Events and Causal Factors Charting, and using a pre-defined generic tree to identify root causes. However, there is no logic incorporated into the SRP tree structure. Furthermore, there is less emphasis on management oversights, because the system was developed for use in the investigation of human performance related events at nuclear power plants.

The initial divisions in the tree relate to 'operator difficulty', 'equipment difficulty' and 'technical difficulty', with aspects of management being incorporated lower down the structure. In addition, the tree was developed specifically for the Savannah River Plant, incorporating the organisational structure into the tree. However, the tree can be tailored to suit most organisational structures.

6.2.2 Structure

The root causes tree is divided into many sections which in the SRP system are referred to as 'nodes'. The tree is further divided into six levels, A to F, with each level becoming successively more detailed until the root causes are reached at level F.

The first branches of the SRP system relate to the type of 'difficulty' encountered. From this point the different departments within the organisation relating to these areas are identified. Under each department Basic Cause Categories (BCC) or Equipment Reliability Causes are listed.

According to Paradies and Busch (1988), the tree used in the SRP system incorporates seven human performance Basic Cause Categories, namely:

- Procedures
- Training
- Quality Control
- Communications
- Management Systems
- Human Engineering
- Immediate Supervision

and five Equipment Reliability Cause Categories:

- Preventative Maintenance Less Than Adequate
- Repeat Failure
- Unexpected Failure
- Design
- Equipment/Parts Defective

The categories included in the tree presented by Armstrong (1989), from which the symbols are obtained, are organised slightly differently, but essentially cover the same items. One notable addition in the Armstrong tree is the Category of Personal Performance, which needs to be used with particular care if the connotation of 'blame' is to be avoided. These categories are further sub-divided into Near Root Causes under which are listed relevant Root Causes.

6.2.3 Conducting an Analysis

Information is collected about the incident and an Events and Causal Factors diagram is constructed. The analyst must decide which of the causal factors, if removed, would have prevented the incident from occurring. It is these factors that are considered further using the root causes analysis tree.

For each causal factor, the analyst determines which top level node is applicable. Based on this decision, the analyst moves down to the next level node and selects another applicable option from this level. Only lower level nodes branching from the node chosen on the previous level can be considered. For those found to be relevant, the process continues with the analyst working further down the tree structure to identify the applicable Near Root Causes and finally the Root Causes. An example of Near Root Cause is the application of a wrong or incomplete procedure, whilst a Root Cause is that that procedure had a typo, was the wrong revision or contained incorrect information.

The system was developed on the basis that 80% of all events in a complex system such as a nuclear plant are caused by "system" problems which are the responsibility of the management and over which, operators have no direct control. The remaining 20% are considered to be strictly human error. Hence both human performance and management system are considered in the technique but the greater emphasis is on system issues.

6.3 TAPROOT™

6.3.1 Overview

Mark Paradies who was involved with the development of SRP went on to become the President of System Improvements Inc., the company responsible for TapRooT™. Published around 1991, the TapRooT™ incident investigation system is a technique that is based closely on the SRP system. After the publication of TapRooT™, System Improvements Inc. and Concord Associates Inc. were commissioned by the US Nuclear Regulatory Commission to develop HPIP which was published in 1993 and is reviewed in Section 6.4.

There are many similarities between the three systems. All three use Events and Causal Factors charting. From the papers examined, Paradies and Busch (1988), Unger and Paradies (1992), and Paradies et al (1993b), the Cause Trees used in TapRooT™ and HPIP would appear to be virtually the same as SRP. TapRooT™ and HPIP differ slightly in that instead of using a complete tree structure they use a logic diagram to steer the auditor to the appropriate Basic Cause Categories. From this point the tree structures are then utilised.

Three steps are included in the TapRooT™ incident investigation system approach to root cause analysis, namely:

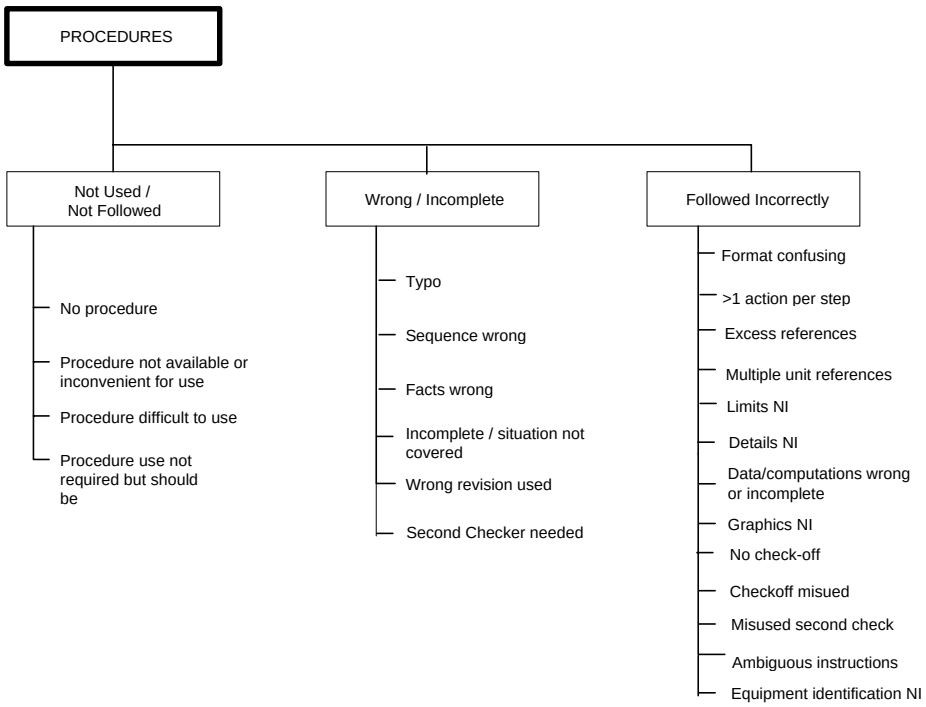
1. Collection of information
2. Development of Events and Causal Factors Chart
3. Use of Root Cause Tree™

6.3.2 Structure

The paper by Unger and Paradies (1992) does not present the completed Root Cause Tree™, but a single Basic Cause Category 'branch' is shown. Twelve Basic Cause Categories are listed, that are the same as those described in Section 6.2.2. An example of the Procedures Basic Cause Category is presented in Figure 6.1. Being a generic system available on the open market, this system does not incorporate the organisational structure defined in the SRP system.

TapRooT™ is an integrated system that includes an investigation process, five root cause analysis techniques and a computer database. The method is specifically designed to help investigators identify the causes of human performance problems. A paper based expert system known as the TapRooT™ Human Performance Trouble Shooting Guide is provided to assist those not so familiar with human performance analysis to determine which categories are most relevant to the incident under investigation. This consists of 15 questions that elicit yes/no responses displayed as a flow diagram.

Figure 6.1: Procedures Basic Cause Category
Used with permission of System Improvements, Inc., USA.



6.3.3 Conducting an Analysis

The overall procedure is essentially the same as that described in Section 6.2.3, with the steps required being collection of information, drawing of an Events and Causal Factors Chart and identification of root causes. Both the second and final steps of this procedure may be carried out either on paper or using computer software developed by System Improvements Inc. for that purpose.

Event and Causal Factors Charting is described in full in the TapRooT™ Manual and section 4.3 of this review. System Improvements Inc. produce a software package for the production of E&CF charts which is essentially a graphics package only. The user must provide the expertise for development of the chart structure and for identification of causal factors. Guidance is given in the TapRooT™ Manual.

The next stage in the TapRooT™ incident investigation system is the use of the TapRooT™ Root Cause Tree. This represents a set of generic causal trees (or check lists) that is applied to each of the previously identified causal factors. The three operational techniques are Barrier Analysis, Change Analysis and Critical Human Action Profile (CHAP). The overall technical approach of TapRooT™ is similar to HPES.

The computer based system, TapRooT™ for Windows uses the Root Cause Tree™ for identification of root causes. An E&CF chart created on computer may be imported directly into the main TapRooT™ Root Cause Analysis software. Alternatively, the analyst may input incident details directly. Information relating to the incident must be readily available and any causal factors already identified. Determination of the correct path through the generic tree for each causal factor is dependant on the analyst, whether using the computer based system or the paper based system.

The Human Performance Difficulty option leads the analyst to answer 15 questions in order to continue down the tree towards the root cause. It should be noted that all questions must be answered otherwise the computer package assumes a positive response. The analyst is led down the tree until the identification of root causes is reached. The TapRooT™ Manual is provided as on line help.

The Equipment Difficulty category also leads the analyst through specific branches of the generic tree. The Natural Phenomenon / Sabotage and Other categories require the analyst to provide an explanation of the choice in comment form.

Reports are produced automatically by the computer package. The software will also produce the completed Root Cause Tree™. Final analysis of the study is left to the analyst.

6.4 HUMAN PERFORMANCE INVESTIGATION PROCESS (HPIP)

6.4.1 Overview

HPIP was developed by Paradies et al (1993a, b & c) to meet the specific requirements of the US Nuclear Regulatory Commission. Essentially HPIP consists of six tools that may be utilised in the accident investigation process as required, namely:

- Events and Causal Factors Charting: - This tool helps to plan an accident investigation, assisting in the collection of facts. This tool enables the development of a thorough understanding of the events, ensuring complete investigation and accuracy of perceptions. Through Events and Causal Factor Charting the correctable causes for specific events can be identified, allowing the incident to be accurately documented and effectively presenting management with the findings.
- SORTM - A guide to HPIP Modules (similar to the TapRooT™ Human Performance Trouble Shooting Guide): - This tool can also be used to assist investigation planning and fact collection. SORTM identifies human performance difficulties for root cause analysis, finding correctable causes for a specific event.
- Barrier Analysis: - Like SORTM, barrier analysis can be used to identify human performance difficulties for root cause analysis. It can also be applied to ensure that corrective actions address the root causes, and that violations are identified.
- HPIP Modules: - This tool essentially identifies important trends or programmatic system weaknesses.
- Change Analysis: - allows understanding of the event and ensures complete investigation and accuracy of perceptions.

- CHAP - Critical Human Actions Profile: - like change analysis, CHAP provides an understanding of the event and ensures complete investigation and accuracy of perceptions.

Three volumes describing these tools and their application to incidents were published in 1993. Events and Causal Charting, Barrier Analysis and Change Analysis have been discussed elsewhere and will not be described further.

The Critical Human Action Profile, (CHAP) is based upon task analysis, a human factors technique and is used to identify the human actions which, if they had been performed correctly, could have prevented the event from occurring or reduced the event's consequences. This tool tends to be used early in the investigation to provide information for later use, rather than identifying root causes per se, and it concentrates on human rather than system performance.

6.4.2 Structure

Instead of an overall tree structure, SORTM, a logic tree, is used to identify the relevant Basic Cause Categories in TapRooT™ or HPIP modules. There are six HPIP modules, which concentrate on factors influencing human error during nuclear events and include all the Basic Cause Categories listed in Section 6.2.2 except for Quality Control. Equipment Reliability is not considered in this system.

Each module is supported by a worksheet in the Investigators Manual which poses a series of questions to assist the analyst in the identification of the Near Root Causes and Root Causes. An example of Near Root Cause is the application of a wrong or incomplete procedure, whilst a Root Cause is that the procedure was the wrong revision or contained incorrect information.

6.4.3 Conducting an Analysis

Information about the incident is gathered. The collection process may be directed by conducting preliminary analysis using E&CF charts and SORTM. When sufficient information is available and the chart is complete, barrier and change analysis can be used to identify the critical steps in the sequence. For each critical step the root causes of failure should be identified using the SORTM and the HPIP modules.

The analyst works through the SORTM logic chart answering the questions 'yes' or 'no'. This enables the appropriate HPIP modules to be identified. For each identified module the analyst considers the questions in the supporting worksheet. An example of the sort of questions asked is, for the Procedure HPIP module, 'was the task done without a procedure when a procedure should be used?' and if the answer is yes the analyst is to continue to other questions such as 'if there should be a procedure, was it available?'. The output of this questioning is to identify the root causes.

6.5 CAUSAL TREE METHOD (CTM)

6.5.1 Overview

CTM is used by Rhone Poulenc and is described by Boissieras (1983), although it was originally developed by Leplat (1978). As the name suggests, CTM involves the development of a tree of causes. The method utilises deductive logic, but attempts have been made to make the construction of the trees and the logic easier to apply.

The underlying principle of the method is that an accident results from changes or variations in the normal process. The analyst must identify the changes in the system, list the changes, organise them into a diagram and define their interrelationship. Unlike a fault tree, the method only includes the branches actually leading to the incident. Thus no 'OR' gates are represented, only 'AND' gates. The construction of the diagram is guided by simple rules which specify event chains and confluent relationships.

This methodology describes seven steps in the incident investigation process from data collection to follow up actions. CTM requires the analysis to be undertaken by a group including the victim (if possible), supervisor, witnesses, safety officer, member of the safety committee, decision maker and someone experienced in CTM.

6.5.2 Structure

A list of facts is drawn up as a result of the data collection phase of the process. The causal tree is used to put these facts in order and to identify the relationship between them.

The tree starts with the end event, i.e. the incident, and works backwards. A completed tree is shown in AIChE (1992).

6.5.3 Conducting an Analysis

The working group selected for the analysis must collect the data and reconstruct the incident. This method stipulates a written summary rather than a diagrammatic form. From this information the working group must extract the facts relating to the incident. Each 'fact' is a singular event or occurrence.

The list of facts is used in the construction of the causal tree. The end event serves as the starting point and the group must select the facts from the list that contributed to this incident. Working one level at a time the group works backwards through the event until a point is reached at which the team agrees it would be unproductive to go further.

To achieve this three questions are asked.

1. What is the cause of this result?

The items in the list are considered, and those that are agreed to be contributory are selected. The next two questions are considered from this filtered list before items are added to the tree.

2. What was directly *necessary* to cause the end result?

Only those factors that were directly necessary to have caused the result to occur should be selected. Effectively, the items are identified that would contribute to an AND gate in fault tree logic. The OR alternatives may be present but these are not listed, as they complicate the picture. This method is only looking at what has happened and not what could have happened.

3. Are these factors (identified from 2) *sufficient* to have caused the result?

If not, the team need to identify the other factors necessary to complete the logic of the tree. If the answer is yes, then the group can move on to the next stage, considering all of the facts identified here as the end result and breaking them down in turn.

The choice of facts and the way in which the tree is structured must be agreed unanimously by the group. When the group decides that a sufficient level of detail has been reached it must then develop proposals to present to management.

In order to avoid single cause findings from incident investigations, the group is asked to identify a minimum of three factors for each incident, one from each of three broad categories: organisational, human and material factors.

6.6 REASON® ROOT CAUSE ANALYSIS

6.6.1 Overview

REASON® Root Cause Analysis is a software based RCA tool developed in 1997 by Decision Systems Inc. REASON is an expert system that: helps the analyst sort information about an individual problem; models and analyses the problem to get real solutions; provides results to assist in the selection of the best control options.

6.6.2 Structure

The REASON® Root Cause Analysis system involves the input of information about an incident resulting from the data collection phase of the incident investigation. The analyst develops a logic tree by entering the sequence of events. The software prompts and questions the analysts about the reasoning and logic included in the tree in order to establish the logic links between events within the incident sequence. The tree starts with the end event, i.e. the incident, and works backwards.

6.6.3 Conducting an Analysis

The analysis begins with inputting the end event, i.e. the incident that triggered the investigation. The analyst is prompted to input any known direct causes leading to that incident and continue building up a logic tree. The basic procedure is to ask ‘why?’ until a point is reached where there is either insufficient data to continue, the event identified is non-correctable or a corrective action may be identified.

The tree of causes is built automatically by the software using the information input by the analyst. Once no more direct causes are identified for any level of the tree, the software asks questions of the analyst to determine reasoning and establish the logic links for the tree.

If a corrective opportunity is identified the analyst is prompted to state at what level the change should be made: management, supervisory or worker.

The programme then automatically builds up a tree of causes, will present various graphical analyses, produces a narrative report of the incident and root causes identified and carried out analysis of which corrective action would be most appropriate and effective.

6.7 EVENT ROOT CAUSE ANALYSIS PROCEDURE (ERCAP)

6.7.1 Overview

ERCAP has been developed by ENCONET Consulting Ges.m.b.H (Austria) and is a structured new method for system investigation and analysis of the direct cause, contributors and root cause. It has been formulated based on a review of a number of full RCA methods.

It was not possible to obtain any information other than that provided by the company itself, hence the review provided is extremely limited.

6.7.2 Structure

ERCAP was originally an adaptation of HPIP and the safety management factors in the MORT system. The developers have also incorporated aspects of the Assessment of Safety Significance Event Teams (ASSET) system (see Section 8.5).

In ERCAP, the basic full RCA techniques (Change Analysis, Barrier Analysis, Event and Causal Factors and Tree Diagrams) are refined and some advanced techniques such as Accident Evolution and Barrier (AEB - see section 8.2.4) are also adopted to focus the interactions between human and technical aspects. In summary, the procedure has the following main factors:

- a systematic procedure for investigations and analyses from collection and review of information, identification of causal / critical factors and contributing causes to root cause identification and final preparation of the RCA report.

- A combination of RCA techniques

- a logic tree for identifying cause categories from failure of prevention measure to operator responses, from individual actions to the method of management during the event development.

- A comprehensive set of cause modules for identifying and allocating causal factors. These modules include seven cause categories and about 200 causal factors in tree structures. They cover both failures of the basic elements (Personnel, Equipment and Procedures) and inadequacies of the environmental / managerial factors contributing to or resulting in the event.

A computer based tool for the system, called CERCA (Code for Events Root Cause Analysis), is currently being developed.

6.7.3 Conducting an Analysis

The information obtained was not sufficient to carry out an example analysis but the following are some example sub-steps used in the final determination of the root cause of an event based on the causal factors identified:

- distinguishing non-problem related factors
- searching the underlying causal factors
- distinguishing the causal factors which cannot be corrected
- determination of the direct cause and contributing factors
- determination of the root cause of an event.

No further information on the current status of the technique was obtained, hence it is not possible to comment on whether the technique has been used successfully.

6.8 SUMMARY

Tree structured root cause analysis techniques offer the analyst a systematic method of considering the possible root causes associated with an incident.

The majority of the techniques, except for the Causal Tree Method, are prescriptive and list potential root causes for consideration among their branches. This philosophy encourages analysts to contemplate a wide range of causal factors and not just those that immediately come to mind. By presenting all analysts with the same classification system, greater consistency is encouraged between analysts, a comprehensive assessment is ensured and statistical examination of the data collected will be easier.

The prescriptive techniques, on the whole, require less resource than non-prescriptive techniques such as the Causal Tree method. The Causal Tree Method, having no listed causes, relies upon group discussion between 'experts' from different fields, including workers and safety specialists. The output is therefore dependent upon the expertise and enthusiasm of those taking part. Group techniques such as this do, however, present benefits to the organisation in terms of team building, increased awareness of safety issues and ownership of resulting actions.

The incorporation of logic into prescriptive tree structures would not appear to lend much benefit. They make the system more complex than necessary and increase the training requirements considerably. Discussing MORT, Ferry (1988) states that 'Unfortunately people do not learn MORT well in these 'all talk' seminars. It has been found that firsthand use of the tool and a high degree of familiarity are necessary to develop proficiency'. Although it is claimed that a simple tree structure such as TapRooT™, can be learnt adequately in a day.

All of the tree techniques except for the Causal Tree require the analyst to initially develop a schematic diagram (the schematic diagram is essentially incorporated into the Causal Tree method). These techniques are also supported by accompanying texts that help the analyst to judge whether an item is adequate or not. Consequently, these are not really 'field' techniques. The Causal Tree method lends itself more to 'field' application because it requires no documentation and incorporates work groups involving those 'on the scene'. Another point to note is that the majority of these systems have been developed in America, with the exception of ERCAP which was developed in Austria. The resulting models have thus incorporated American health and safety standards.

From a review of the TapRooT™ computer based system, other than data storage and manipulation (which may be achieved with a database) it is not apparent that there are any advantages gained over the paper based system other than ease of navigation through the users manual. The user is still required to undergo all stages of the procedure using judgement and expertise, as in the paper based system, whilst moving around the tree in the software package does not appear to be as useful as having the entire paper version of the logic tree available as an overview.

The logic tree and the worksheets incorporated into the HPIP system take the prescriptive element of the root cause analysis a stage further than the tree structure, providing lists of yes/no questions to assist with the selection of causal categories.

The REASON® computer based system is intelligent in that it automatically builds comprehensive method of constructing a logic tree for an incident. However, this is based purely on the information input by the analyst. The software has no data recording or manipulation properties, like TapRooT™. Information about the incident under investigation would need to be at hand before making use of the software. Like the Causal Tree there are no listed causes, relying on the expert judgement, experience and enthusiasm of those taking part in the investigation.

ERCAP is not a rigid, prescriptive procedure, rather it provides an analytical process and tool for investigation and analysis of operational events in two parts. The first part emphasises the analytical process with steps whilst the second describes the tools in detail. Due to insufficient information on ERCAP it was not possible to completely evaluate the procedure.

7.0 ROOT CAUSES ANALYSIS - CHECKLIST METHODS

7.1 HUMAN PERFORMANCE EVALUATION SYSTEM (HPES)

7.1.1 Overview

This summary is based on reviews by Smith (1988), Paradies et al (1993b) and AIChE(1992) as no documentation of the system was obtained. It is not known whether this system incorporates a tree structure. There has been no mention of one in the papers received, only the presentation of checklists. In 1982 the Institute of Nuclear Power Operations (INPO) conducted a pilot study designed with the objective of improving nuclear plant operations by reducing human error through correcting the conditions that cause the errors. It is a non-punitive, self reporting system and, as such, can analyse 'near-misses' as well as actual incidents. One of the strengths of this system is that the results are reported centrally to INPO, who collate the data and publish the results to all participating utilities.

There are five basic steps in the HPES procedure:

- Collect Data
- Assess
  - Event analysis
  - Root cause determination
- Correct
  - Identification, review and implementation of corrective action
- Inform
- Follow up

Documentation is provided which covers general guidance, recommended techniques and further references for accomplishing each step.

The greater part of the methodology concentrates on five techniques recommended for event analysis. These include Events and Causal Charting, Fault Tree Analysis, Change Analysis, Barrier Analysis as well at HPES. Smith (1988) states that the development of HPES was heavily influenced by the MORT technique.

This technique is well supported with training, documentation and advisory service from INPO. Feedback of the results of investigations within the forty installations operating this system occurs regularly through the publication of newsletters and a database. However, INPO have placed restrictions on the use of their documentation and root cause analysis technique.

7.1.2 Structure

Within HPES seventeen causal factor worksheets are provided, one for each major causal factor identified for human and equipment performance problems. Paradies et al (1993b), list twelve factors which related to human performance (the equipment factors used are unknown):

Verbal Communication	Written Procedures and Documents
Man Machine Interface	Environmental Conditions
Work Schedule	Work Practice
Work Organisation/Planning	Supervisory Method
Training/Qualifications	Change Management
Resource Management	Managerial Method

The worksheets allow up to four performance problems associated with the event to be assessed. The analyst must tick boxes to identify whether the causal factor is applicable or not. If applicable, the analyst moves onto the next section and indicates some factual information about the incident.

7.1.3 Conducting an Analysis

The tools used to collect data and describe the incident will be dependent upon what has occurred. Given that the critical events have been identified, the analyst can use HPES to identify the causal factors. It is not clear from the Paradies et al (1993b) review of HPES how the analyst selects which of the seventeen causal factors are appropriate; presumably guidance is given in the documentation. Four steps are required to complete each worksheet:

- Identify whether the factor is applicable or not
- Identify and document some basic information about the nature of the problem, design features, conditions etc., involved in the event
- Indicate whether each of a number of sub-factors was a primary, secondary or possible contributing factor
- Document and record corrective actions

7.2 SYSTEMATIC CAUSE ANALYSIS TECHNIQUE (SCAT)

7.2.1 Overview

The Systematic Cause Analysis Technique (SCAT) is a method which has been developed by the International Loss Control Institute (ILCI), which can be used to determine the root causes of an incident once a description of the sequence of events has been determined. A paper describing SCAT by Bird and Germain (1985) is reproduced in a manual by ILCI (1989).

The ILCI 'Loss Causation Model' is the framework for the SCAT method. This model views the contributory elements to an incident as a series of five dominoes, namely;

- Lack of Control
- Basic causes (personal factors or job factors)
- Immediate causes (substandard acts and conditions)
- Incident (contact with energy or substance)
- Loss (people, property, process)

In this model loss arises from the dominoes tumbling down and knocking into one another. The way to prevent loss according to this model is to remove one of the dominoes in the sequence, thus preventing the momentum from reaching the loss stage.

Although described differently, this principle is the same as that underlying Barrier Analysis, in that there is an energy transfer from one domino to another in order to knock the series down. To prevent an incident, the energy transfer must be prevented by removing one of the intervening dominoes or by erecting a barrier to prevent the energy transfer between dominoes.

This methodology provides a chart with a series of cross referenced categories. The analyst must identify the relevant factors by working systematically through the chart and identifying whether the factors generated by the cross referencing system are relevant. ILCI provides accompanying text to assist with the definition of categories and the acceptance/dismissal of factors.

7.2.2 Structure

SCAT is presented as a chart which contains five blocks corresponding to the five 'dominoes' presented in reverse order. Thus the first block contains space to write a description of the incident. The second block lists the most common categories of contact that could have led to the incident, for example, contact with electricity, heat, cold or radiation, being hit by a moving object or crushed. The third block lists the most common Immediate or Direct Cause/s of this contact, divided into two categories:

- sub-standard or unsafe act
  e.g. removing safety devices, using defective equipment or improper position for the task;
- sub-standard or unsafe conditions
  e.g. inadequate or improper safety equipment, noise exposure or restricted action.

The fourth block identifies Basic or Underlying Cause/s of which there are two categories: 'Personal Factors' and 'Job Factors'. The former encompasses issues such as physical or psychological stress, lack of knowledge or skill and improper motivation, while the latter encompasses inadequate leadership and/or supervision, inadequate maintenance, tools and equipment.

The final block lists safety management practices that should be addressed to prevent incidents from occurring. There are twenty categories in this block corresponding to the 20 elements of the safety management system developed by ILCI.

7.2.3 Conducting the Analysis

The analyst must first write a description of the incident in the top block on the chart. Secondly, an assessment must be made of the loss potential of the incident.

Once the description has been entered, the next step is to identify the type of energy contact from the given list (there may be more than one) in block number 2. The analyst must then follow the trail of cross references listed beside each type of energy contact selected, and consider whether the item references in block 3 are appropriate to the particular incident.

Similarly for each relevant item identified in block 3, the analyst must follow the cross-references listed to items in block 4, and so on.

Eventually a number of items will be identified in block 5. It is then necessary to identify where the fault in the management system lies. Three possibilities are provided:

- performance standards for the item do not exist and therefore need to be developed
- the performance standards are not adequate and need to be revised
- more effort is required in ensuring compliance with these standards

7.3 TECHNIC OF OPERATIONS REVIEW (TOR)

7.3.1 Overview

TOR analysis was initially developed by Weaver (1973) as a training tool to assist with the prevention of incidents. It has subsequently found application as an investigatory technique for the identification of root causes associated with incidents and accidents. The focus of TOR analysis is on system failures, seeking to identify management failures rather than 'blaming' employees involved. Weaver (1987) wrote the chapter in the book by Ferry (1988) and it is this text that forms the basis of this review.

TOR analysis is presented in a work sheet format. It is a group technique requiring participants to progress through the work sheet answering yes or no to a series of questions. A condition of TOR analysis is that the group reaches a consensus on the answers to the questions.

TOR analysis was utilised for over a decade by policy holders of a US insurance company before being made commercially available.

7.3.2 Structure

The TOR worksheet is divided into eight functional areas, namely:

1. Training
2. Responsibility
3. Decision and Direction
4. Supervision
5. Work Groups
6. Control
7. Personality Traits
8. Management.

Between five and eight numbered statements of systemic failures are listed under each functional area. To the right of each statement is a series of numbers. This is a system of cross referencing and the numbers direct the analysis team to other related statements.

Down the middle of the work sheet are listed all of the reference numbers of the statements of systemic failures. This is used as a checklist to quickly appraise whether all the statements have been considered.

7.3.3 Conducting an Analysis

TOR analysis is generally described as a group technique (Hallock and Weaver, 1990; Weaver, 1987) although it could be conducted by an individual.

Once an incident has occurred and the facts concerning the incident identified, these facts may be analysed using TOR analysis. If a group approach is to be used, then members of the group need to be selected and a leader chosen from within the group to direct the analysis and keep it moving. There are four basic steps in the TOR analysis process:

- Establish the facts.
- Trace the root causes.
- Eliminate insignificant causes.
- Identify realistic actions.

Establish the Facts
Within the group the facts of the incident must first be established, understood and agreed. Once this has been achieved the group is ready to move on to the next stage.

Trace the Root Causes
To begin tracing the systemic failures through the TOR worksheet the group must decide on the prime (or main) error that caused or allowed the incident to happen. The TOR worksheet is centred on the management and supervisory factors in an operating system. It is necessary for the group to come to a consensus on this start point. An example of a prime error could be 'Failure to investigate and apply lessons learned from similar mishaps'.

Having identified the prime error, the leader circles the reference number on the trace guide within the work sheet and underlines all those numbers that are cross referenced by the prime error. These are known as possible contributing factors and are drawn from the original functional areas.

The group considers all the possible contributing factors and decides whether or not they were relevant to the particular incident being investigated. The group leader then circles the numbers on the trace guide of those possible contributing factors considered to be relevant and crosses out those that are not. The group then repeats this process for the factors cross referenced by those possible contributing factors considered relevant. This process continues until the trail is exhausted.

The circled factors represent the identified root causes to the particular incident.

Eliminate Insignificant Causes
Once the tracing process has been completed the group may be left with a list of ten or more root causes that were judged to have contributed to the incident. The group must now discuss these in more detail to reduce the list to a more manageable size by assessing the significance of the factors identified.

Identify Realistic Actions
When the problem areas have been identified and reviewed, the group must then identify realistic corrective actions that can be taken. If the group consists of employees from the shop floor not all the actions will be under their immediate control. It is for the group leader to raise the issues identified to more senior management through the appropriate organisational channels e.g. reporting forms, safety committees etc.

7.4 SYSTEMATIC ACCIDENT CAUSE ANALYSIS (SACA)

7.4.1 Overview

SACA was developed by Waldram (1988) for the analysis of accident statistics on offshore installations. It is recognised by Waldram that all accidents have multiple causes. He states that while these causes are of equal importance they are not equally removable. The SACA approach aims to analyse causes on a common basis and produce statistics as an aid to identifying areas for action.

Much emphasis is placed upon the Health and Safety at Work etc Act, 1974 (HSW) for providing the foundation upon which the system is based, firstly for its emphasis on 'reasonable practicability' and secondly for its requirement for organisations to have a statement of General Safety Policy and the Organisation and Arrangements to carry out that policy. By deriving the cause analysis framework from the duties specified in the HSW Act, Waldram argues that it should be relatively easy to allocate responsibility for corrective action, in terms of the Safety Policy Statement.

SACA identifies two types of failure which it is not reasonably practicable for the organisation to prevent, namely:

- failings by those for whom the line management is not responsible e.g. manufacturers, suppliers, members of the public
- failings by employees and contractors which fall within the range of 'normal' error rates.

7.4.2 Structure

SACA identifies four main categories of 'Universal' causes that can be applied to any work situation, these are; Persons directly involved (P), Equipment and Place of Work (E), Systems of Work (S), and Outside Local control (O). These four universal categories are then further divided into:

- Persons directly involved (P) is divided into four sub-categories:
  - P1, Skill / training / information inadequate
  - P2, Personal protective equipment inadequate
  - P3, 'Reasonable' failing
  - P4,'Unreasonable' failing
- Equipment and Place of Work (E) is divided into three sub-categories:
  - E1, Specification / design / layout inadequate
  - E2, Manufacture / construction inadequate
  - E3, Maintenance / operational inspection inadequate

- Systems of Work (S) is divided into three sub-categories:
  - S1, Job arrangements inadequate
  - S2, General systems inadequate
  - S3, Worksite inspection inadequate

and,

- Outside Local Control (O) is divided into four sub-categories:
  - O1, Company offsite procedures inadequate
  - O2, Failure by specialist supplier / contractor
  - O3, Failure by third party (no contractual relationship)
  - O4, Severe weather

In total 14 causes have been identified.

7.4.3 Conducting an Analysis

The aim of the analysis is to highlight the major causes contributing to an organisation's accidents. In the event of an incident, e.g. first aid injury, lost time injury or major disaster the assessor is required to tick all the relevant causes listed. When sufficient data has been gathered the results should be converted into percentages. The sub-category with the highest percentage therefore requires the most attention. The resulting table of values can be used to develop an action list.

7.5 SUMMARY

The comprehensiveness of the checklist methodologies varies greatly; from HPES which is heavily supported by documentation and provides feedback to all participating organisations through INPO, to SACA which does not really get down to the level of root causes and provides little justification for the categories that are presented.

Some of the categories presented in the checklists would appear to encourage rather than discourage blameseeking. For example, TOR includes 'work habits sloppy' and SACA cites 'unreasonable failing' under 'Persons Directly Involved'.

All the techniques except TOR can be conducted by individuals. TOR, like the Causal Tree Method (Section 6) is a group method requiring discussion and consensus among 'experts', that include those witnessing the incident. Again, the advantages of group techniques can be cited as team building, increasing awareness and ownership of actions.

At face value the checklists would appear to be very user friendly requiring analysts to simply tick categories in boxes, but this is at the expense of providing systematic methodologies to obtain and analyse information from the incident.

8.0 ROOT CAUSES ANALYSIS - OTHER METHODOLOGIES

8.1 INTRODUCTION

A number of other methodologies have been identified in literature reviews by other authors. In some instances no other information was forthcoming and in others the emphasis of the methodology did not appear to be strictly relevant to root cause analysis, which includes the full gamut of management and organisation al failures. A brief overview of these methodologies is described below.

8.2 AMERICAN INSTITUTE OF CHEMICAL ENGINEERS' REVIEW (AIChE)

In the book entitled 'Guidelines for Investigating Chemical Process Incidents', a variety of root causes analysis methods are described for application in the process industry. These are categorised into four groups, namely:

1. Deductive: - This approach involves reasoning from the general to the specific (e.g. Fault Tree Analysis (FTA), Management Oversignt Risk Tree (MORT), Causal Tree Method (CTM))
2. Inductive: - This approach involves reasoning from individual cases to general conclusions, providing an overview approach (e.g. Accident Anatomy Method, Action Error Analysis, Cause-Effect Logic Diagram, HAZOP Analysis)
3. Morphological: - This method is based upon the structure of the system being studied. Morphological approaches focus upon the potentially hazardous elements, concentrating primarily upon the factors having the most significant influence on safety (e.g. Accident Evolution and Barrier Technique and Work Safety Analysis)
4. Non-systems Oriented Techniques: - Concepts and techniques that are not as comprehensive as systems oriented techniques mentioned above (e.g. Change Analysis, Human Error Probability Study (HEPS), Multiple Events Sequencing (MES), Sequentially Timed Events Plotting (STEP), Systematic Cause Analysis Technique (SCAT), Technique of Operations Review (TOR), TapRooTtm, Human Reliability Analysis Event Tree Technique)

Many of these methods have already been discussed in this report and are therefore not described further here.

8.2.1 Accident Anatomy Method (AAM)

AAM was developed in the 1970s, at the Riso National Laboratory in Denmark and many of the basic concepts have been adapted from MORT. The technique involves developing a schematic diagram and applying a logic tree to the critical events. It is stated that either a generic tree can be used based upon historical data or a specific tree can be built based upon hypotheses of the incident.

The main difference between AAM and MORT is the representation of information. MORT is a strictly deductive technique, whereas AAM incorporates both inductive and deductive reasoning. The symbols used in the AAM tree are slightly different and more complex than those used in MORT.

This technique has only really been applied in Denmark and mostly on an exploratory basis. The development of the AAM trees has been reported as time consuming.

8.2.2 Action Error Analysis (AEA) Technique

AEA examines human performance and is intended to be used to determine potential problems with written instructions. Human actions to be carried out on the process plant are listed. These actions are then drawn as a sequence and the consequences of the action on the plant are identified. When the correct procedure has been modelled the effects of errors are then examined and added to the diagram.

8.2.3 Hazard and Operability (HAZOP) Analysis

The HAZOP technique was developed to identify operability problems during the design stage of a plant. It uses a structured, systematic brainstorming approach with an interdisciplinary team to identify problems resulting from deviations from the design intent. The identification of such deviations is prompted by guide words that are applied to all relevant variables.

Although not strictly an incident investigation technique, the principle of using a multidisciplinary group to undertake a structured brainstorming examination of a system has been adopted by TOR and CTM.

8.2.4 Accident Evolution and Barrier (AEB) Technique

This method was under development by the Swedish Nuclear Power Inspectorate at the time it was described in the AIChE book. Again this is a method that has been strongly influenced by the principles incorporated into the MORT technique.

However, it is specifically intended for investigating near-misses in the nuclear industry, focusing on the interactions between technical systems and human factors.

Two columns of empty rectangular boxes are presented on a worksheet, one column relating to human organisational systems and the other to technical component systems. This sheet is used to model the sequence of failures with arrows indicating the interactions. It is assumed that there are barrier functions that can arrest the sequence and prevent the unwanted development of an incident.

8.2.5 Work Safety Analysis (WSA)

WSA is essentially a method for systematic risk assessment. It is usually applied as a preventative technique rather than an incident investigation tool, although in the AIChE it is argued that the same methods could be applied to incident investigation.

8.2.6 Human Reliability Analysis (HRA) Event Tree Technique

This method has been designed to examine human errors. It is a graphic method of presenting human errors identified through task analysis. The resulting errors are entered as binary branches on the HRA event tree. The branches are arranged in chronological order. The technique requires analysts to be familiar with human factors issues.

8.3 HSYS

8.3.1 Overview

HSYS is described by Paradies et al (1993b) in their review of root causes methodologies. However, the full title of the technique is not given. This system was developed at the Idaho National Engineering Laboratory (INEL) for analysing human performance deficiencies in technologically complex operations.

Like MORT, HSYS is a generic model based on fault tree principles. However, instead of modelling safety management systems, HSYS models human performance. This diagrammatic representation of human performance runs to approximately 45 pages of tree diagrams and is supported by 72 pages of questions and 9 pages of definitions. At the time of the Paradies review this system was still under development as attempts were being made at simplification.

The tree is built upon a model of human performance consisting of five sequential components:

- Input decision
- Understanding of input meaning
- Action selection
- Action planning
- Action execution

The model assumes that all of these components are required for successful performance; thus failure is modelled by linking these components through an 'OR' gate. These components are decomposed hierarchically down to between 3 and 6 levels.

This technique is rather theoretical and cumbersome and has yet to be proved in practice.

8.4 CHECKLISTS

Other checklists have been published, similar to that described in Section 7.4, for example Senecal and Burke (1993), Wu and Hwang (1989) and Roig and Schneider (1994). These checklist approaches have been developed in order to collect statistical information on root causes and to design databases. Unfortunately, the categories do not appear to have been selected systematically, nor do they appear to be based on any particular principles of safety management. Indeed, frequently readers are encouraged to add their own categories to the lists as required.

The importance of collecting data to identify trends has been recognised by the majority of the systems discussed in this review. Nothing new is contributed by any of the papers referred to in this section.

8.5 ASSESSMENT OF SAFETY SIGNIFICANT EVENT TEAMS (ASSET)

8.5.1 Overview

ASSET is a methodology developed by the International Atomic Energy Authority (IAEA) for event analysis at nuclear power plants. It assumes that events (deviations, anomalies, incidents or accidents) occur as a consequence of a failure which, due to latent weakness (direct causes), could have been expected (IAEA, 1991).

The process is described by Fahlbruch in the book *After The Event - From Accident To Organisational Learning,* in which the technique is reviewed along with others in an attempt to create a hybrid method of problem solving.

8.5.2 Structure

The technique assumes that latent weakness were not detected and eliminated because of inadequacies in the plant surveillance programme concerning equipment, personnel and procedures (root causes). Thus, ASSET identifies the root cause of each event as a deficiency of the nuclear power plant surveillance programme. The approach, therefore, limits the variety of potential contributing factors and excludes for instance, extra-organisational aspects.

8.5.3 Conducting an Analysis

ASSET investigations are conducted by internationally composed teams of nuclear power experts who co-operate with local nuclear power plant personnel. ASSET missions are thorough and expensive, which limits their use for the analysis of a larger number of events, including 'smaller' ones. Their practicality is also confined due to the use of external experts. However, ASSET offers guidance and suggestions for the elimination of potential weaknesses and direct causes.

The comprehensiveness of the approach is guaranteed by procedures indicating 'basic elements' for the analysis of direct causes. Further, ASSET grants discretionary freedom to the analysts in offering only general hints and investigative proposals for the three basic elements: functional efficiency of equipment, personnel performance and the usability of procedures. Similarly, for the identification of root causes only general instructions and proposals for their elimination are given.

8.6 SAFETY THROUGH ORGANISATIONAL LEARNING (SOL)

8.6.1 Overview

The Research Centre of Systems Safety of the Berlin University of Technology in co-operation with TUV Rheinland has developed an event analysis approach which is based on axoims of the socio-technical systems approach (STSA) and theoretical assumptions about event genesis (Becker *et al.,* 1994). The process is aimed at the nuclear industry.

This review has been limited to reading an article written by one of the procedure developers. No further information on the technique appears to be available.

8.6.2 Structure

SOL proposes that event analysis always be conducted by a qualified team of nuclear power plant personnel composed of persons with different backgrounds and operative experience in order to minimise cognitive bias and perceptual blind spots. General guidelines have been developed to assist the analysis team by the provision of heuristic frameworks and instrumental aids encouraging them to exploit the expert knowledge and creativity of the team.

SOL favours a structured approach to the process of incident investigation over the pre-structured content of the analysis, i.e. the standard logic tree employed in TapRooT™. Hence, SOL depends to a greater extent on the expertise of the analysts.

8.6.3 Conducting an Analysis

SOL operationalises event analysis as a set of standardised process steps which start with the event and comprise a situational description, the identification of contributing factors, reports with descriptors for later statistical analysis and decisions on event identification and safeguarding measures.

The SOL procedure advocates the modelling of event sequences by using as much as possible of the conceptual representations and competencies of the analysis team. Guidance is provided to support this process. An identification aid for determining contributing factors was developed by deriving contributing factors from theory and collecting empirical data. The aid contains general questions related to possible contributing factors and has in-built links to direct the team to related questions. Examples are provided for each of the general questions to assist in stimulating the problem solving process. This is quite different from the more mechanical path through an error/failure tree like MORT or a checklist type approach such as HPES.

A set of 6 specific instruments are designed to aid the process of event analysis and to ensure its standardised conduct. These are:

Event Description
Guideline for Situational Description (1)

Identification Of Contributing Factors
Guideline For Sequence Of Event Analysis Steps (2)
Aid For Identification Of Contributing Factors (3)

Reporting
Guideline For Event Description (4)
Guideline For Event Reporting (5)
Guideline For Descriptors (6)

The technique has undergone preliminary validation and evaluation but is still in the early stages of use.

8.7 PROACT™

8.7.1 Overview

Reliability Center, Inc. was established in 1972 as a Research & Development arm of a major U.S. corporation. In 1985, RCI became an independent corporation under the direction of founder and president Charles J. Latino. PROACT™ software is an easy to use software package which aims to assist the incident investigator identify, analyse and recommend solutions for the root causes of the incident. All information reviewed was obtained from the vendors web site and from a review of a demonstration version of the software.

8.7.2 Structure

The software package is aimed at helping to store failure data, put a structured process to the investigation and analyse the failure data, communicate findings and recommendations and track corrective actions. A logic tree is developed to show the progression and causes of the incident. The tree starts with the end event, i.e. the incident, and works backwards.

The software package offers no guidance on who should carry out the analysis or how to identify causal factors or root causes, although the vendors offer a training course in the software.

8.7.3 Conducting An Analysis

All accident data would need to be gathered prior to using the software. Information on the failure is input into the package using a variety of screens for data recording, analysis, construction of a logic tree and tracking of actions.

The software is not intelligent and relies solely on the expertise of the analyst in the construction of the logic tree and the analysis of the information. It is however, very user friendly and presents the results of the analysis automatically in report form.

The company web site claims that numerous operators in various industries are using the software, from Eastman Chemicals to Shell and BP Exploration.

9.0 CONCLUSIONS

None of the techniques discussed adequately addresses every stage of the incident investigation process shown in Figure 3.1. A number of root causes 'procedures', or 'systems' have adopted a battery of techniques that can be applied at particular stages of the investigation. For example, HPIP, utilises up to six techniques, the selection of which will rely on the analyst's judgement of what is 'appropriate'. As a minimum, a method of schematically representing information concerning the incident sequence will be used prior to applying the root cause methodologies to 'significant' causal factors.

The majority of root causes analysis methodologies reviewed were essentially checklists of potential root cause factors to stimulate thought. These 'checklists' are presented in a number of forms:

- as trees incorporating fault tree logic, e.g. MORT,
- as simple trees without fault tree logic, e.g. SRP
- as lists with cross referencing systems e.g. SCAT and TOR
- as simple lists e.g. SACA.

The analyst must work systematically through the 'checklist' and judge firstly, whether the causal factors presented were applicable to the incident and secondly, for those that are found to be applicable, whether they were necessary and sufficient to be one of the contributory causes of the incident.

A variety of root cause analysis techniques have been discussed in this review and those from Sections 6 and 7 are compared against a range of criteria presented in Figure 9.1. (Those methods from Section 5 have not been included because they only identify direct causal factors rather than root cause factors. Methods outlined in Section 8 have been omitted either because there is insufficient information on the technique, or because the methods described are not considered to be true root causes analysis methodologies).

Based on this literature review it is apparent that there are three key components that need to be applied to ensure effective root causes analysis incident investigation, namely:

1. A method of describing and schematically representing the incident sequence and its contributing conditions.

2. A method of identifying the critical events and conditions in the incident sequence.

3. Based on the identification of the critical events or active failures, a method for systematically investigating the management and organisational factors that allowed the active failures to occur, i.e. a method for root causes analysis.

Underpinning these three components are the following premises:

- The barrier/energy transfer model of incident causation. This postulates that an incident can be likened to the transfer of energy and therefore for an incident to occur, there needs to be a person present, a source of energy and a failed barrier between the two.

- Incidents typically have more than one causal factor. Multiple causation models have been utilised throughout the texts reviewed and the methods frequently provide linkages between related factors.

Finally, in selecting or developing a root causes analysis method to apply, the analyst / organisation needs to consider whether the method specifically facilitates the identification of safety management and organisational inadequacies and oversights which relate to their own operations. The method needs to identify those factors that exert control over the design, development, maintenance and review of their risk control systems and procedures.

SYSTEM	1	2	3	4	5	6	7	8	9	10	11	12
MORT	Public	Nuclear	>20	Y	Y			Y	Y		Y	
SRP	Unknown	Nuclear	>5	Y	Y	Y	Y	Y	Y	Y	*	
TapRooT™	Proprietary	General	<5	Y	Y	Y	Y	Y	Y	Y	*	
HPIP	Unknown	Nuclear	<5	Y	Y			Y	Y			
HPES	Proprietary	Nuclear	>10	Y	Y			Y	Y	Y		
SCAT	Proprietary	General	>10	Y		Y	Y	Y	Y		#	
TOR	Proprietary	General	>20			Y	Y			Unknown	Y	
SACA	Public	Offshore	>5			Y	Y		Y			Y
CAUSAL TREE	Proprietary	Chemical	>15			Y	Y			Y		

KEY

1. Is the system publicly available?
2. What industries has the technique been applied in?
3 How many years has the technique been in existence?
4. Is it a structured methodology?
5. Is a schematic diagram drawn first?
6. Is this a stand alone technique (i.e. not part of a battery of different methods?
7. Can the method be summarised on 2 sides of A4?
8. Is there supporting documentation for analysts?
9. Can this method be applied by a single analyst?
10. Is the training requirement less than 2 days?
11. Is the emphasis on organisational arrangements rather then human performance?
12. Developed in the UK?

* covers management issues and equipment issues although there is a focus on human performance
# general management, although goes into detail on human performance issues

Figure 9.1: Comparison of Root Causes Analysis Techniques

10.0 REFERENCES

10.1 REFERENCES INCLUDED IN THE TEXT

* Indicates papers that have been cited in other references, but have not been read

American Institute of Chemical Engineers, Centre for Chemical Process Safety (AIChE), (1992), Guidelines for Investigating Chemical Process Incidents, New York, AIChE

Armstrong, ME, **(1989)**, *Human Factors in Incident Investigation*, in Proceedings of the Human Factors Society 33rd Annual Meeting, 1989, Human Factors Society

* Becker, G B. Wilpert, R. Miller, B. Fahlbruch, M. Fank, M. Freitag, HG. Giesa, S. Hoffman, Schleifer (1994), *Analysis and Causes of Human Failures In Nuclear Power Plants*, Der Bundesminster fuer Unwelt, Naturschultz und Reaktorsicherheit (BMU-1996-457), Bonn.

Benner, L Jr, **(1975)**, *Accident Investigations: Multilinear Events Sequencing Methods*, Journal of Safety Research, v7n2 , pp:67-73, Washington DC, USA

Bird, FE Jr and Germain, GL, **(1985)**, *Proactical Loss Control Leadership*, ILCI, Loganville, Georgia.

Dew John R, **(1991)**, *In search of the Root Cause*, Quality Progress, V23n.3, pp:97-102

Ferry TS, **(1988)**, *Modern Accident Investigation and Analysis*, (2nd Ed), New York, Wiley, ISBN 0471624810

***** Gibson JJ, **(1961)**, *Contribution of experimental psychology to formulation of problem of safety, Behavioural Approaches to Accident Research, Association for the Aid of Crippled Children*

***** Haddon W Jr, **(1966)**, *The Prevention of Accidents, Preventive Medicin*e, Little Borwn, Boston

***** Haddon W Jr, **(1973)**, *Emergency Damage and the Ten Counter-Measure Strategies*, Human Factors Journal, August

Hale, A. Wilpert, B. Freitag, M. (1997) *After The Event - From Accident To Organisational Learning*, Pergamon, ISBN 0080430740

Hallock RG & Weaver DA, **(1990)**, *Controlling Losses and Enhancing Management Systems with TOR Analysis*, Professional Safety Journal

***** Hendrick K and Benner L Jr, **(1987)**, *Investigating Accidents with S-T-E-P*, New York: Marcel Dekker

Johnson WG, **(1980)**, *MORT, Safety Assurances Systems*, New York, Marcel Dekker

***** Kepner CH & Tregor BB, **(1976)**, *The Rational Manager,* 2nd Ed, Princeton NJ, Kepner-Tregoe Inc.

Lewis EE, **(1987)**, *Introduction to Reliability Engineering*, Wiley & Sons

Paradies M, Busch D, **(1988)**, *Root Cause Analysis at Savannah River Plant*, IEEE Conference on Human Factors and Power Plants, pp:479-483

Paradies M, Unger L, Haas P, Terranova M, **(1993a)**, *Development of the NRC's Human Performance Investigation Process (HPIP), Summary*, Division of Systems Research Office of Nuclear Regulatory Research, NUREG/CR-5455, SI-92-101, Vol 1, Washington, USA, System Improvements Inc.

Paradies M, Unger L, Haas P, Terranova M, **(1993b)**, *Development of the NRC's Human Performance Investigation Process (HPIP), Investigators Manual*, Division of Systems Research Office of Nuclear Regulatory Commission, NUREG/CR-5455, SI-92-101, Vol 2, Washington, USA, System Improvements Inc.

Paradies M, Unger L, Haas P, Terranova M, **(1993c)**, *Development of the NRC's Human Performance Investigation Process (HPIP), Investigators Manual*, Division of Systems Research Office of Nuclear Regulatory Commission, NUREG/CR-5455, SI-92-101, Vol 3, Washington, USA, System Improvements Inc.

Roig RA & Schneider P, **(1994)**, *Audits and Root Cause Analysis*, Total Quality Environmental Management, V4nl, pp: 67-74, Wiley & Sons, Inc.

Senecal P & Burke E, **(1994)**, *Root Cause Analysis: What took us so long?*, Occupational Hazards V56n3, pp 63-65

Smith RG, *Implementation of the Human Performance Evaluation System at Virginia Power*, pp:475478, Virginia Power, Virginia, USA

Toft B & Turner BA, **(1987)** *The Schematic Report Analysis Diagram: a simple aid to learning from large-scale failures*, International CIS Journal v1n2, pp12-23,

Unger L, Paradies M, **(1992)**, *Using the TapRooT™ Incident Investigation System to Analyse Operator Mistakes in the Simulator*, 1992 SCS Eastern Simulation Multiconference, Sharon A, v24n4, pp:121-124, Orlando, Society for Computer Simulation, P.O. Box 17900, San Diego, USA

Waldram I, **(1988)**, *What Really Causes Accidents?*, The Safety Practitioner

***** Weaver, DA **(1973)**, *TOR Analysis: A Diagnostic Training Tool*, ASSE Journal, June, pp 24 - 29

Weaver, DA **(1987)**, *Technic of Operations Review TOR*, in Modern Accident Investigation and Analysis, ed. TS Ferry (1988), New York: Wiley

10.2 PAPERS REVIEWED BUT NOT MENTIONED IN THE TEXT

Benson TE, **(1992)**, *Industry Treats Root Causes*, Industry Week v241n11, pp: 28-29

Bishop J, LaRhette R, *Managing Human Performance - INPO's*, Human Performance Evaluation System, pp:471-474

Dunford N, *A Strategy for Plant Management to Prevent Loss - 7 Ways for Managers to Cut Incidents by up to 44%*, Loss Prevention Bulletin 093,

Kjellen U & Larsson TJ, **(1980)**, *Investigating Accidents and Reducing Risks - A Dynamic Approach*, Journal of Occupational Accidents v3 pp:129-140, Amsterdam, Scientific Publishing Company,

Knox NW and Eider EW, **(1983)**, *MORT User;s Manual for use with the Management Oversight and Risk Tree Analytical Logic Diagram*, DOE 76/45-4, SSDC-4 (rev 2), GG & G Idaho

Krause TR & Finley RM, **(1993)**, *Safety and Continuous Improvements - Two Sides of the Same Coin*, The Safety & Health Practitioner

Krause TR & Russel LR, **(1994)**, *The Behaviour-Based Approach to Proactive Accident Investigation, Professional Safety*, American Society of Safety Engineers v39,pp:22-26

Livingston A D and Green M (1992). *Evaluation of Incident Investigation Techniques and Associated Organisational Issues*. 7th International Symposium on Loss Prevention and Safety Promotion in The Process Industries. Taormina, Italy.

Paradies M, Unger L and Ramey-Smith A, **(1992)**, *Development and Testing of the NRC's Human Performance Investigation Process (HPIP)*, in International Conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety, Jan 15 - 17, Marriott Hotel (Airport), Orlando Florida, New York: American Institute of Chemical Engineers.

Pate-Cornell ME, **(1992)**, *Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organisational Factors*, Risk Analysis v13n2 pp:215-232,

Philley J, **(1992)**, *Investigate Incidents with MRC*, Hydrocarbon Processing Sept.92, pp: 77-81,

Tritsch S, **(1992)**, *Accident Investigations: How to Ask Why*, Safety & Health Dec 92

West Garmon Jr, Eckenrode RJ & Goodman PC, **(1991)**, *Investigation of Events Involving Human Performance*, Proceeding of the Human Factors Society 35th Annual Meeting - 1991, San Francisco, Human Factors Society Inc, Santa Monica CA, USA

Wu TM & Hwang SL, **(1989)**, *Maintenance Error Reduction Strategies in Nuclear Power Plants, Using Root Cause Analysis*, Applied Ergonomics, pp 115-121

10.3 REFERENCES NOT OBTAINED

Armstrong, ME, Cecil, WL and Taylor, K, **(1988)**, *Root Cause Analysis Handbook* DPSTOM - 81, EI du Pont de Nemours & Co, Savannah River Laboratory, Aiken SC29808

Boissieras J, **(1983)**, *Causal Tree. Description of the Method*, Princeton NJ, Rhone-Poulenc, US Contact : Corporate Director, CN5266

Cojazzi G **(1993)**, *Root Cause Analysis Methodologies. Selection Criteria and Preliminary Evaluation*, Commission of the European Communities, Tech. Note No I.93.93

Cojazzi G, Pedrali M, Cacciabue PC, **(1993)**, *Human Performance Study. Paradigms of Human Behaviour and Error Taxonomies*, Commission of the European Communities, Tech. Note No I.93.146

Rasmussen J, Duncan A and Leplat, **(1987)**, New Technology and Human Error, Wile

GLOSSARY

AEC	Atomic Energy Commission
ASSET	Assessment of Safety Significant Event Teams
CHAP	Critical Human Actions Profile
CTM	Causal Tree Method
E&CF	Events and Causal Factors Charts
HPES	Human Performance Evaluation System
HPIP	Human Performance Investigation Process
HSE	Health & Safety Executive
ILCI	International Loss Control Institute
INEL	Idaho National Engineering Laboratory
INPO	Institute of Nuclear Power Operations
LTA	Less Than Adequate
MCS	Minimal Cut Set
MES	Multiple Events Sequencing
MORT	Management Oversight and Risk Tree
NTSB	National Transportation Safety Board
REASON	Trade name for root cause software package
RoSPA	Royal Society for the Prevention of Accidents
SACA	Systematic Accident Cause Analysis
SCAT	Systematic Cause Analysis Technique
SORTM	Stimulus, Operation, Response, Team Performance, Management
SRP	Savannah River Plant Root Cause Analysis System
STEP	Sequentially Timed Events Plotting Procedure
TapRooT™	Trade name for a root cause software package
TOR	Technique of Operations Review Analysis
Incident	Throughout this report the term incident has been used to encompass both the principles of incident (near-miss) and accident.
Analyst	The term analyst has been used through the report to refer to the person conducting the root cause analysis.

Printed and published by the Health and Safety Executive
C1 02/01

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from
good booksellers

HEALTH AND SAFETY ENQUIRIES
HSE InfoLine
Tel: 08701 545500
or write to:
HSE Information Centre
Broad Lane
Sheffield S3 7HQ
Website: www.hse.gov.uk

CRR 325

£10.00

ISBN 0-7176-1966-4