Broad Lane, Sheffield, S3 7HQ
Telephone: +44 (0)114 289 2000
Facsimile: +44 (0)114 289 2500

HEALTH & SAFETY LABORATORY

REVIEW OF HAZARD IDENTIFICATION TECHNIQUES

HSL/2005/58

Project Leader: John Gould

Michael Glossop **MEng, PhD**
Agamemnon Ioannides **BEng, MSc**
John Gould **BSc**

HEALTH AND SAFETY LABORATORY
An agency of the Health and Safety Executive

Summary

Objectives

The objective of this project was to gain an overview of the hazard identification techniques commonly used at sites that will fall within the COMAH Regulations [COMAH 1999]. This has been achieved by:-

(i) Performing a comprehensive literature review of hazard identification techniques and summarising in a document.

(ii) Reviewing the relative strengths and shortcomings of current hazard identification techniques with a view to providing advice to CHID and identifying where further advice is required.

Main Findings

This report has provided a useful overview of the majority of the hazard identification techniques that will be found in COMAH reports and other high hazard industries. It has also given an indication of the applicability of each technique for SME's, offshore and nuclear facilities.

There are a wide range of hazard identification techniques available most of which have many examples published. In total, 40 techniques have been identified in this study. However with the notable exception of HAZOP there are few formal guidance documents on the application of such techniques. The most common method of learning to apply a technique is attendance at one of the many training courses or working with a more experienced colleague.

The lack of formal guidance is to be expected with a range of techniques that need to be very flexible to allow application to a wide range of circumstances without discouraging free thinking. The guidance available appears to concentrate on providing a description of the technique rather than setting any standards relating to the quality of its application.

Main Recommendations

(i) Feedback on this work should be sought from both industry and the regulators of experience gained from applying hazard analysis to satisfy the COMAH Regulations. This report should be updated to take into account any significant comments.

(ii) A small number of techniques that are most commonly used on COMAH installations should be reviewed in greater detail. This detailed review should provide guidance on the information required for COMAH reports and assessment criteria.

Contents

1 INTRODUCTION

The chemical and process industries have been using a variety of hazard identification techniques for many years, the most well known of which is HAZOP. Each technique has its own strengths and weaknesses for identifying hard (e.g. mechanical) and soft (e.g. computer controls) failures. Establishments that will be top tier sites under the forthcoming COMAH Regulations [COMAH 1999] are required to demonstrate that they have identified all the major hazards of their facilities and Inspectors will be expected to have some expertise in evaluating these techniques and identifying weaknesses. There has been little investigation into the effectiveness and evaluation of these different hazard identification techniques and guidance is required for both Inspectors and SME's.

1.1 Aim

The objective of this project is to gain an overview of the hazard identification techniques used at sites that will fall within the COMAH Regulations. This will be achieved by:-

(i) Performing a comprehensive literature review of hazard identification techniques and summarising them in a document.

(ii) Reviewing the relative strengths and shortcomings of current hazard identification techniques with a view to providing advice to CHID, and identifying where further advice is required.

This report examines various aspects of the hazard analysis. It covers the importance of choosing an appropriate hazard identification technique (section 2), how the review of the techniques was performed (section 3), details of the literature review (section 4), the phases of the process life cycle (section 5), summarises the hazard identification techniques (section 6), makes a comparison of the applicability of each techniques for various types of installation (section 7). The information provided in the report was then discussed (section 8), and a number of conclusions (section 9) and recommendations (section 10) were made.

2 BACKGROUND

Hazard analysis involves the identification of hazards at a facility and evaluating possible scenarios leading to unwanted consequences. The hazard analysis stage is a very important part of the risk management process, as no action can be made to avoid, or reduce, the effects of unidentified hazards. The hazard analysis stage also has the largest potential for error with little or no feedback of those errors.

Hazard analysis relies on a structured and systematic approach to identify potential hazards. There are a large number of techniques that can be used to perform this task at various stages during the life cycle of the process. These vary from a concept safety review, which is performed as early as possible in the concept stage of the process, to a HAZOP study which can be performed on a fully operational plant. As well as being performed at different stages during the life cycle of the process, the level of detail for the different techniques is significant. Concept safety review can only be used to provide insight in to the potential major hazards of the process, and hence steer the design of the plant to be more inherently safe. In contrast a HAZOP study is a systematic review of the process and should be able to identify the causes and consequences of deviations from the design intent.

It is important to choose the most appropriate identification technique, as this not only provides the appropriate level of detail, but can also be aimed at identifying hazards relating to specific areas. There are many factors to consider when choosing a technique. Many techniques have similar objectives and applied correctly should give comparable results. The hazard identification techniques are structured processes to identifying fault conditions that lead to hazards, and reduce the chance of missing hazardous events. They all require considerable experience and expertise.

3 METHODOLOGY

This review of the hazard identification techniques commonly used at major hazard sites is a desk top study with most of the information extracted from references after a literature review. There are already several references available that list hazard identification techniques [CCPS 1992, Eades 1998, Greenberg 1992, Lees 1980, Parry 1986, Stewart 1997, Wells 1996, Worsell 1994], however none of these are comprehensive, and many only provide a brief listing of methodologies. Considerable effort has been made to identify the original documents that describe each technique described here plus any reported experience of applying it.

The hazard identification techniques have been divided into four categories depending on the area in which they are predominantly applied:-

(i) Process hazards identification;

(ii) Hardware hazards identification;

(iii) Control hazards identification;

(iv) Human hazards identification.

The methodology for each of the hazard identification techniques is briefly described, preceded by a table summarising the phase of the project to which it is usually applied and the nature of the results, and ranking its applicability to COMAH installations and SME's, as well as a guide to the time and cost requirements of the technique. The resources required for each technique were ranked on a scale of 1 to 3, with one being quick and inexpensive and three being time consuming and expensive. The applicability of the techniques to SME's, COMAH, offshore and nuclear installations were ranked using a four point scale, with one not being applicable and four very applicable. Additional work comparing the various hazard identification techniques is given in section 8. Bullet points giving the advantages and disadvantages for each technique are provided at the end of each description.

Table 1, Abbreviations and acronyms used.

Abbreviation or acronym	Full title
HAZOP	Hazard and operability study
CHA	Concept hazard analysis
CSR	Concept safety review
PHA	Preliminary hazard analysis
FTA	Fault tree analysis
CCA	Cause-consequence analysis
Pre-HAZOP	Pre-hazard and operability study
FIHI	Functional integrated hazard identification
CEX	Critical examination of safety systems
MOSAR	Method organised systematic analysis of risk
GOFA	Goal oriented failure analysis
Inherent	Inherent hazard analysis
FMEA	Failure mode and effect analysis
Func. FMEA	Functional failure mode and effect analysis
FMECA	Failure modes, effects, and criticality analysis
MOp	Maintenance and operability study
Block diagram	Reliability block diagram
Structural	Structural reliability analysis
Vulnerability	Vulnerability assessment
CHAZOP	Computer hazard and operability study
Struc. english	Structured english
Spec. language	Specific language
SADT	Structured analysis and design techniques
State-transition	State-transition diagrams
GRAFCET	Graphe de commande etat-transition
HTA	Hierarchical task analysis
AEA	Action error analysis
Human rel.	Human reliability analysis
Pattern search	Pattern search method
PHEA	Predictive human error analysis

4 LITERATURE REVIEW

A literature review was carried out by HSE Information Services for references on hazard identification techniques. Over 1,000 relevant references were identified by the search. Additional references were taken from text books such as “Loss Prevention in the process Industries” [Lees 1996] and an earlier HSL project on machinery safety [Worsell 1994]. These sources of information were valuable in identifying the various techniques, but details of each technique were generally taken from specific references describing the development and application of the technique. In total, 40 techniques were identified. These are listed in Table 1 along with their commonly used acronyms/abbreviations.

Table 2 shows the specific references identified for each technique. Many of the references contain details of more than one of the techniques and where possible these reviews have not been used as a basis to describe the technique.

For some of the techniques there is a large supply of reference material to aid in their understanding and performance. Examples of these are HAZOP, fault tree analysis, safety audit, failure mode and effect analysis, CHAZOP, and task analysis. These techniques are all popular for identifying hazards, though are complex to perform to the appropriate standard, and have been used for a long time. The newer hazard identification technique, and the common techniques which are less complex (i.e. 'what if?' analysis, checklists), have less reference material available, and for checklists it mainly consists of lists of questions to be applied to various processes.

5 APPLICABILITY OF TECHNIQUES TO DIFFERENT PHASES OF A PROJECT

The cost of alterations to the plant, to produce an inherently safer process, corresponds to the stage in the process life cycle in which they are performed. Generally the earlier in the process life cycle the hazard is identified, the lower the cost of improving the safety of the process is, as it allows simple alterations to be performed before any of the items have been built. However, expense though is balanced with the inability of techniques performed early in the process life cycle to identify all the hazards associated with the process allowing the potential for hazards to be missed.

Hazard identification studies can be performed at seven stages during key stages in the life cycle of a new process (figure 1).

Not all of the hazard identification techniques are suitable for all stages in the life cycle. Some of the techniques may be suitable to more than one stage in the life cycle, but others have been specifically developed for one stage and it would be inappropriate to apply these in some of the other stages. Table 3 lists the reviewed hazard identification techniques and indicates their appropriateness for each of the seven stages.

To offset the various limitations of the techniques, two separate techniques can be incorporated. This often occurs for checklists and 'What if?' analysis. The checklist speeds up the normal 'What if?' technique which is used to bolster the checklist by identifying any missed hazards, and allowing it to be applied to new processes.

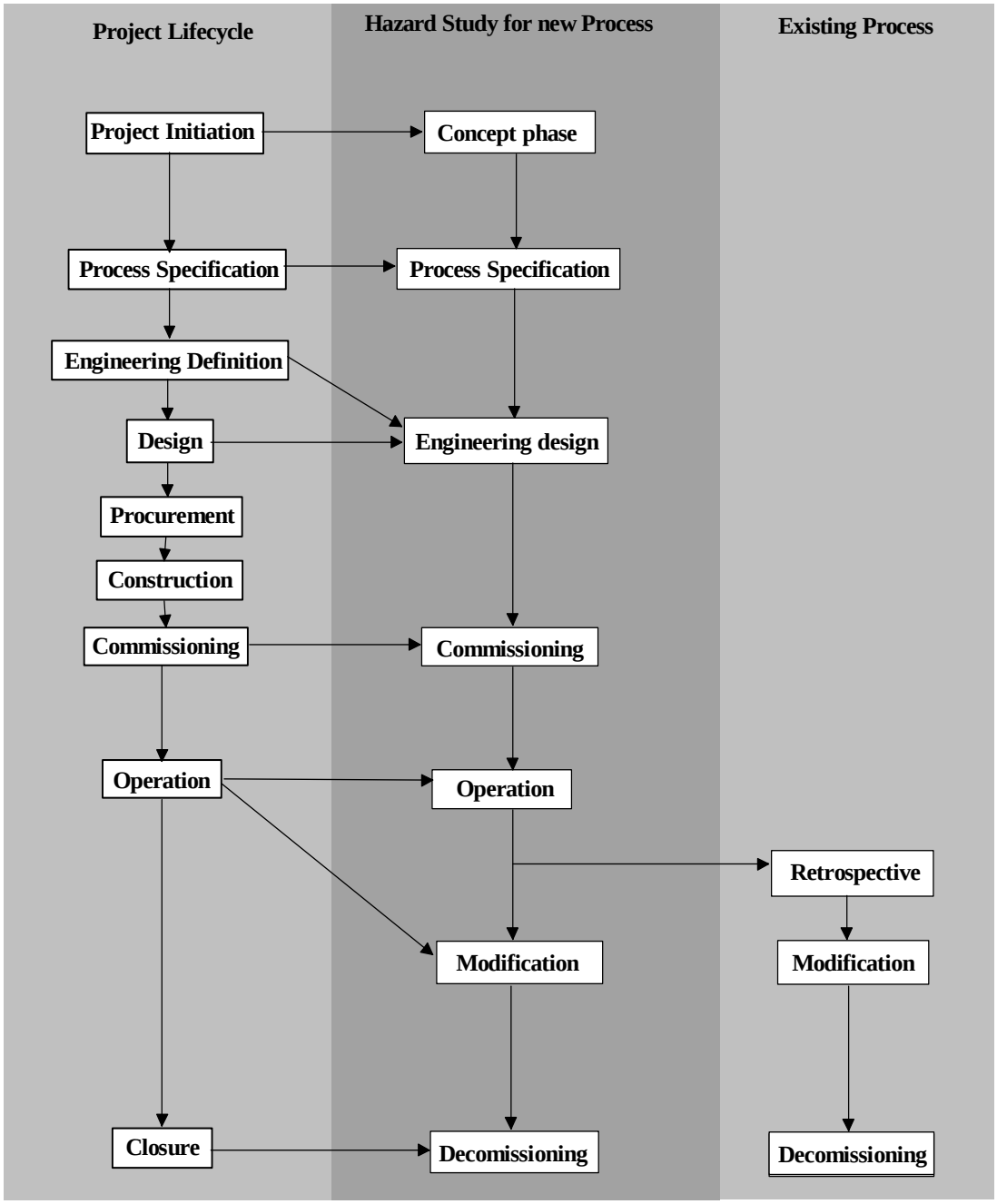

Figure 1, hazard identification in the process life cycle

Table 3, Suitability of techniques to phases of project

	Concept	Process	Design	Commissioning	Operation	Modification	Decommissioning
HAZOP	x	x	✓	✓	✓	✓	✓
What if	o	o	✓	✓	✓	✓	✓
CHA	✓	✓	o	x	x	x	x
Safety review	✓	o	x	x	x	x	x
PHA	✓	✓	o	x	x	x	o
FTA	o	o	✓	✓	✓	✓	✓
CCA	o	o	o	✓	✓	✓	✓
Pre-HAZOP	✓	✓	o	x	x	x	x
Standards	✓	o	o	o	o	o	o
FIHI	x	o	✓	✓	✓	✓	✓
Checklists	o	o	✓	✓	✓	✓	✓
CEX	x	x	✓	✓	✓	✓	✓
MOSAR	x	x	o	✓	✓	✓	✓
GOFA	x	x	o	✓	✓	✓	✓
Matrices	o	✓	✓	o	o	o	o
Inherent	o	✓	✓	o	o	o	o
Safety Audit	✓	✓	✓	✓	✓	✓	✓
FMEA	x	x	✓	✓	✓	✓	✓
Func. FMEA	x	x	✓	✓	✓	✓	✓
FMECA	x	x	✓	✓	✓	✓	✓
MOp	x	x	✓	✓	✓	✓	✓
Maintenance	x	x	✓	✓	✓	✓	✓
Sneak analysis	x	x	✓	✓	✓	✓	✓
Block diagram	x	x	✓	o	o	o	o
Structural	x	x	✓	o	o	o	o
Vulnerability	x	x	✓	o	o	o	o
DEFI	x	x	✓	o	o	o	o
CHAZOP	x	x	✓	✓	✓	✓	✓
Struc. english	x	✓	o	x	x	x	x
Spec. language	x	✓	o	x	x	x	x
SADT	x	✓	o	x	x	x	x
State-transition	x	✓	o	x	x	x	x
Petri-nets	x	✓	o	x	x	x	x
GRAFCET	x	✓	o	x	x	x	x
Task analysis	x	x	✓	✓	✓	✓	✓
HTA	x	x	✓	✓	✓	✓	✓
AEA	x	x	✓	✓	✓	✓	✓
Human rel.	x	x	✓	✓	✓	✓	✓
Pattern search	x	x	✓	✓	✓	✓	✓
PHEA	x	x	✓	✓	✓	✓	✓
✓ most suitable				o suitable			x not suitable

6 REVIEW OF TECHNIQUES

6.1 Process hazards identification

These methods are used to evaluate possible hazards due to mal-operations associated with the process, and to identify any potential hazards. The techniques predominantly deal with

hazards due to deviation from the normal operating conditions (e.g. temperature, pressure), and the presence of harmful materials.

6.1.1 HAZOP

Process phase the technique is used	Predominantly after the design phase, though can be earlier		
Applicability to COMAH sites	4	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	3

A hazard and operability study (HAZOP) [CIA 1993, Schlecter 1995] can be used at varying times during the life cycle of the process, from process development through to the closure of the plant, including hazard assessment of any modifications proposed during its operational life span. The degree of detail produced by the study increases as the process is developed, requiring P&I drawings, flow charts, process description, and for batch/semi-batch processes an operating guide, to produce the maximum detail.

The study is usually performed by 4-6 people led by a chairman with experience in performing safety studies. One of the other members is generally designated secretary and records all the finding of the group. The remainder of the group are usually comprised of additional specialists with specific knowledge of the process, engineering, and safety.

To produce a comprehensive evaluation of the process a number of guidewords (typically no/not/none, more, less, part of, reverse, other than, as well as) are combined with parameters (flow, pressure, temperature, reaction, level, composition) and systematically applied to each pipe and vessel of the process. The records produced by the study group should indicate:-

(i) The design intent of the pipe or vessel.

(ii) Any viable deviations from the intent.

(iii) Possible causes of the deviation.

(iv) Possible consequences of the deviation if it occurs.

(v) Additional action that can be performed to minimise the hazard associated with the deviation, if practicable.

Many companies have modified the guidewords and parameters they use during HAZOP to better define the process that is to be investigated. This is especially true in the nuclear industry where additional terms are required to evaluate the specific hazards due to radiation.

For batch/semi-batch processes, where the process is not at a steady state, a HAZOP should be performed at discrete time intervals during the operation of the process. The operating manual, as previously mentioned, is required to produce a complete assessment of the process.

Help is also now available through a number of computer packages that can aid in the performance of the HAZOP. These packages produce a similar layout for the results as the manual approach, and allow the whole team to see the minutes as they are produced in the meeting.

Advantages of HAZOP

- *Systematic and comprehensive technique. A detailed plan for performing the technique is available which systematically applies guide words and parameters to all the pipes and vessels in the process.*
- *Examines the consequences of the failure. Thought should be given by the assessment team to the consequences of the deviations identified. This aids in the production of recommendations for methods to minimise or mitigate the hazard.*

Disadvantages of HAZOP

- *Time consuming and expensive. Most plants contain a large number of pipes and vessels each of which need to be examined by the application of the various guidewords and parameters.*
- *Requires detailed design drawing to perform the full study. To fully perform the study the process has to be designed to such a level that all the pipes and vessels are detailed with their operating conditions, and control instrumentation.*
- *Additional guide words are required for unusual hazards. For specific dangers that will not be covered by the general guide words, further words (such as radiation for the nuclear industry) will need to be applied.*
- *Requires experienced practitioners. Experienced team members are required to identify all possible causes and consequences of the deviations, as well as producing realistic recommendations.*
- *Focuses on one-event causes of deviation only. Only the hazards associated with single deviations can be studied. Hazards that are caused by two or more separate deviations cannot be identified by the technique.*

6.1.2 'What if?' analysis

Process phase the technique is used	Any time during and after the design phase		
Applicability to COMAH sites	4	Nature of the results	Qualitative
Applicability to SMEs	3	Time and cost requirements	2

"What if?" analysis [Lees 1980, CCPS 1992] uses a creative brainstorming methodology, and can be used to evaluate any aspect of a process. For a simple project only 1 or 2 people are required, though with increasing complexity the group size will need to be increased. The examiners are all required to be experienced in performing such studies as it can be easy to miss hazards, and hence the evaluation would be incomplete.

The assessment asks a number of questions that begin with "What if" to attempt to identify any associated hazards. These answers can then be further developed by examining specific conditions i.e. "What if the raw material is the wrong concentration?" could be further developed by evaluating what would happen if the concentration was doubled.

Before the examination begins a certain level of process information is required. This includes a description of the process, the process drawings, and the operating procedure. If the review is to be performed on an existing plant then interviews with the operating staff can

be performed along with a site visit. A list of preliminary questions should be formed by one of the team members to act as an aid in the initiation of the review.

The results are often documented in a table format and will often contain the "What if" question asked, the hazard or consequence related to the question, safeguards present in the process at that time, and recommendations if applicable.

Advantages of 'What if?' analysis

- *Easy to apply. The principle behind the technique is simple and therefore can be easily applied to a process.*

Disadvantages of 'What if?' analysis

- *Experienced assessors are required or hazards can be missed. The principle is simple though experience is required to ask all the appropriate questions or hazards might be overlooked.*
- *Time consuming for complex processes. Complex processes will contain many items that are required to be assessed. Each one needs to have the appropriate questions applied to it and the results need to be recorded with associated hazards and consequences.*

6.1.3 Concept Hazard Analysis (CHA)

Process phase the technique is used	During the concept and early design phases		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

Concept hazard analysis [Wells 1993, Wells 1996] consists of a literature review of previous incidents, allowing identification of areas of the process of specific concern. It is performed during the concept and early design stages, and requires the process flow diagram, with any main add-on safety systems. Each plant section should be evaluated, with perceived dangers noted with suggested safeguard. The methodology is usually structured as :-

(i) Assemble a team.

(ii) Define the objectives and scope of the study.

(iii) Agree a set of keywords.

(iv) Partition each process flow diagram or block diagram into reasonably sized sections.

(v) Identify the dangerous disturbances and consequences generated by each word.

(vi) Determine if the hazard can be designed out, or the hazard characteristics reduced.

(vii) Determine any protections and safeguards.

(viii) Determine comments and safeguards.

(ix) Report the results and recommendations.

A preliminary study can also be performed before the more detailed evaluation, and is called a concept safety review (see section 6.1.3.1).

Advantages of CHA

- *Good basis for a more detailed study. The study is able to identify areas of concern that should be evaluated in greater detail later in the life cycle of the process when more detail is available.*
- *Aids in the production of a more inherently safe process. Hazards identified in the early concept stages can be easily evaluated, and either designed out or additional safety measures added.*

Disadvantages of CHA

- *Concentrates only on major hazards. Due to the minimal information available while performing this study only major hazards that are evident from the low level of detail can be identified and examined.*

6.1.3.1 Concept Safety Review

Process phase the technique is used	During the concept phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

A concept safety review [Wells 1993, Wells 1996] should be performed as soon as possible during the concept phase of the process. It should define the objectives and scope of the project, and identify the main hazards present (i.e. hazards associated with the chemicals present). The review should also establish all criteria that the plant must adhere to fulfill specific legislation.

Advantages of concept safety review

- *Good basis for further studies. This study identifies areas that require additional investigation early in the life cycle of the process to aid in the development of a more inherently safe plant.*
- *Aids in the production of a more inherently safe process. The identification of hazards early in the life cycle of the process allows either the hazard to be designed out, or the addition of extra safety measures.*

Disadvantages of concept safety review

- *Initial review identifying major hazards only. The technique is performed when only minimal information is available and only major hazards will be evident to the investigators.*

6.1.4 Preliminary Hazard Analysis (PHA)

Process phase the technique is used	During the early design phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

Preliminary hazard analysis [Wells 1993, Wells 1996, Ozag 1987] is used as an early means of hazard identification during the design and development of the process. The method is often used to follow-up on the hazards that have been identified during concept hazard analysis. It follows an approach similar to HAZOP, though splits the process into larger sections, generally major process items and associated lines and heat exchangers. The technique requires a minimum level of knowledge before it can be performed:-

(i) Notes on dangerous reactions and side reactions.

(ii) Data on hazardous materials.

(iii) A process flow diagram showing control measures and safeguards, or an initial P&ID.

(iv) Equipment specification sheets.

(v) Notes on inventory levels.

(vi) Any available operating information.

The assessment starts with the examination of 'dangerous disturbances of the plant', which include:-

(vii) Disturbances resulting in rupture or exceeding mechanical limits.

(viii) Critical defect in construction.

(ix) Flow through abnormal openings to the atmosphere.

(x) Adverse change in a planned product or other release.

The disturbance should be further developed until the immediate causes can be identified (e.g. human error, process item defect, design defect, control defect, change of design intent, or external threats). The study can then be widened to evaluate the consequence of the deviation, and to assign a potential risk to it.

Advantages of PHA

- *Facilitates the building of fault trees and event trees. The technique can be used to identify the events from which the fault trees and event trees can be developed.*
- *Systematically identifies the accident scenarios. A systematic plan is applied to the process to identify possible deviations leading to potential hazards.*
- *Easy to perform. Due to the systematic plan and the low level of detail available for its performance little expertise is required to apply the technique.*
- *Aids in the production of a more inherently safe process. Hazards identified in the early concept stages can be easily evaluated, and either designed out or additional safety measures added.*

Disadvantages of PHA

- *Will not identify all the causes. Due to the initial evaluation of the plant enough information might not be available to fully identify all the causes of the hazards.*
- *Will only identify and examine the major hazards. When the technique is generally applied only minimal information is available and so only major hazards can be identified.*

6.1.5 Fault Tree Analysis (FTA)

Process phase the technique is used	After the design phase is completed		
Applicability to COMAH sites	3	Nature of the results	Both
Applicability to SMEs	1	Time and cost requirements	3

Fault tree analysis [BS5760:7 1992, BS5760:2 1992, Vesely 1981, Ozag 1987] is a graphical representation of the combination of faults leading to a predefined undesired event. The methodology uses logic gates to show all credible paths from which the undesired event could occur. The fault tree is developed from the top down (i.e. from the undesired top event to the primary events which initiated the failure) and the logic gates indicate the passage of the fault logic up the tree. The event should be traced back until it cannot be developed further, either due to lack of knowledge or because no other causes can be identified.

The logic gates predominantly consist of AND and OR gates (or modified versions) to indicate if the preceding event requires either one or a number of failures to occur. Once the fault tree has been fully developed frequencies/probabilities can be designated to each primary event, and by following the logic in the diagram the risk associated with the top event can be calculated.

The assessment is usually completed in six stages :-

(i) Definition of the scope of the analysis. It defines the purpose and extent of the assessment, as well as the basic assumptions made.

(ii) Familiarisation with the design, functions, and operations of the process. The process should be described so that all of the members of the assessment team understand it.

(iii) Identification of the top event. An event appropriate to be assessed using the fault tree methodology should be identified, and is usually the onset or existence of a dangerous condition, or the inability of the system to provide the desired performance.

(iv) Construction of the fault tree. This consists of the breakdown of the top event to identify the primary events.

(v) Analysis of the fault tree. The addition of frequencies and probabilities into the fault tree for the primary events to quantify the risk of the top event.

(vi) Documentation of the results. This should include documentary evidence of all of the work performed by the assessment team, the information required for its performance, as well as the results produced by the team with any associated conclusions.

Advantages of FTA

- *It is able to produce quantitative results. Probabilities or frequencies can be allocated to the initiating conditions, and using the logic present in the developed tree the probability or frequency of the event can be calculated.*
- *Shows a logical representation of the sequence of events. A pictorial representation of the failure path is produced which indicates the logical sequence of events leading to realisation of the hazard.*
- *Can be used to assess a wide range of failures. Hardware, software, human, and process failures can all be easily incorporated into the logic of the process.*

Disadvantages of FTA

- *Time consuming and expensive for complex systems. Each event has to be broken down to its initiating conditions, values for these conditions are then required to be identified and the logic followed to quantify the hazard.*
- *An experienced assessment team is required or errors in the logic can be made. The connection between the initiating conditions are required to be properly identified or errors can occur in the logic and from that to the quantification of the hazard.*
- *Some top events might be missed. Time and effort is required to identify all the top events that are required to be studied. A preliminary study might need to be performed to fulfil this criteria, as this technique can not easily identify these events.*

6.1.6 Cause-Consequence Analysis (CCA)

Process phase the technique is used	After the design phase is completed		
Applicability to COMAH sites	3	Nature of the results	Both
Applicability to SMEs	1	Time and cost requirements	3

Cause-consequence analysis [Nielson 1975] combines the hazard identification and quantification methodology of fault tree analysis with event tree analysis. With the use of the event tree methodology cause-consequence analysis is able to investigate the incident past the hazard (e.g. item rupture) to the possible consequences (e.g. fire). The methodology is graphical, and once completed the consequences can be related back to their causes.

The technique is split into 6 stages :-

(i) Select the event or type of accident. Choose an event suitable for development as a top event in fault tree analysis, and as an initiating event in event tree analysis (e.g. loss of cooling).

(ii) Identify the safety functions that influence the course of the incident resulting from the event. Identify any safety functions that are available after the event has occurred, and how they can affect the outcome.

(iii) Develop the accident path resulting from the event (Event tree analysis). The accident paths are constructed based on the success or failure of the safety functions. A different symbol is used than that for event tree analysis and it contains a description of the safety function that can be answered by either yes or no, and produces two output relating to either outcome.

(iv) Develop the initiating event and the safety function failure event to determine their basic causes (Fault tree analysis). This follow the techniques used in fault tree analysis, and produces similar results.

(v) Evaluate the accident sequence minimal cut sets (the smallest group of events which can occur, in the appropriate sequence, for the top event to occur). This is used to replace the previously developed diagram produced for after the event, with a more fault tree like diagram so that the risk can be quantified. This is performed by connecting all the failures of the original diagram with the use of AND and OR gates.

(vi) Document the results. All the information used and results produced should be supplied along with a discussion of the consequences, evaluation of the significance of accident sequences, and any recommendation that were produced.

Advantages of CCA

- *Able to produce quantitative results. The probabilities or frequencies of the initiating events are used to quantify the consequences by applying the logic present in the diagram.*
- *Examines both the causes of the event and its consequences. The technique develops the logic backwards and forwards from the events to identify their causes and consequences.*
- *Can be used to assess a wide range of failures. Most causes for the hazard (i.e. human, process, hardware, and software) can be evaluated by the technique.*
- *Produces a logical representation of the sequence of events. Produces a graphical representation of the sequence of the logical stages leading to the event and on to the consequence.*

Disadvantages of CCA

- *Time consuming and expensive for complex systems. For complex processes there will be a large number of events to be studied. Each event must be fully investigated by the technique so that it can be quantified and the causes identified.*
- *An experienced assessment team is required or errors in the logic can be made. Experience is required to identify the appropriate relationship and logic between the causes, or errors can be made in the diagram producing errors in the quantification of the event.*
- *Initial events can be missed. Care must be taken to identify all the events associated with the process, if appropriate safeguards are not present some of the events can be missed.*

6.1.7 Pre-HAZOP

Process phase the technique is used	In the early design phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	1

Pre-HAZOP [CIA 1993] uses a top down approach, and is performed during the early design and development stages of the process where it would be impracticable to perform a full HAZOP study. The study team uses more wide ranging guide words to complete the study (such as fire, explosion/detonation) and evaluates the process to establish whether the terms are appropriate and if any redesign is required. This method is predominantly used to identify potential hazards as soon in the design and development phase of a process as possible so that safety precautions can be easily and relatively cheaply incorporated into the process.

Advantages of pre-HAZOP

- *Relatively quick. The technique uses broad guide words that can be quickly applied to the process. The low level of detail also minimises the number of items over which the guide words need to be applied.*
- *Aids in the production of a more inherently safe process. Hazards identified early in the design phase can be either designed out or mitigated through the addition of extra safety systems.*
- *Good basis for further studies. The technique identifies areas of the process that require additional study by more detailed hazard identification techniques.*

Disadvantages of pre-HAZOP

- *Is unable to identify all hazards. The use of the broad guide words allows more complex hazards to be missed.*
- *Concentrates on the major hazards only. Limited knowledge of the process when the technique is performed, and the wide ranging guide words applied means that only major hazards can be identified.*

6.1.8 Standards/Codes of practice/Literature review

Process phase the technique is used	During the concept phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	4	Time and cost requirements	1

These methods can be used to ensure that the design criteria meets the minimum safety requirements that have been identified for the process. Possible sources of such guidelines can be standards and codes of practice which have been produced by international/national legislation, or more stringent in-house requirements. In addition a literature review of previous related incidents can be performed to identify hazards that have occurred, and their failure route. This methodology is often incorporated into many of the hazard identification techniques which can be used early in the concept and design phase of the process.

Advantages of standards/codes of practice/literature review

- *They provide authoritative guidance on design criteria and possible hazards. The standards and codes of practices will provide minimum safety considerations for the process and recommended working practices.*
- *Can be used as a start to a more detailed technique. They can provide evidence of areas that require significant evaluation with more detailed techniques.*

Disadvantages of standards/codes of practice/literature review

- *Careful consideration is required to identify if they apply. There are a wide range of standards and codes of practice with many of them irrelevant to the process under consideration.*
- *Can be time consuming to understand. It can be time consuming reading and identifying information of use which then needs to be fully understood or errors can occur in their application.*
- *Often already incorporated into other techniques. Most techniques will incorporate this within the wider frame work of their assessment.*
- *Standards and codes of practice can change. Legislation can change with time and the retrofit of equipment to meet these new requirements can be time consuming and costly.*
- *Little help might be available for new processes. For new processes the appropriate standards might not be available to detail the minimal safety requirements*

6.1.9 Functional Integrated Hazard Identification (FIHI)

Process phase the technique is used	During and after the design phase		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

FIHI [Rasmussen 1997] requires a functional model of the system to be formally defined in terms of :-

(i) Intents. A single statement describing the purpose of the function.

(ii) Methods. A list of statements describing how the intent is to be satisfied.

(iii) Constraints. A list of statements describing any restrictions on how the intent can be achieved.

Any methods or constraints which contain additional intents should be further detailed in a similar fashion to fault-tree or hierarchical task analysis. HAZOP like guide words are then applied to each intent, and possible causes and consequences for each deviation are discussed, with records kept on a suitable record sheet.

Advantages of FIHI

- *Uses a functional approach which allows the assessment to be performed earlier in the process life cycle. The function of the various items are used as the basis for the technique allowing it to be performed before they are fully designed.*
- *Can be used to assess a wide range of failures. Due to its functional approach the cause of the failure (i.e. hardware, software, human or process) can be treated the same and so can be easily assessed.*

Disadvantages of FIHI

- *Time consuming. The process has to be split into suitable functional units, and the guide words have to be applied to all of them.*
- *Requires experienced practitioners. Experience is required to split the process into appropriate functional units and then to identify the hazards from the use of the guide words.*

6.1.10 Checklists

Process phase the technique is used	Any time during and after the design phase		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	4	Time and cost requirements	2

Checklists [Miller 1971, Balemans 1974] produce a detailed examination of the process plant by applying experience of everyday operations and previous incidents in similar plants. If an assessment of a process is to be performed with the aid of a checklist, it is believed that the use of a detailed list early on will minimise the inventiveness of the team members, and so only a coarse list should be used to aid in the direction of the work. Once the brainstorming has been completed the detailed checklist can then be used to identify areas that have been overlooked.

The main task for the assessment team is to identify the potential hazards of the process. Once a hazard has been identified, recommendations should be made of possible methods for it to be minimised. When the assessment has been completed a report should be produced, in co-operation with the people who have to perform the modifications, giving the alterations required as well as an appropriate timescale for completion.

There are a large number of checklists available to aid in hazard identification, and a list of sources is provided in Lees (1996). An example of an appropriate checklist for the chemical industry is reported by Balemans (1974).

Advantages of checklists

- *Easy to apply. The principle behind the technique is simple, compares a list of predefined questions to the process to aid in the identification of hazards.*
- *A simplistic assessment can be performed by inexperienced practitioners. Little experience is required to perform a simplistic assessment consisting of checking the list against existing conditions.*

Disadvantages of checklists

- *The assessment will only be as complete as the list used. The methodology will only ask questions stated in the checklist; if this is not comprehensive areas might be left unevaluated, leaving possible hazards unidentified.*
- *Not easy to apply to novel processes. A check list is generally formulated from past experience. For new plants there is no past experience limiting the information available for the preparation of an appropriate checklist.*

6.1.11 Critical Examination of System Safety (CEX)

Process phase the technique is used	During and after the design phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	3

CEX [Wells 1993, Wells 1996, Elliott 1968] was the precursor to HAZOP, and uses brainstorming techniques to formulate a series of questions (such as What, When, How and Where) which can be related to a particular activity or operation. The answers to these questions can then be further enhanced by the appropriate use of other questions (such as Why, Why then, Why that way, and Why there).

The methodology requires a statement for the design intent describing what is to be achieved. The significant aspects of the achievement can then be questioned to identify strengths and weaknesses. Alternatives can then be assessed if required to help minimise the associated hazards.

Advantages of CEX

- *Encourages innovation and inherent safety by design. If the technique is used early in the design phase then any major hazards identified could be either designed out or the risk reduced.*
- *Can be used as a start for more detailed techniques. The technique identifies events that can be carried on to fault tree and CCA, and can also identify areas requiring greater study later in the design phase.*

Disadvantages of CEX

- *Needs experienced practitioners. Experienced practitioners are required to formulate appropriate questions for the study.*
- *Hazards can be missed. If all appropriate questions are not asked then the associated hazards might be missed.*

6.1.12 Method Organised Systematic Analysis of Risk (MOSAR)

Process phase the technique is used	After the design phase		
Applicability to COMAH sites	2	Nature of the results	Both
Applicability to SMEs	1	Time and cost requirements	2

MOSAR [BSEN1050 1997] uses a series of steps to examine the safety of the process. The process is taken as a series of interacting subsystems, and tables are filled out by the members of the assessment team covering :-

(i) Hazard identification.

(ii) Adequacy of prevention.

(iii) Interdependency.

(iv) Operating safety study using FMEA or HAZOP.

(v) Logic trees.

(vi) Severity table.

(vii) Linking severity with protection objectives.

(viii) Technological barriers (no human intervention).

(ix) Utilisation barriers (with human intervention).

(x) Acceptability table for residual risk.

Advantages of MOSAR

- *Systematic risk analysis technique. The framework of the methodology systematically evaluates the process for hazards and then quantifies the associated risk.*
- *Will have the additional advantages applicable to the hazard identification technique applied to the process.*

Disadvantages of MOSAR

- *Time consuming. The technique incorporates time consuming hazard identification techniques as part of its methodology, and then the risk of the hazards identified needs to be calculated.*
- *Will have the additional disadvantages applicable to the hazard identification technique applied to the process.*

6.1.13 Goal Oriented Failure Analysis (GOFA)

Process phase the technique is used	After the design phase		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

(i) GOFA [Reeves 1989] uses a system analysis approach to develop a system diagram which is then used in the hazard identification process. It uses a top-down technique which is a hybrid of failure mode effect analysis and fault tree analysis. A number of steps are used in the evaluation :-

(ii) Define the failure goal.

(iii) Draw up and agree the system diagram.

(iv) Determine the fault modes for each component in each subsystem of the system diagram, using checklists for support.

(v) Choose a component for detailed study.

(vi) Choose a fault mode for this component.

(vii) Identify failure mechanisms for the chosen fault mode.

(viii) Choose a failure mechanism.

(ix) Identify the failure causes for this failure mechanism. These may be external to the systems diagram or internal if caused by the other components.

(x) Return to step 7 until complete.

(xi) Return to step 5 until complete.

(xii) Return to step 4 until complete.

Advantages of GOFA

- *Provides a practical approach to identifying the factors that can lead to the realisation of the hazard. It uses practical knowledge of the failure of equipment to identify the hazards.*
- *A wide range of causes can be evaluated. Process, hardware, software and human errors can all be evaluated by the technique.*

Disadvantages of GOFA

- *Time consuming. A large number of failure modes and process items are required to be investigated for a comprehensive assessment.*
- *Difficult to learn. The method performs a number of tasks which require experience practitioners in order to perform them properly.*
- *Scope of the application is limited to the failure goals considered. The technique will only assess hazards that occur from the failures considered, and so hazards might be missed if some of the failures are omitted.*

6.1.14 Matrices

Process phase the technique is used	The early design phase		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

During the early stages of process design and development, matrices [Clark 1997] can be used to identify potential hazards. The technique can be performed to varying levels of complexity, and cross-references a number of aspects of the plant. The most complex matrices can be used to identify interactions between :-

(i) The various chemicals present in the process. This should include all reactants, intermediates, and products. Any interaction between these chemicals should also be listed.

(ii) Materials of construction. This should be a list of all of the materials of construction used in the plant.

(iii) Operator. This is present to aid in the identification of specific hazards to the operator.

(iv) Utilities. This should be a list of all utilities used in the plant, and should also include possible cleaning solutions and lubricants.

(v) Energy source. This covers a wide range of sources, such as kinetic and potential energy, electrical energy, and radiation.

(vi) Air, land, and sea. This can be used to help identify the effects of the process on the environment and surrounding life.

Generally, using this technique produces a large, complex, matrix and care is required to ensure that all results are taken into consideration as well as that a proper recording method is used.

Advantages of matrices

- *Can be used as a start to more detailed techniques. The technique can identify hazards or areas that require further evaluation by a more detailed hazard identification technique.*

Disadvantages of matrices

- *Will only identify hazards due to the interaction of two components. The technique only examines what occurs when two components come into contact.*
- *Can miss some of the hazards of the process. Due to the limited information available, and to only examining the interaction between two components hazards can be missed.*
- *The presentation of the results in the matrix can be confusing, unless proper precautions are taken. For a complex process the size of the matrix produced can be extremely large, and unless proper precautions are taken can become confusing.*

6.1.15 Inherent Hazard Analysis

Process phase the technique is used	The early design phase		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

Inherent hazard analysis [Hawksley 1987] should be performed early in the design and development phase of the process. It is used to minimise the inherent danger of the process due predominantly to the presence of hazardous reactants, intermediates, or products. The process is initially divided into basic process items, and each item is evaluated with the help of a few basic questions :-

(i) Are there significant hazards associated with the unit?

(ii) Can the need for the unit be avoided?

(iii) Can less hazardous chemicals or subsidiary materials be used?

(iv) Can the hazardous inventory be reduced?

(v) Can the operation be carried out under more moderate conditions?

(vi) Can the hazardous inventory be contained chemically or physically?

(vii) Can the operation be carried out safer, more simply?

Any other consideration should then be reviewed that could aid in minimising the potential hazards.

Advantages of inherent hazard analysis

- *Can be used as a start to more detailed techniques. The methodology identifies hazards and areas that should be further evaluated by more detailed hazard identification techniques.*
- *Aids in the production of an inherently safer process. The identification of major hazards early in the design phase means they can be either designed out or additional safety measures added to produce an inherently safer process.*

Disadvantages of inherent hazard analysis

- *Can miss some of the process hazards. The limited information available when the assessment is being performed will mean that some of the hazards might be missed.*

6.2 Hardware hazards identification

Hardware tools have been classified as the techniques that predominantly evaluate the hazards due to failures in the process equipment. They assess the possible failures of the process plant items, and the knock-on effects for the rest of the process.

6.2.1 Safety audit

Process phase the technique is used	Any phase during the process life time		
Applicability to COMAH sites	4	Nature of the results	Qualitative
Applicability to SMEs	4	Time and cost requirements	3

A safety audit should subject all areas of a company to a critical examination to help minimise loss. It can be performed at a number of stages during the life cycle of a process [CIA 1970, CIA 1977, Williams 1971] :-

(i) Pre authorisation study.

(ii) In depth study. Carried out when the process package plan is complete.

(iii) Insurance study. Usually undertaken as soon as agreement of stage 2 has been reached.

(iv) Follow up studies. Carried out at regular intervals during construction.

(v) Pre start-up study. Carried out within one month of start-up.

(vi) Safety review. Carried out within six months of start-up and subsequently regular audits of defined areas and activities, which can also be performed for existing plants.

A safety review generally consists of an on-site walk-through inspection of the plant, and can vary from an informal routine function (which is primarily visual) to a formal in-depth

evaluation. The informal walk-through of the plant can be used to identify lapses in safety procedures, while the in-depth review should be used to ensure that the plant, as well as the operating and maintenance procedures, comply with the design intent and standards. The review should include interviews with employees working on the process plant (including operators, managers and maintenance workers), as well as applying additional techniques such as checklists and auditing areas such as :-

(vii) Management policy.

(viii) Attitudes training.

(ix) Features of both the process and design.

(x) Layout and construction of the plant.

(xi) Operating procedures.

(xii) Emergency plans.

(xiii) Personal protection standards.

(xiv) Accident records.

Once the review has been performed recommendations should be made of areas where action is needed, along with a justification and a completion date. A follow-up visit should then be performed to assess whether the recommendations have been performed to the required standard.

The technique can also be referred to as process safety review, design review, or loss prevention review.

Advantages of safety audits

- *The technique can be easily tailored to evaluate one specific area. The technique can be tailored to examine most areas of the plant from management and accounting to the plant itself.*
- *Parts of the review can be performed at regular intervals using inexperienced personnel. A cursory audit of the plant can be performed at regular intervals by inexperienced personnel and often comprises a walk through of the plant with a check list to identify hazards.*

Disadvantages of safety audits

- *Can be time consuming, and expensive. The safety audit often incorporates the use of other techniques to aid in the identification of hazards, and a large number of areas of the plant can be examined.*

6.2.2 Failure Mode and Effect Analysis (FMEA)

Process phase the technique is used	Once the design phase has been completed		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	3

The purpose of FMEA is to identify potential hazards associated with a process by investigating the failure modes for each process item. FMEA has difficulty in identifying hazards that require the failure of more than one process item, due to the complex interaction of the failures. The following steps [BS5760:5 1992] are performed during the analysis :-

(i) Describe the system. A detailed description of the process is initially required so that it can be broken down into either a functional, hierarchical or reliability block diagram. The assessment team also needs a detailed description of the various actions performed by each section, including a description of their modes of success or failure.

(ii) Establish the basic principles and purposes of the study. The purpose and scope of the assessment needs to be stated, along with how the results will be displayed, and whether there will be any interaction between the results and any further studies to be performed.

(iii) Carry out the study. Initially all items should be identified in the various systems or subsystems produced by the graphical breakdown of the process. All the possible failure modes of these items should then be collated. The most likely failures caused by the failure modes can then be identified, and their effects on the process evaluated.

(iv) Report the results. The report should include the diagram produced in stage 1, a detailed record of the analysis, a summary, recommendations indicating possible improvements, failures which have significant effect on the process, as well as those that produce none.

Advantages of FMEA

- *Performs a systematic review of the process. A detailed methodology is available to assess the plant item by item.*

Disadvantages of FMEA

- *Can be time consuming and expensive. For complex processes there will be many items to be investigated each with a complex series of failure modes to be examined.*
- *Difficulty identifying hazards due to more than one failure. It is hard to combine the effect of multiple failure modes of different items to identify combined hazards.*
- *Difficulty finding all the failure modes. Most items have been investigated to identify their various failure modes, newer equipment might be less well documented and some of the failure modes might have been missed.*
- *Requires a large amount of data. The plant needs to be well developed before the technique can be performed, and the various failure rates for each item also needs to be known.*

6.2.3 Functional FMEA

Process phase the technique is used	Once the design phase has been completed		
Applicability to COMAH sites	3	Nature of the results	Qualitative

Applicability to SMEs	2	Time and cost requirements	3

Functional FMEA uses the FMEA methodology [BS5760:5 1992], and breaks down the process into a functional diagram instead of either hierarchical or block reliability diagrams. All possible failure modes for these functions are then analysed along with possible causes and consequences (as with FMEA). A discussion of possible recovery mechanisms may also be included, and should be recorded in a suitable table.

Because a functional approach has been adopted, all aspects of the design can be examined with no distinction made between whether the function is implemented by hardware, software or human action. This is particularly helpful as informed decisions on how to implement each function can be made with a better understanding of the associated hazards.

Advantages of functional FMEA

- *Performs a systematic review of the process. A detailed methodology is available to assess the plant item by item.*
- *A wide range of errors can be evaluated. The technique only examines the function of the plant, and so process, hardware, software and human errors can be evaluated.*

Disadvantages of functional FMEA

- *Can be time consuming and expensive. For complex processes there will be many items to be investigated each with a complex series of failure modes to be examined.*
- *Difficulty identifying hazards due to more than one failure. It is hard to combine the effect of multiple failure modes of items to identify combined hazards.*
- *Difficulty finding all the failure modes. Most items have been investigated to identify their various failure modes, newer equipment might be less well documented and some of the failure modes might have been missed.*
- *Requires a large amount of data. The plant needs to be well developed before the technique can be performed, and the various failure rates for each item is also needs to be known.*

6.2.4 Failure Modes, Effects, and Criticality Analysis (FMECA)

Process phase the technique is used	Once the design phase has been completed		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	3

FMECA also uses the same methodology as FMEA though two additional steps are required to be performed [BS5760:5 1992, BS5760:2 1992] :-

(i) Determine the severity of the effect caused by the failure. The severity of the failure is generally classified as being in the range of; complete loss of capability with loss of life, to negligible effect on success with no injuries.

(ii) Evaluate the frequency of the effect caused by the failure. The easiest method for evaluating the event frequency is to examine previous data for similar processes to that under

consideration, operating at similar conditions. If no appropriate data is available then additional factors can be used to convert frequencies from unrelated processes.

Once the appropriate data has been compiled, the severity and frequency of the event caused by the failure can be compared producing a criticality rating. The most critical failures would cause an event that produced very severe results very often, while the least critical would produce negligible results very infrequently.

Advantages of FMECA

- *Performs a systematic review of the process. A detailed methodology is available to assess the plant item by item.*
- *A wide range of errors can be evaluated. If the technique applies a functional approach towards the plant process, hardware, software and human errors can be evaluated.*
- *It semi-quantifies the hazards by ranking them with respect to their frequency and effect. A criticality ranking is placed on all the hazards identified to indicate where additional safety measures are required.*

Disadvantages of FMECA

- *Can be time consuming, and expensive. For complex processes there will be many items to be investigated each with a complex series of failure modes to be examined.*
- *Difficulty identifying hazards due to more than one failure. It is hard to combine the effect of multiple failure modes of items to identify combined hazards.*
- *Difficulty finding all the failure modes. Most items have been investigated to identify their various failure modes, newer equipment might be less well documented and some of the failure modes might have been missed.*
- *Requires a large amount of data. The plant needs to be well developed before the technique can be performed, and the various failure rates for each item also needs to be known.*

6.2.5 Maintenance and Operability study (MOp)

Process phase the technique is used	Early stages of the design phase		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	3

A MOp study [Chastain 1997] is performed during the early stages of the design, and requires a team composition similar to that for HAZOP studies. A suitable team might consist of a leader, engineer, operator (if a similar plant is in operation), mechanic and technical scribe, with additional members depending on the process under evaluation. Initially the P&ID is split into a number of sections consisting of separate process items. The intent of each section is then fully defined to the satisfaction of the team present, and the P&ID altered if any changes or errors are identified. The leader then asks a list of questions for each process item such as :-

(i) Can the equipment be properly isolated for maintenance?

(ii) Can the equipment be properly drained for maintenance?

(iii) Are there plans to deal with mechanical failure of equipment?

(iv) Are there plans for critical spare parts to be available?

There are a number of other general questions that are asked, as well as those that are item specific. From these questions, areas that require additional thought to minimise hazards are identified, and recommendations can be made.

Advantages of MOp

- *Investigates the hazards related to the maintenance of plant items. The technique can be used to identify hazards, or poor design leading to hazards, during the maintenance of the various plant items.*

Disadvantages of MOp

- *Can only be applied to maintenance. The technique cannot be used on other areas of the plant except for maintenance procedures.*
- *Experienced practitioners are required. Experience is required to identify the appropriate questions to be asked of the plant items.*

6.2.6 Maintenance Analysis

Process phase the technique is used	Once the design phase has been completed		
Applicability to COMAH sites	3	Nature of the results	Both
Applicability to SMEs	2	Time and cost requirements	3

Maintenance analysis [Worsell 1994] is usually used to identify equipment availability, and can also be used to identify particular hazards associated with maintenance. A number of questions are asked of each piece of equipment, such as :-

(i) What failure can occur?

(ii) How a fault would be identified/detected?

(iii) How the underlying failure could be diagnosed?

(iv) What preparations are required for repair?

(v) What resources are required for repair?

(vi) How the failed part should be removed, repaired if possible, and replaced?

(vii) What checks are required after maintenance?

(viii) How normal operations should be restored?

The review can identify failures in maintenance procedure, and also if additional backups are required to minimise any hazards identified.

Advantages of maintenance analysis

- *Problems with maintenance are examined systematically. Each piece of equipment is examined to identify the potential hazards due to maintenance or availability.*
- *Can produce frequencies as well as identify hazards. Frequencies of maintenance or availability can be identified by the process.*

Disadvantages of maintenance analysis

- *Can be time consuming and expensive. Most plants have a large number of pieces of equipment which can be examined by the technique.*
- *Requires personnel experienced in the procedure. Experience is required to know the appropriate questions that should be asked for the various pieces of equipment.*

6.2.7 Sneak Analysis

Process phase the technique is used	Once the design phase has been completed		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

Sneak analysis was first developed in the aerospace industry to identify why spacecraft rockets would accidentally fire, or not fire when required. It is split into a number of separate paths for error [Whetton 1993, Whetton 1994] :-

(i) Sneak flow. The unintended flow of material, energy or information from one area to another. This is often due to either human error, performing tasks in the wrong order, or the failure of equipment. The sneak flow of material through utility lines (such as drains) is common.

(ii) Sneak indication. This is when the indicators for the processes condition are wrong or ambiguous. This can occur if an indicator is taken to read a value at one point, though in fact is linked to a slightly different area in the system, and indicates a wrong value only during certain mal-operations.

(iii) Sneak label. Due to either wrong or ambiguous labelling of indicators, chemicals, or other equipment. This can lead to the wrong conditions being applied to the process, or the wrong material being added.

(iv) Sneak energy. Unintended presence or absence of energy. This is often due to the presence of unreacted materials in the process, and can be caused by agitation failure, or the formation of layering in batch reactors.

(v) Sneak reaction. Unintended reaction. This can be due to unanticipated changes in the process conditions, or the presence of a material in the process that could catalyse the reaction.

(vi) Sneak procedure or sequence. The occurrence of events in either an unintended or conflicting order. This often occurs when no procedure is available for the operators to

follow, and they perform the task to the best of their ability. Information can also be lost, or misunderstood, during shift changes leading to possible hazards.

The identification of sneak flows can be performed by one of two methods. The first is by the addition of coloured lines onto a P&ID to indicate possible sneak paths, and once this has been completed the additional lines can be evaluated to identify if, and how, a sneak path could occur. The second method is by the use of a tree diagram, which produces a clearer assessment.

Tracing the possible sneak flows is performed by choosing each material present in the process (including utilities) and (by assuming all the pumps are turned on and all the valves are open) identifying all their possible flows through the process and where they can go. The process should then be checked for any incompatible substances coming together, and then if the associated flow paths are practical. A table is also produced indicating all the different valve and pump settings during the various operations of the process (this is of special interest in batch/semi-batch processes where the valve and pump settings can alter regularly). The table can then be assessed by assuming one valve is set in the wrong condition, and evaluating the hazards produced.

Identification of the other sneak paths is generally performed by the use of check lists, which are often called sneak clue lists. These aid in the identification of the sneak paths by specifying possible causes that can then be checked to see if they can occur.

Advantages of sneak analysis

- *Systematic evaluation of the process. A well defined methodology is available which can be applied to all parts of the plant in a systematic order.*

Disadvantages of sneak analysis

- *Requires experienced personnel to perform the review. Experience is required to aid in the identification of possible sneak paths.*
- *Time consuming and expensive for complex systems. For complex plants there will be many plant items increasing the number of possible sneak paths that are required to be examined.*

6.2.8 Reliability Block Diagram

Process phase the technique is used	Early process design		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

A reliability block diagram is a pictorial representation of the reliability of a process. It is used to indicate the required functioning components for the process to perform, and is applied primarily to systems without repair, and where the order of failure does not matter. For this technique it is assumed that there are only two possible states for each component, operational or faulty.

To successfully apply the technique [BS5760:9 1992, BS5760:2 1992] the operation of the process is required to be described in detail. There should also be statements concerning :-

(i) Functions to be performed.

(ii) Performance parameters and possible limits.

(iii) Environmental and operating conditions.

The process is then divided into blocks, which can be further divided into separate reliability block diagrams if required. Each block should be, where possible, independent of the other blocks, and contain no redundancy. The system definition is then used to organise the block diagram, where the output of one block is used as the input to the next. If there is no redundancy present, the reliability block diagram drawn will be linear indicating that the failure in any of the blocks will cause the entire process to fail. If redundancy is present within the process then where it is present blocks can be drawn in parallel, indicating that with the failure of one of these blocks a path for the process to work is still available.

Advantages of reliability block diagrams

- *Often used as a starting point for other techniques. Can be used to identify areas where reliability is of concern and should be further evaluated by a more detailed technique.*
- *Can identify where redundancy is required. It specifically examines the plant to identify where inbuilt redundancy would aid in safety.*

Disadvantages of reliability block diagrams

- *Trivial except for complex systems. The technique will be of little use on simple systems were only a small number of functions are performed.*
- *Limited to investigating reliability. The technique can not be easily applied to identify hazards that are not associated with reliability.*

6.2.9 Structural Reliability Analysis

Process phase the technique is used	Once the process design has been completed		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

The method [Worsell 1994] examines the structures associated with the process to identify their in-built safety margins. It can also be used to assess the effect of a partial failure on the overall structure, and the process.

Advantages of structural reliability analysis

- *Identifies hazards relating to the infrastructure. The technique is used solely to identify potential hazards related to the failure of the infrastructure of the plant.*

Disadvantages of structural reliability analysis

- *The study is only applicable to buildings and structures. The technique cannot be applied to identify hazards in other areas of the plant.*

6.2.10 Vulnerability Assessment

Process phase the technique is used	Once the design and layout has been completed		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

The vulnerability assessment [Socha 1996] is used to evaluate the safety of plant items if a failure occurs in a nearby item. Initially the location of all plant items need to be identified. This is usually performed by placing a 3D grid over the layout of the plant, and specifying a grid co-ordinate for all of the process items, providing an indication of the distances between items. The possible hazards of the various process items need to be identified, along with their effect on the other process items (e.g. debris, heat). The hazard is significant if it can directly impinge on the required safety systems needed for its mitigation, or will cause a secondary hazard in adjacent items.

Advantages of vulnerability assessments

- *Investigates secondary hazards to the process. The technique does not evaluate the hazards due to failure of equipment but evaluates the additional hazards caused once the incident (e.g. explosion) has occurred.*

Disadvantages of vulnerability assessments

- *Requires knowledge of the consequences of incidents. The area of effect and consequences of the initial incident are required to be known to identify how it impinges on the remainder of the plant.*

6.2.11 DEFI method

Process phase the technique is used	Once hardware has been built		
Applicability to COMAH sites	1	Nature of the results	Quantitative
Applicability to SMEs	1	Time and cost requirements	2

This method [Worsell 1994] is used to evaluate the possible failures relating to a piece of equipment. It is often use in the computer industry to test prototype hardware as it is developed. A computer is used to send failure inputs to the piece of equipment, and the consequence and failure rates can be calculated.

Advantages of DEFI

- *Can be used to examine equipment before it is fitted to the plant. The technique is usually applied to prototypes to aid in assessing its reliability and identifying possible failure modes which can be used in other hazard identification techniques.*
- *Produces frequencies for failure. Due to the significant testing regime that the equipment undergoes, failure frequencies can be identified.*

Disadvantages of DEFI

- *It is more applicable to assessing reliability than hazard identification. The technique is geared to the identification of reliability and failure frequencies and these values can be incorporated into other hazard identification techniques.*

- *Hardware needs to be constructed before testing can be performed. The hardware needs to be available as either a prototype or a production model for the technique to be performed.*

6.3 Control hazards identification

The increased use of computers within safety systems allows for significant hazards to occur due to their mal-operation. Computers have the additional problem that many of their operations share the use of the same component, hence if this component fails all the operations routed through it will also fail, producing Common Mode Failures. Software tools are applied to control systems and critical applications to identify hazards.

A number of techniques described elsewhere can be used to identify the hazards associated with the failure of the software, these are FMEA, checklists, 'What if?' analysis, and fault tree analysis. There are a number of additional techniques that are specific to identifying hazards in computer systems. These are still mainly in their development stage and are still subject to improvements, and are described below.

6.3.1 Computer HAZOP (CHAZOP)

Process phase the technique is used	Once the software design is completed		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	3

CHAZOP [Andow 1991, Lear 1993, Kletz 1995] is based on the methodology used in HAZOP studies. As with HAZOP it can be performed at a number of stages in the process development, and is split into two formats which can be performed in conjunction with the appropriate stage of HAZOP.The preliminary study is used to define critical features early in the design, and consists of :-

(i) Proposals on the system architecture.

(ii) A review of safety related features.

(iii) Review of performance after system failure.

(iv) Review of performance after utilities failure.

The full study goes through the programmable electronic systems building up a detailed view of how the system is intended to work, and what will happen if they fail. A number of areas are considered :-

(v) Random failure in the computer system environment. For each failure the following should be considered: what should happen, will the operator know, what should he do, and if there are any changes needed.

(vi) Input / output signals. For each signal it should be identified where it is used for a safety related function, and then a number of guide words (such as low signal, high signal, invariant signal, drifting signal, bad signal) should be applied. The questions does it matter,

will the operator know, is there any action required by the operator or other systems, and any modifications required, should also be asked.

(vii) Complex control schemes. For each scheme its function and method of operation should be given. The schemes should then be systematically reviewed for signals used, operator access, limits applied, interaction, controller tuning, relationships, performance monitoring, actions on a process mal-operation, protection against unauthorised changes, safety functions, and other ideas identified by the assessment group.

(viii) Batch systems. All the same points as for complex control systems should be considered, though they should be performed at each stage of the batch process.

(ix) Protective systems. Again the same points as for complex control systems should be used where applicable.

As with HAZOP, the assessment team should record all the hazards identified by the technique, and provide recommendation for possible improvement.

Advantages of CHAZOP

- *Methodical study of errors within the software. Systematically applies a set of guide words to the software and process control systems.*

Disadvantages of CHAZOP

- *Can be expensive and time consuming. For a complex process there will be a large number of computer systems that need to be evaluated.*
- *Can only be applied to software and control systems. The technique is specifically designed to identify hazards in computer systems, and cannot be easily applied outside this area.*

6.3.2 Structured methods

Structured methods [PSLP Mod 9 1998] are predominantly used to identify the appropriate software structure that needs to be developed, and should be performed early in the design and development phase of the process.

6.3..2.1 Structured english

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

Structured english is mainly used to expand ideas and functions from vague generalities, to precise statements in a hierarchical fashion. The method is given in terms of a set of logical conditions. Each function of the computer control system is written up as a restricted set of nouns and verbs, but in a format of the user's own design, which resembles a computer program.

The technique begins by stating the purpose of the instrumentation system and then proceeds to define what equipment that is to be used and how often the process needs to be performed. Once this is done, the process is then described indicating how to achieve the control system's objectives.

Advantages of structured english

- *Helps to produce an inherently safer control system. The technique identifies hazards early in the design phase allowing alterations in the system architecture so that they can be either removed or minimised.*

Disadvantages of structured english

- *Can only be applied to the computer system. The methodology is geared towards examining software and cannot be readily used to identify hazards in other areas of the process.*
- *Can only identify major hazards. The technique is performed before the computer architecture is fully developed and the limited information available means that only major hazards can be identified.*

6.3.2.2 Specification language

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

This method is similar to that of Structured english and incorporates a graphical format known as "requirements net" (network), and uses more restrictive verbs and nouns. The requirements net diagram is constructed first to show the flow of data and actions through the control system, and various symbols are used to indicate alternate paths and events taking place.

This type of method includes tools for checking the specification for completeness, consistency, and such tasks as compiling a data dictionary.

Advantages of specific language

- *Helps to produce an inherently safer control system. The technique identifies hazards early in the design phase allowing alterations in the system architecture so they can be either removed or minimised.*

Disadvantages of specific language

- *Can only be applied to the computer system. The methodology is geared towards examining software and cannot be readily used to identify hazards in other areas of the process.*
- *Can only identify major hazards. The technique is performed before the computer architecture is fully developed and the limited information available means that only major hazards can be identified.*

6.3.2.3 Structured Analysis and Design Techniques (SADT)

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

SADTs are another way of expressing the activities of a control system by the use of diagrams that resemble conventional engineering blocks. The technique incorporates a graphical language and a set of methods and management guidelines [Fairley 1985]. The SADT model consists of an ordered set of diagrams, which themselves contain 3-6 nodes with their respective arcs. There are two basic types of diagram :-

(i) Activity diagram. The nodes specify activities, while the arcs specify data flow between the activities. The arcs denote control data, input data and processor leading into the node, and output data leading out.

(ii) Data diagram. The nodes specify data objects and the arcs activities. The arcs denote control activity, generating activity and storage devise leading into the node, and using activity leading out.

The technique uses a top-down technique to breakdown high level nodes into further diagrams.

Advantages of SADT

- *Helps to produce an inherently safer control system. The technique identifies hazards early in the design phase allowing alterations in the system architecture so that they can be either removed or minimised.*
- *Produces easily understandable results. The technique produces a graphical representation of the software, which is split into easily understood blocks.*

Disadvantages of SADT

- *Can only be applied to the computer system. The methodology is geared towards examining software and cannot be readily used to identify hazards in other areas of the process.*
- *Can only identify major hazards. The technique is performed before the computer architecture is fully developed and the limited information available means that only major hazards can be identified.*

6.3.3 State-transition Diagrams

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

The state-transition diagram is one of the oldest graphical methods for indicating state-machines. It represents the sequence of operation of programmable electronic systems through control loop diagrams.

Advantages of state-transition diagrams

- *Easily understandable. Once the diagram is drawn the operations performed can be easily followed.*

Disadvantages of state-transition diagrams

- *Can only be applied to the control system. The methodology is geared towards examining control systems and cannot be readily used to identify hazards in other areas of the process.*
- *The diagram can be difficult to draw. The diagram can become complex if the system under evaluation is large, and simultaneous parallel operations cannot be represented.*

6.3.4 Petri-nets

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

Petri-nets [Agerwala 1979] applies a graphical methodology, and utilises a number of bubbles and arcs to represent the process. The bubbles identify places, while the arcs indicate transactions that occur. They can easily represent the flow structure of a computer control program which incorporates such constructs as If-Then-Else, Do-While, or Goto.

Advantages of petri-nets

- *The graphical representation assists understanding of the program. The graphical results can easily be understood and produces a simplistic representation of the computer program.*
- *The methodology can be either bottom-up, or top-down. The methodology allows either specific causes to be developed to provide their consequences, or specific consequences can be broken down to identify their causes.*

Disadvantages of petri-nets

- *Mainly applicable to computer systems. Petri-nets have mainly been developed to aid in the identification of hazards within computer programs, and are not easily converted to evaluate other sections of the plant.*

6.3.5 GRAFCET

Process phase the technique is used	During the design of the computer architecture		
Applicability to COMAH sites	1	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

Grafcet (GRAphe de Commande Etat-Transition) [PSLP Mod 9 1998] is a graphical method of specifying control sequences, and was developed in France in the 1970's. It defines the orders of the actions to be executed, and the actions themselves. It is tailored towards batch processes as it will show the sequence of events (in terms of control operations such as opening and closing valves) that are to be performed to complete a process cycle.

Advantages of GRAFCET

- *Produces easily understandable results. The graphical results show the sequence of operations that need to be performed in an easily understandable way.*

Disadvantages of GRAFCET

- *Can only be applied to the control system. The methodology is geared towards examining control systems and cannot be readily used to identify hazards in other areas of the process.*

6.4 Human hazards identification

Human tools assess the hazards associated with the interaction of the human operators with the process. They are used to identify hazards occurring due to human error while performing standard procedures, and also improper safety measures if an initial hazard occurs.

6.4.1 Task Analysis

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	2	Time and cost requirements	2

Task analysis [Kirwan 1992] is a systematic method for analysing a task in terms of its goals, operations and plans. The task is a set of operations/actions required to achieve a set goal. The goal represents the required outcome of the actions, the operation represents the various stages required to implement the goal; while the plans are methods and conditions under which the stages are performed.

Task analysis assesses what people might do while performing the operations, and asks questions such as :-

(i) What actions do the operators perform?

(ii) How do operators respond to different cues in the environment?

(iii) What errors might be made and deviations caused in plant operations?

(iv) How might any errors be recovered, or any deviations be controlled?

(v) How do operators plan their actions?

To perform task analysis a certain level of data is required :-

(vi) The general operating procedure including job descriptions, process diagrams, and operating manual.

(vii) Output from a hazard review.

(viii) Plant records.

(ix) A number of interviews with people who have experience of the process and plant.

(x) Observations of the general operation of the plant.

These can also be augmented by standards, exposure limits and data from previous incidents.

The analysis itself is then performed in a number of stages :-

(xi) Goals of the analysis. The operation to be investigated should be fully described to the agreement of all of the assessment team, and the requirements of the study defined.

(xii) Breakdown of the operation into steps. The original operation should be broken down to a level appropriate to the detail of the study. This is generally the individual steps required to perform the operation, but can often have nonessential information removed.

(xiii) Creating a plan. The methods and conditions under which the various stages are performed should be defined.

(xiv) Analysing the plan. The plan created in stage 3 should be fully analysed, to identify hazards to the equipment, the environment, lack of controls and protection etc.. Possible deviations should also be examined along with their likelihood.

(xv) Modifying the plan. The modifications to the plan should improve the method of working, safety, and minimise any deviations. The plan should also give advice on possible actions if deviations do occur.

The plan can then be fully reported along with a description of the work performed to identify the appropriate method and conditions.

Advantages of task analysis

- *Allows complex tasks to be analysed in detail. The technique splits complex tasks into a number of more simplistic ones to allow detailed examination and to allow them to be easily understood and followed.*

Disadvantages of task analysis

- *Only applicable to human interaction with the process. The technique is applied to tasks performed by the plant operators and maintenance workers, and can not be easily applied to other areas.*
- *Time consuming and expensive. A large number of tasks will be required to be performed for complex processes, and each needs to be fully developed to provide detailed information to whoever has to perform the task.*

6.4.2 Hierarchical Task Analysis (HTA)

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	3

Hierarchical task analysis [Kirwan 1992] uses the same methodology as task analysis, though a hierarchy is placed on the order of the tasks to be investigated. A complex task is broken down into a number of simpler sub-tasks, which can then be further split until they become

only individual tasks. The methodology produces either a tree structure, with the most complex task on the top and the simplest on the bottom, or a list of steps that are required to be performed in order to produce the required goal. The procedure for the task can then be easily assessed, and any possible human errors can be identified with appropriate consequences.

Advantages of HTA

- *Allows complex tasks to be analysed in detail. Tasks performed by humans on the plant are split-up by the technique to provide a detailed guide to whoever is to perform them.*
- *Provides an easily understandable procedure for the task, which can also be used in a number of other assessment techniques. The technique provides an easily understandable breakdown of the tasks which are listed in order of when they should be performed. The results are often incorporated into other human hazard identification tools.*

Disadvantages of HTA

- *Only applicable to human interaction with the process. The technique is designed to evaluate human tasks and cannot be easily applied to other areas of the process.*
- *Time consuming and expensive. A complex process will contain a large number of tasks that need to be examined by the technique to the appropriate level of detail.*

6.4.3 Action Error Analysis (AEA)

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	3	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

Action error analysis [Worsell 1994] uses the output from a hierarchical task analysis as its starting point. Each step is then analysed to identify all the errors which the human operators can commit, and their effects on the process can be evaluated. Action error analysis can easily identify hazards produced by single actions, though for large processes it is impracticable to attempt to identify hazards occurring from more than one wrong action.

The errors are broken down into a number of categories :-

(i) Unconscious slips.

(ii) Mistakes in planning or understanding.

(iii) Conscious violation of the operating procedure.

(iv) Sabotage.

The most common violations are usually due to poor equipment design which allows the task to be performed more easily in a different way to that stated in the operation manual..

Advantages of AEA

- *Allows complex tasks to be analysed in detail. It incorporates hierarchical task analysis that splits the required tasks into their components.*

Disadvantages of AEA

- *Only applicable to human interaction with the process. The technique is designed to evaluate the errors made by human operators and maintenance workers and is not easily related to other areas of the process.*
- *Time consuming and expensive. There are a large number of tasks that need to be evaluated and a large number of possible errors for each task.*
- *Difficult identifying hazards occurring from more than one error. The technique becomes very complex when attempting to identify hazards occurring from multiple errors during the performance of one or more tasks.*

6.4.4 Human Reliability Analysis

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	3	Nature of the results	Both
Applicability to SMEs	2	Time and cost requirements	3

Human reliability analysis [Swain 1983, Dougherty 1988, Dhillon 1986] is used to quantify the human errors. The assessment is performed in a number of stages :-

(i) Define the system failures of interest.

(ii) List and analyse the related human operations.

(iii) Estimate the relevant error probabilities.

(iv) Estimate the effects of human errors on the system failure rate.

(v) Recommend changes to the system and recalculate the system failure probabilities.

The first two stages are performed during task analysis, and the results from such a study can be incorporated into the final stages of the technique. It is unknown how accurate the values produced by human reliability analysis are, so the results should only be regarded as estimations.

Advantages of human reliability analysis

- *Allows complex tasks to be analysed in detail. The technique incorporates task analysis, and so allows a detailed assessment of complex tasks.*
- *Quantitative technique allowing limited predictions of human error. Probabilities are assigned to the human errors identified by the technique, and this can produce an overall probability of human error while the task is being performed.*

- *Disadvantages of human reliability analysis*

- *Only applicable to human interaction with the process. The technique is specifically tailored to assess human errors in performing tasks, and cannot be easily applied to other areas of the process.*
- *Time consuming and expensive. There are a large number of tasks and human errors that need to be evaluated by the technique, and each error has to be allocated a probability.*
- *Relies on availability of human failure rate data for the lowest level individual task. The probabilities assigned to the various errors are often estimated which can lead to errors in the calculation of the probability of an overall error.*
- *Requires skilled practitioners. Skilled team members are required to produce realistic probabilities for these errors, as well as splitting the task into its components.*

6.4.5 Pattern search method

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	2

The pattern search method [Worsell 1994] is used to identify hazards due to a number of errors. It attempts to look for a common cause which could lead to the appropriate errors, and identifies areas of importance for safety considerations.

Advantages of pattern search method

- *Can identify hazards due to more than one error. The technique examines common causes that can lead to more than one error within the process, which when combined can lead to a hazard.*

Disadvantages of pattern search method

- *Time consuming and expensive. All the causes need to be examined as well as how they interact between each other. A possible common cause would also need to be identified.*

6.4.6 Predictive Human Error Analysis (PHEA)

Process phase the technique is used	After the design phase is complete		
Applicability to COMAH sites	2	Nature of the results	Qualitative
Applicability to SMEs	1	Time and cost requirements	3

PHEA [Lees 1996] uses hierarchical task analysis to plan the task. It then systematically analyses them for :-

(i) Task type.

(ii) Error type.

(iii) Task description.

(iv) Consequences.

(v) Recovery.

(vi) Error reduction strategy.

Advantages of PHEA

- *Allows complex tasks to be analysed in detail. The technique applies hierarchical task analysis to split the complex tasks into component parts.*
- *Assesses the consequences of the hazards. The technique examines the consequences of the human errors if they occur within the process.*

Disadvantages of PHEA

- *Only applicable to human interaction with the process. The technique is designed to evaluate human error on the plant and can not be easily applied to other areas of the process.*
- *Time consuming and expensive. Each task has to be evaluated or hazards might be missed.*

7 COMPARISON OF TECHNIQUES

It is impossible to compare hazard identification techniques and come to any conclusion as to which is the best. Each technique has been developed for a specific range of circumstances taking many factors into account including the resources required to undertake the analysis, expertise available and stage of the process. This project has attempted to classify the resources required for each technique on a scale of 1 to 3 with one being quick and inexpensive and three being time consuming and expensive. Further comparisons of their applicability to SME's, COMAH, offshore and nuclear installations have been made using a four point scale with one not being applicable and four very applicable. Table 3 gives the results of the comparisons.

Table 4, Hazard identification applicability to several industries.

					Applicability to			
Ref	**Hazard Identification Techniques**	**Nature of results**	**Process life cycle phase**	**Time/Cost**	**COMAH Sites**	**SME's**	**OSD**	**Nuclear Industry**
1	Concept Hazard Analysis	Qualitative	Concept	2	3	2	2	3
2	Concept Safety Review	Qualitative	Concept	2	3	2	2	2
3	Preliminary Hazard Analysis	Qualitative	Design/operation	2	3	2	2	2
4	Pre-HAZOP	Qualitative	Design stage	1	3	2	2	3
5	HAZOP	Qualitative	Any phase	3	4	2	4	4
6	"What if?" Analysis	Qualitative	Any phase	2	4	3	3	3
7	Checklists	Qualitative	Concept/design	2	2	4	2	2
8	Standards/Codes of practice	Qualitative	Concept/design	1	3	4	3	3
9	FMEA	Qualitative	Design/operation/mods	3	3	2	3	4
10	Functional FMEA	Qualitative	Design/operation/mods	3	3	2	3	4
11	FMECA	Qualitative	Design/operation/mods	3	3	1	2	4
12	Safety Audit	Qualitative	Any phase	3	4	3	4	4
13	CHAZOP	Qualitative	Design/mods	3	3	1	3	4
14	Critical Examination of System Safety	Qualitative	Design/operation	2	2	2	1	1
15	Cause-Consequences Analysis	Both	Design/operation/mods	3	3	1	3	3
16	Fault Tree Analysis	Both	Design/operation/mods	3	3	1	3	4
17	Structured methods	Qualitative	Design stage	2	2	1	2	2
18	PETRI NETS	Qualitative	Design stage	2	2	1	1	1
19	Sneak Analysis	Qualitative	Design/operation	2	3	2	2	2
20	Structural Reliability Analysis	Quantitative	Design/construction	2	2	1	2	2
21	Reliability Block diagram	Quantitative	Design/mods	2	2	2	2	2
22	Human reliability Analysis	Semi-qualitative	Operation/mods	3	3	2	3	3
23	Action Error Analysis	Both	Operation/mods	2	3	1	3	3
24	Task Analysis	Both	Design/operation/mods	2	3	2	3	4

Table 4, Continued

Ref	Hazard Identification Techniques	Nature of results	Process life cycle phase	Time/Cost	Applicability to			
					COMAH Sites	SME's	OSD	Nuclear Industry
25	Maintenance and Operability study	Qualitative	Design/operation/mods	3	3	2	3	2
26	Predictive Human Error Analysis	Semi-qualitative	Design/operation/mods	3	2	1	2	3
27	Pattern Search method	Qualitative	Operation/mods	2	2	1	2	2
28	Vulnerability Assessment	Qualitative	Design/mods	2	2	1	2	2
29	DEFI method	Quantitative	Design stage	2	1	1	2	2
30	Maintenance Analysis	Both	Operation/mods	3	3	2	3	3
31	Matrices	Qualitative	Design stages	2	2	1	1	1
32	GOFA	Semi-qualitative	Design/operation/mods	2	2	1	2	2
33	MOSAR	Semi-qualitative	Operation/mods	2	2	1	2	1
34	FIHI	Qualitative	Design/operation	2	2	1	2	2
35	State-Transition Diagrams	Qualitative	Design stage	2	2	1	1	2
36	GRAFCET	Qualitative	Design stage	2	1	1	1	1
37	Inherent Hazard Analysis	Qualitative	Design stage	2	2	2	2	2
38	Hierarchical Task Analysis	Qualitative	Operation/mods	3	3	1	3	4

Note:

COMAH = Control Of Major Accident Hazards
SME = Small Medium Enterprises
OSD = Offshore Safety Division
Both = The nature of the results are qualitative and quantitative

8 DISCUSSION

The literature review has provided an overwhelming source of information on hazard identification techniques. Many of the references are themselves a comparison of hazard assessment schemes to a particular application. Whilst there is a wealth of information on examples of applying hazard identification techniques, there is little guidance available on how to apply them.

Whilst the literature was wide ranging it is impossible to claim that every technique has been listed. Many of the techniques have been developed for particular applications and renamed. No attempt has been made to sort out this 'family tree' of techniques but where they are obviously similar they have been grouped together as a single technique.

The most difficult aspect of this review was deciding on the amount of detail to be included for each technique: too little and the review becomes little more that a list, too much and it becomes an unreadable tome. A subjective assessment of the advantages and disadvantages is given, but the real question about hazard identification is related to its ability to carry out the task of identifying all the relevant hazards. This question can only be answered on a case by case basis. Most techniques can be applied in any circumstances provided enough resources and expertise is available. The most suitable technique will not only depend on the application but also the available resources. It would be nonsensical to embark upon a HAZOP without access to an experienced chairman. Other less applicable techniques could probably be undertaken with more chance of success by utilising available expertise.

The comparison has attempted to match techniques with various types of installations taking into account not only the probable availability of resources to carry out the assessment but also the magnitude of the hazards present.

9 CONCLUSIONS

This report has provided a useful overview of the majority of the hazard identification techniques that will be found in COMAH reports and other high hazard industries. It also gives an indication of the applicability of each technique for SME's, offshore and nuclear facilities.

There are a wide range of hazard identification techniques available most of which have many examples published. With the notable exception of HAZOP there are few formal guidance documents on the application of such techniques. The most common method of learning to apply a technique is attendance at one of the many training courses or working with a more experienced colleague.

The lack of formal guidance is to be expected with a range of techniques that need to be very flexible to allow their application to a wide range of circumstances without discouraging free thinking. The guidance available appears to concentrate on providing a description of the technique rather than setting any standards of quality for applying the technique.

10 RECOMMENDATIONS

(i) Feedback on this work should be sought from both industry and the regulators of experience gained from applying hazard analysis to satisfy the COMAH Regulations. This report should be updated to take into account ant significant comments.

(ii) A small number of techniques that are most commonly used on COMAH installations should be reviewed in greater detail. This detailed review should provide guidance on the information required for COMAH reports and assessment criteria

11 REFERENCES

1. Agerwala 1979, PUTTING PETRI NETS TO WORK, T.Agerwala, Computer, v12, n12, p85-94, 1979.
2. Andow 1991, GUIDANCE ON HAZOP PROCEDURES FOR COMPUTER - CONTROLLED PLANTS, HSE contract research report No. 26/1991, P.Andow, Her Majesty's Stationary Office, 1991.
3. Balemans 1974, CHECK-LIST. GUIDE LINES FOR SAFE DESIGN OF PROCESS PLANTS, A.W.M.Balemans, 1st International Loss Prevention Symposium, p7-33, 1974.
4. BSEN1050 1997, SAFETY OF MACHINERY - PRINCIPLES FOR RISK ASSESSMENT, BS EN 1050 : 1997.
5. BS5760:2 1992, GUIDE TO THE ASSESSMENT OF RELIABILITY, BS 5760 : Part 2 : 1992.
6. BS5760:5 1992, GUIDE TO FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMEA AND FMECA), BS 5760 : Part 5 : 1992.
7. BS5760:7 1992, GUIDE TO FAULT TREE ANALYSIS, BS 5760 : Part 7 : 1992.
8. BS5760:9 1992, RELIABILITY OF SYSTEMS, EQUIPMENT AND COMPONENTS. PART 9. GUIDE TO THE BLOCK DIAGRAM TECHNIQUE, BS 5760 : Part 9 : 1992.
9. CCPS 1992, GUIDELINES FOR HAZARD EVALUATION PROCEDURES, SECOND EDITION, Centre for Chemical Process Safety, American Institute of Chemical Engineers, 1992.
10. Chastain 1997, CONDUCT BETTER MAINTENANCE AND OPERABILITY STUDIES, J.W.Chastain, J.H.S.Jenson, Chemical Engineering Progress, v93, p2, p49-53, 1997.
11. CIA 1970, SAFE AND SOUND, British Chemical Industry Safety Council of the Chemical Industries Association Limited, 1970.
12. CIA 1977, SAFETY AUDITS. A GUIDE FOR THE CHEMICAL INDUSTRY, The Chemical Industry Safety and Health Council of the Chemical Industries Association, 1977.
13. CIA 1993, A GUIDE TO HAZARD AND OPERABILITY STUDIES, Chemical Industries Association, 1993.

14. Clark 1997, APPLY THESE MATRICES TO HELP ENSURE PLANT SAFETY, D.G.Clark, Chemical Engineering Progress, v93, n12, p69-73, 1997.

15. COMAH 1999, A GUIDE TO THE CONTROL OF MAJOR ACCIDENT HAZARDS REGULATIONS, L111 HSE Books, 1999.

16. Dougherty 1988, HUMAN RELIABILITY ANALYSIS. A SYSTEMS ENGINEERING APPROACH WITH NUCLEAR POWER PLANT APPLICATIONS, E.M.Dougherty.Jr., J.R.Fragola, John Wiley & Sons, 1988.

17. Dhillon 1986, HUMAN RELIABILITY WITH HUMAN FACTORS, B.S.Dhillon, Pergamon Press, 1986.

18. Eades 1998, APPROACHES TO HAZARD IDENTIFICATION, M.Eades, Health and Safety Executive (OTO 97 068), 1998.

19. Elliott 1968, CRITICAL EXAMINATION IN PROCESS DESIGN, D.M.Elliott, J.M.Owens, The Chemical Engineer, p377-383, Nov. 1968.

20. Fairley 1985, SOFTWARE ENGINEERING CONCEPTS, R.E.Fairley, McGraw-Hill, 1985.

21. Greenberg 1992, RISK ASSESSMENT AND RISK MANAGEMENT FOR THE CHEMICAL PROCESS INDUSTRY, H.R.Greenberg, J.J.Cramer, Van Nostrum Reinhold, 1992.

22. Hawksley 1987, RISK ASSESSMENT AND PROJECT DEVELOPMENT, J.L.Hawksley, The Safety Practitioner, v5, n10, p10-16, 1987.

23. Kirwan 1992, A GUIDE TO TASK ANALYSIS, B.Kirwan, L.K.Ainsworth. (Ed.), Taylor&Francis Ltd. 1992.

24. Kletz 1995, COMPUTER CONTROL AND HUMAN ERROR, T.Kletz, et.al., Institution of Chemical Engineers, 1995.

25. Lear 1993, COMPUTER HAZARD AND OPERABILITY STUDIES, J.Lear, Safety and Reliability of Process Control Systems Symposium, Sydney University Chemical Engineering Association, 6th Oct. 1993.

26. Lees 1996, LOSS PREVENTION IN THE PROCESS INDUSTRIES, VOLUME 1, F.P.Lees, Butterworth & Co. Ltd., 1996

27. Miller 1971, MANAGEMENT TOOLS IN LOSS PREVENTION, R.L.Miller, W.B.Howard, Major Loss Prevention in the Process Industries, The Institute of Chemical Engineers I.Chem.E Symposium Series No. 34, p203-209, 1971.

28. Nielson 1975, CAUSE-CONSEQUENCE DIAGRAMS, D.S.Nielson, Nordic Working Group on Reactor Safety, 1975.

29. Ozag 1987, HAZARD IDENTIFICATION AND QUANTIFICATION, H.Ozag, L.M.Bendixen, Chemical Engineering Progress, v83, n4, p55-64, 1987.

30. Parry 1986, A REVIEW OF HAZARD IDENTIFICATION TECHNIQUES AND THEIR APPLICATION TO MAJOR ACCIDENT HAZARDS, S.T.Parry, United Kingdom Atomic Energy Authority (SRD R379), 1986.

31. PSLP Mod 1 1998, RISK ASSESSMENT AND HAZARD ANALYSIS, MSc in Process Safety and Loss prevention, Module 1, University of Sheffield, 1998.

32. PSLP Mod 9 1998, COMPUTER CONTROL SAFE PRACTICES, MSc in Process Safety and Loss prevention, Module 9, University of Sheffield, 1998.

33. Rasmussen 1997, HAZARD IDENTIFICATION BASED ON PLANT FUNCTIONAL MODELLING, B.Rasmussen, C.Whetton, Reliability Engineering and Systems Safety, v55, p77-84, 1997.

34. Reeves 1989, A DESCRIPTION OF GOFA, A.B.Reeves, G.L.Wells, D.A.Linkens, Loss Prevention and Safety Promotion 6, p28.1, 1989.

35. Schlechter 1995, PROCESS RISK ASSESSMENT - USING SCIENCE TO "DO IT RIGHT", W.Schlechter, International Journal of Pressure Vessels and Piping, v61, n2-3, p479-494, 1995.

36. Socha 1996, USE OF VULNERABILITY ASSESSMENT IN HAZARD ANALYSES, N.E.Socha, Professional Safety, v41, n9, p23-25, 1996.

37. Stewart 1997, PROBABILISTIC RISK ASSESSMENT OF ENGINEERING SYSTEMS, M.G.Stewart, R.E.Melchers, Chapman and Hall, 1997.

38. Swain 1983, HANDBOOK OF HUMAN-RELIABILTY ANALYSIS WITH EMPHASIS ON NUCLEAR PLANT APPLICATIONS, A.D.Swain, H.E.Guttman, U.S. Nuclear Regulatory Commission, Report No. NUREG-CR-1278, 1983.

39. Vesely 1981, FAULT TREE HANDBOOK, W.E.Vesely, F.F.Goldberg, N.H.Roberts, D.F.Haasl, U.S. Nuclear Regulatory Commission, 1981.

40. Wells 1993, PRELIMINARY SAFETY ANALYSIS, G.Wells, M.Wardman, C.Whetton, Journal of Loss Prevention in the Process Industry, v6, n1, p47-60, 1993.

41. Wells 1996, HAZARD IDENTIFICATION AND RISK ASSESSMENT, G.Wells, Institution of Chemical Engineers, 1996.

42. Whetton 1993, SNEAK ANALYSIS OF PROCESS SYSTEMS, C.P.Whetton, Transactions of the Institute of Chemical Engineers, v71B, p169-179, 1993.

43. Whetton 1994, SNEAK ANALYSIS OF BATCH PROCESSES, C.Whetton, W.Armstrong, Journal of Hazardous Materials, v38, p257-275, 1994.

44. Williams 1971, SAFETY AUDITS, D.Williams, Major Loss Prevention in the Process Industries, The Institute of Chemical Engineers Symposium Series No. 34, p220-242, 1971.

45. Worsell 1994, THE APPLICATION OF RISK ASSESSMENT TO MACHINERY SAFETY, N.Worsell, J.Wilday, Health and Safety Executive, Report No. IR/L/RAM/94/02, 1994.