HSE
Health & Safety Executive

A comparison of accident experience with Quantitative Risk Assessment (QRA) methodology

Prepared by **Det Norske Veritas Ltd**
for the Health and Safety Executive

CONTRACT RESEARCH REPORT
293/2000

HSE
Health & Safety Executive

A comparison of accident experience with Quantitative Risk Assessment (QRA) methodology

Andrew Franks, Gareth Hughes and Sajid Hanif
Det Norske Veritas Ltd
Highbank House
Exchange Street
Stockport
SK3 0ET

QRA methodology for onshore process plants was studied and compared with accident experience, as drawn from accident databases (MHIDAS, MARS and the Institution of Chemical Engineers Accident Database) and accident theory.

The analyses of accident databases indicate that the proportion of accidents occurring when the plant is in some abnormal state may be 40% or more. Maintenance appears to be a particularly important abnormal state.

Whether or not accidents occurring during maintenance or other abnormal states need to be considered explicitly within a QRA study depends to a large extent on the scope and purpose of the QRA, as well as the complexity of the plant being studied. This is thought to be particularly important for cases where the QRA is to be used for producing recommendations for risk reduction options.

Where necessary, this could be done by building upon the existing practice of supplementing the conventional 'top down' approach with other hazard identification methods. This could include a review of hazard identification studies performed for other purposes. Ultimately, as experience in performing QRA studies in this way develops, it may be possible to extend the generic lists of events used in the 'top down' approach to include events occurring during some abnormal states.

No attempt has been made during this study to quantify the effect of excluding events occurring during abnormal plant states on the risk figures obtained from a QRA study. It is recommended that case studies be conducted to investigate this area further.

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

HSE BOOKS

First published 2000

ISBN 0 7176 1849 8

CONTENTS

EXECUTIVE SUMMARY

Uncertainty in Quantitative Risk Assessment (QRA) can take several forms, as discussed by Cassidy (1994). One such source of uncertainty is described as 'Uncertainty in knowing whether or not there is an effect to be incorporated in an estimate'. In other words, there is uncertainty associated with knowing which events or phenomena to attempt to model within a QRA as applied to onshore process plant.

A QRA will postulate a number of failure events resulting in a loss of containment of a hazardous material. Typically these failure events consist of leaks from pipework and vessels, assumed to occur under otherwise normal operating conditions for the system under study. It is unusual for a QRA to consider explicitly accidents occurring during abnormal or process upset conditions (although there are some notable exceptions such as exothermic reaction runaway and boiling liquid expanding vapour explosions, or BLEVEs).

In contrast, a number of recent, high profile accidents have been reported which happened outside the normal operating parameters of the plant in question. Consider, for example:

- The fire and explosion at the Pembroke Cracking Company refinery in Milford Haven in July 1994. A flare line, designed to carry hydrocarbon vapour, ruptured during a process upset when liquid was carried over into the flare system.
- The fire at Hickson and Welch Ltd., Castleford, when unstable residues in a still base self heated and ignited during a cleaning operation.

It may therefore be legitimate to ask to what extent the events postulated withinQRAs reflect experience as recorded in accident reports. The aim of the study was to compare the available accident records with QRA methodology and assumptions in order to begin to answer this question.

The following approach was adopted:

- A survey of the literature on QRA methodology was conducted, in order to study the approaches used and assumptions made by QRA practitioners in determining what events should be modelled within a given QRA study.
- It is common practice to use 'generic failure data' within a QRA (see Section 3 for more details). Information on generic failure data was gathered and analysed in order to determine what kinds of events are encompassed by such data (and, by implication, what kinds of events are considered by a QRA that makes use of such data).
- Relevant information on the subject of uncertainty and quality in QRA was also studied. This is discussed in Section 4.
- The application of QRA was investigated through consideration of a number of published QRA studies, to examine which approaches had been used in practise.
- The literature concerning accident theory was surveyed and a brief summary is presented in Section 6. A comparison was made with QRA methodology.
- A search was made of the MHIDAS, IChemE and MARS databases for records of major accidents or 'near miss' incidents which had the potential to be major accidents. Other sources of information on major accidents (such as HSE investigation reports) were also consulted. In order to limit the scope of the searches, attention was focused on incidents in the UK since 1984.
- A comparison was made of QRA methodology (including the use of generic failure rates) with the findings of the analysis of the information on major accidents and accident theory.

A survey of the literature on QRA methodology and an examination of published reports on QRA studies have revealed that, broadly speaking, approaches divide into two categories:

1. An approach that is similar in many respects to that adopted in the nuclear industry. This involves a hazard identification study of the plant under investigation (using techniques such as HAZOP or FMEA), selection of scenarios of interest (usually by expert judgement, and usually focussing on major events) and detailed quantification of those scenarios.
2. The so-called 'top down' approach, involving consideration of potential leaks and major releases from fractures of all process pipes, equipment and vessels. This typically generates a large number of scenarios, which may then be subjected to a selection process before producing a final list of events to be modelled. This approach usually involves the use of generic failure frequency data, since it would be impractical to use detailed techniques such as fault tree analysis to quantify the failure frequencies for the large number of scenarios produced.

The two approaches would probably converge if the hazard identification studies performed under the first approach were comprehensive and only limited screening of scenarios was performed.

A broad comparison of QRA methodology with accident theory has indicated that tools exist that would enable QRA to address most of the levels described within hierarchical or sequential accident models, although these tools are not always used.

The hazard identification and incident selection process is critical to determining which events are modelled within a QRA study. Research has shown that hazard identification studies using the available techniques are unlikely to identify every hazard present. This situation is improved by using a combination of techniques rather than a single technique. This research also led to consideration of ways of addressing issues of uncertainty and quality in QRA. Four approaches to evaluating the quality of a given QRA were identified:

- Carrying out a complete parallel analysis on the same system.
- Carrying out a parallel analysis on some parts of the same system.
- Comparing the analysis with experience, including descriptions of accidents which have occurred in similar systems and/or the system under consideration.
- Examining the process used to conduct the analysis.

The last of these is analogous to evaluation of the quality policies and procedures of a supplier instead of testing samples of their product. It is the least demanding of resources of all of the methods listed. A checklist (known as QUASA) has been developed to assist in the evaluation. The section of the QUASA checklist dealing with identification of hazards contains questions to evaluate the extent to which abnormal plant conditions, management and human factors have been covered. The checklist also has sections relating to frequency analysis and consequence analysis. However, there is no section that deals explicitly with the process of incident enumeration and incident selection.

As stated above, the 'top down' approach to QRA usually involves the use of generic failure frequency data. The assumption made in using these data is that they 'include' contributions from all of the failure causes of interest. However, an examination of the sources of generic failure frequency data for pipes and pressure vessels has shown that few of the sources contain information of direct relevance to the onshore process industry. Most of the data related to equipment used for steam, water or air service.

Data sources that draw predominantly upon information collected on such equipment are unlikely to include some of the failure causes that are of concern within the onshore process industry. Hence there is a strong possibility that should these generic failure frequency data be used in a QRA, the assumption that all relevant failure causes will be 'included' in the generic frequency would be incorrect.

A number of sources indicated the importance of the human error-related element of the frequency data. The occurrence of human error is clearly influenced by the quality of safety management and other performance shaping factors, many of which are specific to the system under study. Attempts to address this within QRA by application of modification factors derived from audit results have been reported.

A further difficulty with the 'top-down' approach is that, although leak sources are comprehensively addressed, other, more complex failures may be neglected. This difficulty has not gone unrecognised. It is evident from published QRA studies that this problem is usually addressed by complementing the 'top-down' approach with other methods of identifying hazards, including:

- A consideration of the properties of the materials under investigation.
- An examination of the historical accident record for similar plant.
- More detailed hazard identification studies of particular areas of the plant.

At the consequence analysis stage, it is common practise to assume that the leak or failure occurs under otherwise normal conditions for the process. However, an analysis of three accident databases (MHIDAS, MARS and the IChemE Accident Database) has indicated that the proportion of accidents that occur when the plant is in some abnormal state may be 40% or more. A significant proportion of these 'abnormal states' appears to be associated with maintenance operations. Previous studies by HSE of maintenance related accidents have indicated that 30% of such accidents had had the potential to present an off-site risk.

The extent to which the issues outlined above represent a cause for concern will depend on the scope and purpose of the QRA, as well as the level of complexity of the plant under investigation.

A QRA can never be expected to address all potential accidents at a given plant, but it should address all of those potential accidents that are relevant to the scope as defined. Thus, if the scope of the study involves calculation of the off-site risk, the QRA should consider all accidents with the potential for off-site effects. Given the results of the analyses of the accident databases and the previous HSE work on maintenance related accidents, it cannot be assumed that accidents occurring when the plant is in an abnormal state do not have the potential for off-site effects. Similarly, if the scope of the QRA study includes a calculation of on-site risk, then maintenance related accidents, for example, may clearly be of significance.
It could be argued that the range of accidents modelled within a QRA would be representative of the full range of accidents that might occur. For example, consider the situation where a vessel storing flammable liquid is analysed within a QRA. Typically, leaks or major failures of the vessel would be modelled, assuming some level of vessel contents, resulting in fires and explosions. It could then be argued that an explosion within the vessel during a maintenance operation is 'bracketed' or adequately represented by the range of fires and explosions already modelled. This may indeed be the case, but whether or not this is satisfactory depends on the purpose of the QRA. If the QRA is simply to be used to give an estimate of the off-site risk, then the position may be satisfactory. If the QRA is to be used to make decisions concerning options for reduction of risk, then the position may not be satisfactory. The fact that events that have been modelled within the QRA assume otherwise normal conditions means that recommendations arising from the QRA are likely to relate to

the normal operation of the plant. It is difficult to use the QRA to produce recommendations concerning abnormal plant operations such as upsets or maintenance, even though these areas could be significant.

It might be expected that simple plant (such as bulk storage of chlorine at water treatment works) would be less prone to accidents arising from certain abnormal states such as process upsets. No analysis of the accident records obtained from databases has been attempted in this regard.

CONCLUSIONS AND RECOMMENDATIONS

The analyses of accident databases indicate that the proportion of accidents occurring when the plant is in some abnormal state may be 40% or more. Maintenance appears to be a particularly important abnormal state.

Whether or not accidents occurring during maintenance or other abnormal states need to be considered explicitly within a QRA study depends to a large extent on the scope and purpose of the QRA, as well as the complexity of the plant being studied. This is thought to be particularly important for cases where the QRA is to be used for producing recommendations for risk reduction options.

Where necessary, this could be done by building upon the existing practise of supplementing the conventional 'top down' approach with other hazard identification methods. This could include a review of hazard identification studies performed for other purposes. Ultimately, as experience in performing QRA studies in this way develops, it may be possible to extend the generic lists of events used in the 'top-down' approach to include events occurring during some abnormal states.

No attempt has been made during this study to quantify the effect of excluding events occurring during abnormal plant states on the risk figures obtained from a QRA study. It is recommended that case studies be conducted to investigate this area further.

1. INTRODUCTION

1.1 BACKGROUND

This report deals with one source of uncertainty in Quantitative Risk Assessment (QRA) as it is applied in the onshore process industry.

Risk is the chance of something adverse happening (HSE 1995). In the present context, the 'something adverse', or consequence, is usually fatality, or exposure of people to a specified level (or dose) of a harmful substance or source of energy. The 'chance' is usually expressed as a probability or a frequency. QRA methodology is discussed further in Section 2.

A risk assessment consists of an estimation of the risks arising from identified hazards, with a view to the control, avoidance or comparison of those risks. A QRA is a risk assessment which incorporates numerical estimates (i.e. – of consequences and frequency). QRA is not an exact science and uncertainties within the numerical risk estimates produced arise from a number of sources (HSE 1989, Cassidy 1994):

1. Errors, in the formal sense of scientific measurement.
2. Uncertainties in the modelling process and in estimates of biological effects such as vulnerability.
3. Uncertainty in whether or not there is indeed an effect to be incorporated in an estimate.
4. Omissions of possible causes of risk due to.
    - Incomplete analysis of the mechanical or engineering sources of plant failure.
    - Non-quantification of human error.
    - Omission of extreme natural causes.

It is the third of these sources which is the focus of this research. This could also be expressed as uncertainty associated with knowing which events or phenomena to attempt to model within a QRA.

A QRA will postulate a number of failure events resulting in a loss of containment of a hazardous material. Typically these failure events consist of leaks from pipework and vessels, assumed to occur under otherwise normal operating conditions for the system under study. It is unusual, if not rare, for a QRA to consider explicitly accidents occurring during abnormal or process upset conditions (although there are some notable exceptions such as exothermic reaction runaway and boiling liquid expanding vapour explosions, or BLEVEs).

In contrast, a number of recent, high profile accidents have been reported which happened outside the normal operating parameters of the plant in question. Consider, for example:

- The fire and explosion at the Pembroke Cracking Company refinery in Milford Haven in July 1994. A flare line, designed to carry hydrocarbon vapour, ruptured during a process upset when liquid was carried over into the flare system.
- The fire at Hickson and Welch Ltd., Castleford, when unstable residues in a still base self heated and ignited during a cleaning operation.

It may therefore be legitimate to ask to what extent the events postulated withinQRAs reflect accident experience as recorded in historical records, or as embodied by accident theory. The aim of the proposed study is to compare the available accident records and accident theory with QRA methodology and assumptions in order to begin to answer this question.

1.2 AIMS

The aims of the project were therefore as follows:

- To investigate the extent to which the events modelled within QRAs reflect accident experience.
- To consider whether or not QRA methodologies and assumptions need to be altered in the light of the project and make recommendations.

1.3 APPROACH

In order to meet the stated aims, the following approach was adopted:

- A survey of the literature on QRA methodology was conducted, in order to study the approaches used and assumptions made by QRA practitioners in determining what events should be modelled within a given QRA study.
- It is common practice to use 'generic failure data' within a QRA (see Section 3 for more details). Information on generic failure data was gathered and analysed in order to determine what kinds of events are encompassed by such data (and, by implication, what kinds of events are considered by a QRA that makes use of such data).
- Relevant information on the subject of uncertainty and quality in QRA was also studied. This is discussed in Section 4.
- The application of QRA was investigated through consideration of a number of published QRA studies, to examine which approaches had been used in practise.
- The literature concerning accident theory was surveyed and a brief summary is presented in Section 6. A comparison was made with QRA methodology.
- A search was made of the MHIDAS, IChemE and MARS databases for records of major accidents or 'near miss' incidents which had the potential to be major accidents. Other sources of information on major accidents (such as HSE investigation reports) were also consulted. In order to limit the scope of the searches, attention was focused on incidents in the UK since 1984.
- A comparison was made of QRA methodology (including the use of generic failure rates) with the findings of the analysis of the information on major accidents and accident theory.

2. QRA METHODOLOGY

This section details the findings of the survey of relevant literature on QRA methodology. In addition to papers, books, guidance and standards relating to QRA, publicly available QRA studies were also considered. These are discussed separately in Section 5.

2.1 A DESCRIPTION OF QRA METHODOLOGY

QRA and many of its related techniques were initially developed in the aerospace, electronics and nuclear power industries (where it is known as Probabilistic Safety Assessment, PSA, or Probabilistic Risk Assessment, PRA). The method began to be applied to the process industry in the 1970s and 1980s, with examples such as the Canvey study (HSE 1978, 1981) and the Rijnmond study (Rijnmond Public Authority, 1982) being well known.

The British Standard giving guidance on the risk analysis of technological systems (BSI 1996) was designed to be broadly applicable to a range of industries or types of system. The standard views risk analysis as taking place within an overall process of risk management, as illustrated in Figure 1.

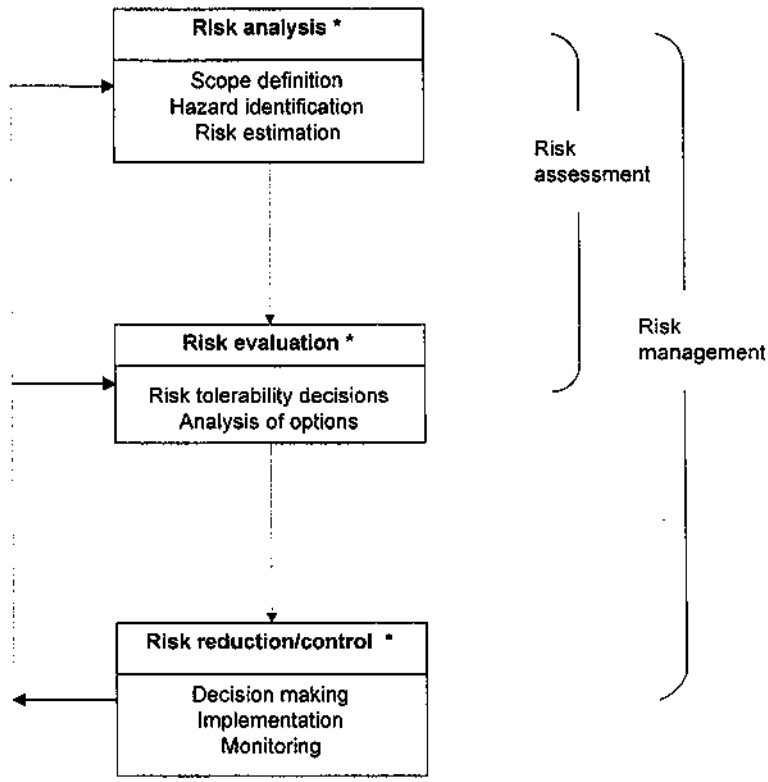

Figure 1
Relationship between risk analysis and risk management

Risk management is carried out with the objective of preventing, controlling, or reducing risk. Before this can be done, risk has to be measured using risk analysis. The results of the analysis are then evaluated (perhaps by comparison with risk criteria) to determine whether or not the risks are acceptable, or whether more needs to be done to reduce them. Different options for risk reduction may be considered before decisions are taken and implemented.

The risk analysis seeks to provide the answers to three questions:

- What can go wrong (by hazard identification)?
- How likely is this to happen (by frequency analysis)?
- What are the consequences (by consequence analysis)?

The overall objective of the analysis is given as being to provide a rational basis for decisions concerning risk. The risk analysis process is shown in more detail in Figure 2, with the various steps described in more detail below.

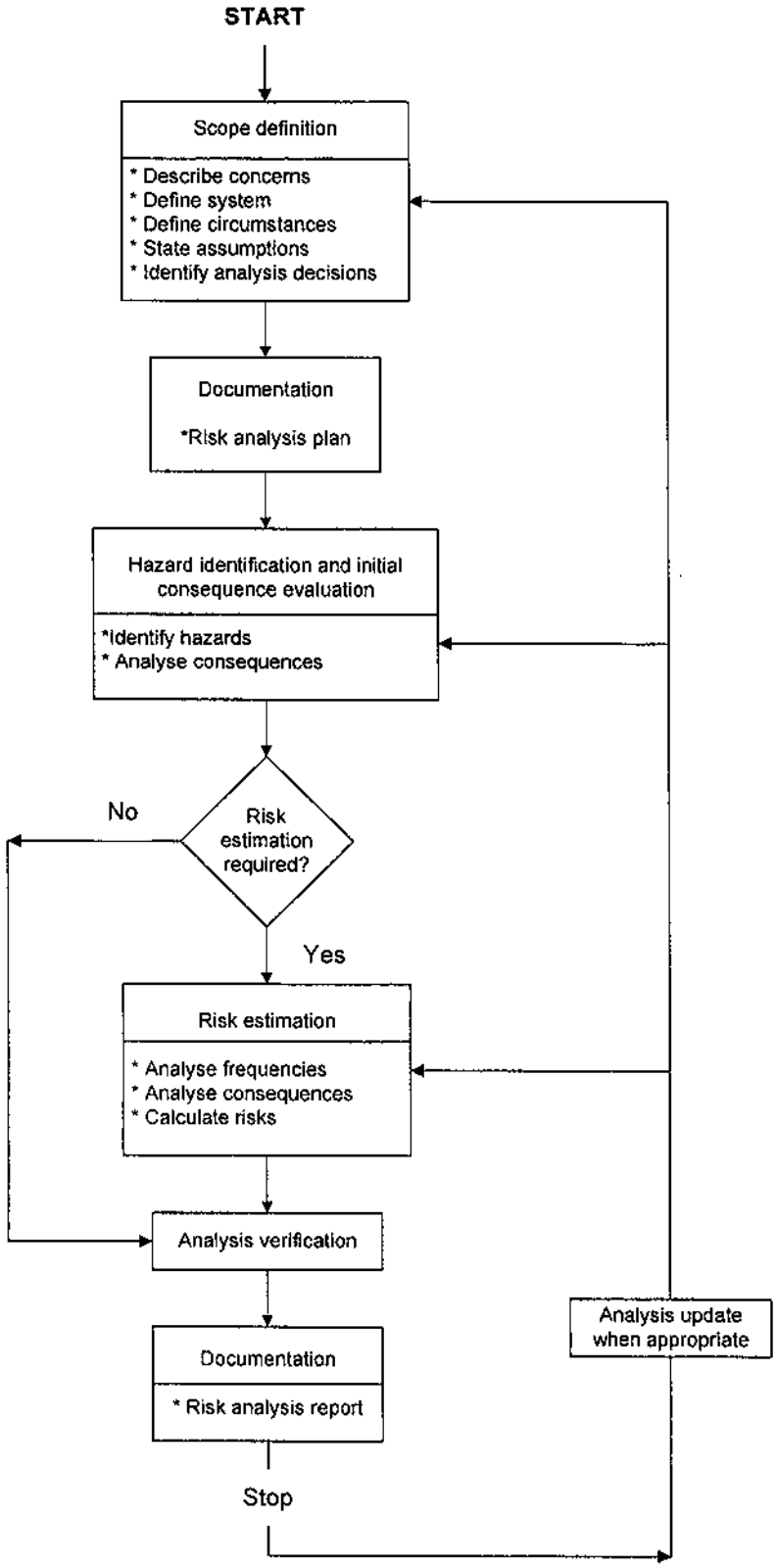

Figure 2
Risk analysis process

A more detailed procedure for Chemical Process QRA (CPQRA) is given by the American Institute of Chemical Engineers Center for Chemical Process Safety (CCPS 1989). It is broadly similar to that given in the British Standard. This is shown in Figure 3.

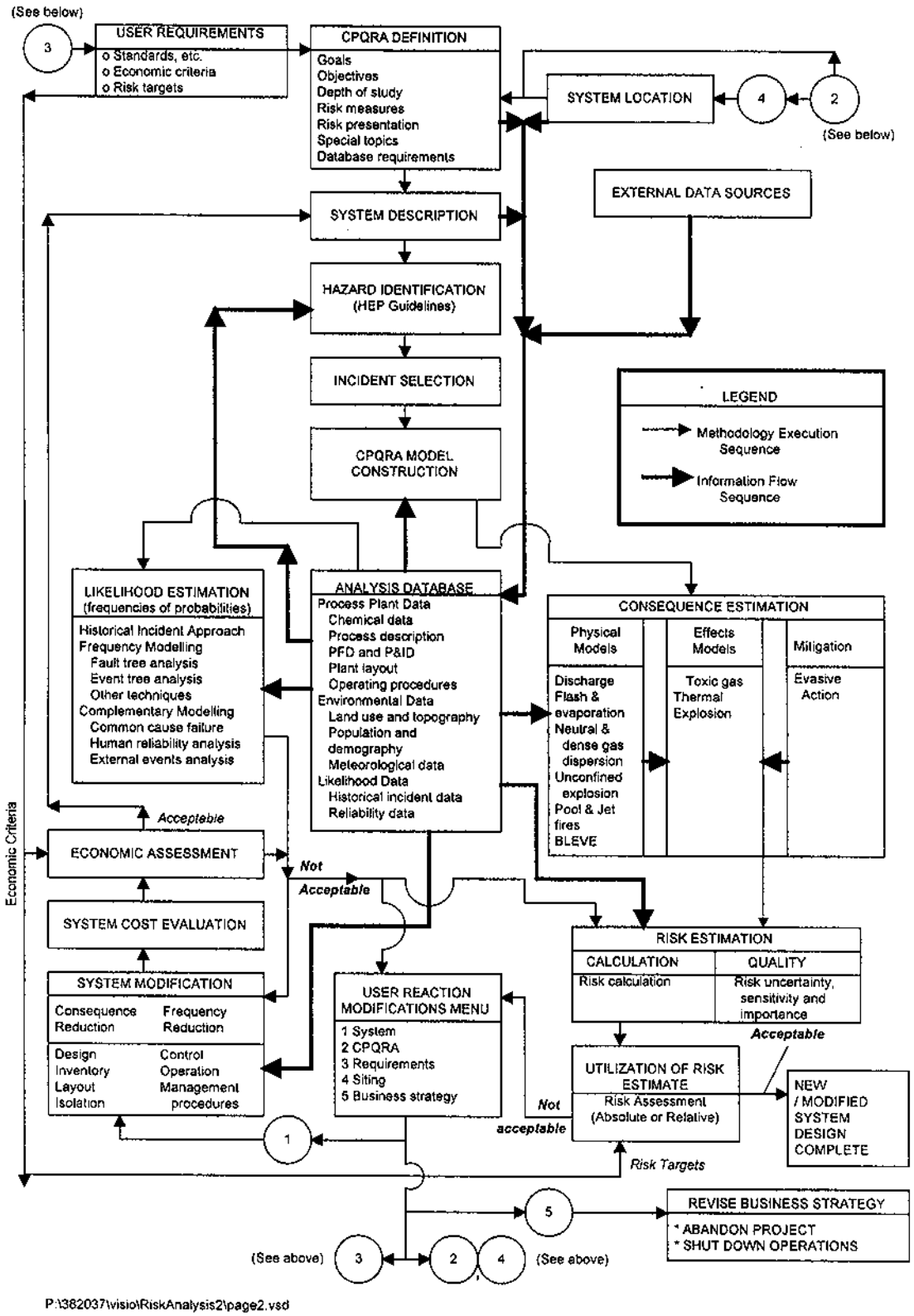

Figure 3
Framework for Chemical Process QRA (CPQRA)

In general terms, other descriptions of the overall QRA process (CONCAWE 1982, World Bank 1988, IAEA 1998) do not differ greatly from those shown.

2.1.1 Scope Definition

Scope definition is an essential part of the process, since it will determine the breadth, depth and outputs of the analysis. It involves:

- Describing the reasons for and / or the problems that led to the risk analysis (involving formulation of the objectives of the analysis and defining the events occurring within the system that are of concern).
- Defining the system to be analysed (including a general description, system boundaries, surrounding environment, energy / material flows and operating conditions).
- Identifying relevant information sources.
- Stating any assumptions to be made or any constraints on the analysis.
- Identifying the decisions that have to be made, the required outputs from the study and the decision makers.

2.1.2 Hazard Identification and Initial Consequence Evaluation

The aim of the hazard identification is to identify all of the hazards which generate risk within the system, together with the way in which the hazards could be realised. This may involve the use of accident / incident data (representing known hazards) and / or the use of formal methods such as Hazard and Operability Studies (HAZOP) or Failure Modes and Effects Analysis (FMEA). The choice of formal method should be appropriate to the system under examination.

The British Standard states that an initial evaluation of the significance of the hazards should be conducted on the basis of consequence analysis. This should determine one of three possible courses of action:

1. Take corrective action at this point to eliminate or reduce the hazards.
2. End the analysis here because the hazards or their consequences are insignificant.
3. Proceed with the risk estimation.

As pointed out by several authors, hazard identification is a critical stage in the risk analysis, since it will determine what is carried forward into the risk calculations. A hazard omitted at this stage will not be included in the final risk estimate, resulting in an underestimate of risk.

This step (and the related steps of Incident Enumeration and Incident Selection, see below) is also of considerable relevance to the present study, since it governs the decisions made concerning which events are to be incorporated into the analysis.

2.1.3 Incident Enumeration and Incident Selection

These steps are described explicitly in the CCPS reference. They are not specifically referred to in the British Standard, but may be implicit in the carrying forward of identified hazards to the frequency analysis and consequence analysis stages.

As stated above, the hazard identification process should identify all of the relevant hazards and the ways in which those hazards are realised. Realisation of a hazard involves an initiating event and intermediate events. Incident enumeration involves identifying and listing all incident scenarios of potential interest on the basis of the information generated by the hazard identification study. The product is an Initial List of incidents. An example is given in Table 1 below.

Table 1
Example of incident enumeration

Hazard	Initiating event	Intermediate events	Incident scenario
Storage of liquefied petroleum gas (LPG)	Impact on pipe giving leak	Failure to isolate Flammable cloud ignites immediately	Jet fire

This Initial List is then subjected to a selection process, with the goal of limiting the total number of incidents carried forward to subsequent steps in the QRA to a manageable size.

Firstly, the Initial List is reviewed in order to identify any incidents which are too small or trivial to be of concern (bearing in mind the scope of the QRA). These incidents are then removed from the Initial List to produce the Revised List.

The Revised List is then condensed further by combining redundant or very similar incidents together, producing the Condensed List. The Condensed List can be compressed further by grouping similar incidents into subsets and replacing each of these subsets with single, representative incidents. The list formed in this manner is termed the Expansive List.

A detailed or complex study might use all of the incidents on the Expansive List. In some cases, however, it may only be necessary to use a bounding set of 'worst case' incidents or a representative set illustrating the range of incidents that could occur.

A methodical treatment of the findings of the hazard identification exercise in this way should result in all relevant incident scenarios being carried forward to the risk assessment, although there is, of course, scope for error.

2.1.4 The 'Top Down' Approach

An alternative approach is described by CCPS and other authors (World Bank 1988, Pape and Nussey 1985, Clay et al. 1988) which effectively bypasses much of the hazard identification, incident enumeration and incident selection stages.

Known as the 'top down' or 'methodical rupture' approach, it involves considering potential leaks and major releases from fractures of all process pipes, equipment and vessels. Although a comprehensive list of potential leak sources is generated in this manner, other, more complex incident scenarios, that may have been raised as a result of a hazard identification exercise, will be missed. Freeman et al. (1986) describe a method which considers both fractures and other events by applying a consequence screening protocol.

2.1.5 Consequence Analysis

According to the British Standard, Consequence Analysis is used to obtain an estimate of the impact (on people, property or the environment) of undesired events. The analysis should:

- Be based on the undesired events selected.
- Describe any consequences arising from the undesirable events.
- Take into consideration existing measures to mitigate the consequences together with all relevant conditions that have an effect on the consequences.
- Give the criteria used for completing the identification of the consequences.
- Consider both the immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the study.
- Consider secondary consequences, such as those associated with adjacent equipment and systems.

The 'undesired events' are those arising from the hazard identification study.

The CCPS guidelines describe a number of primary components within Consequence Analysis, as follows:

- Source term / discharge modelling, describing the behaviour of materials as they are released from containment.
- Dispersion modelling, to analyse the movement of the material through the environment (usually considering the spread of gases or vapours through the atmosphere).
- Fire and explosion modelling, to determine the hazard potential of releases of flammable materials in terms of thermal radiation and blast overpressure.
- Effect modelling, to convert gas concentrations, thermal radiation fluxes or blast overpressures into effects on people or structures.
- Mitigation factors, to study the effect of mitigation measures (such as sheltering or evacuation) on the effects predicted.

A flow diagram is presented which illustrates the range of consequences that typically might be considered within a QRA. his is shown in Figure 4 below (CCPS 1989).

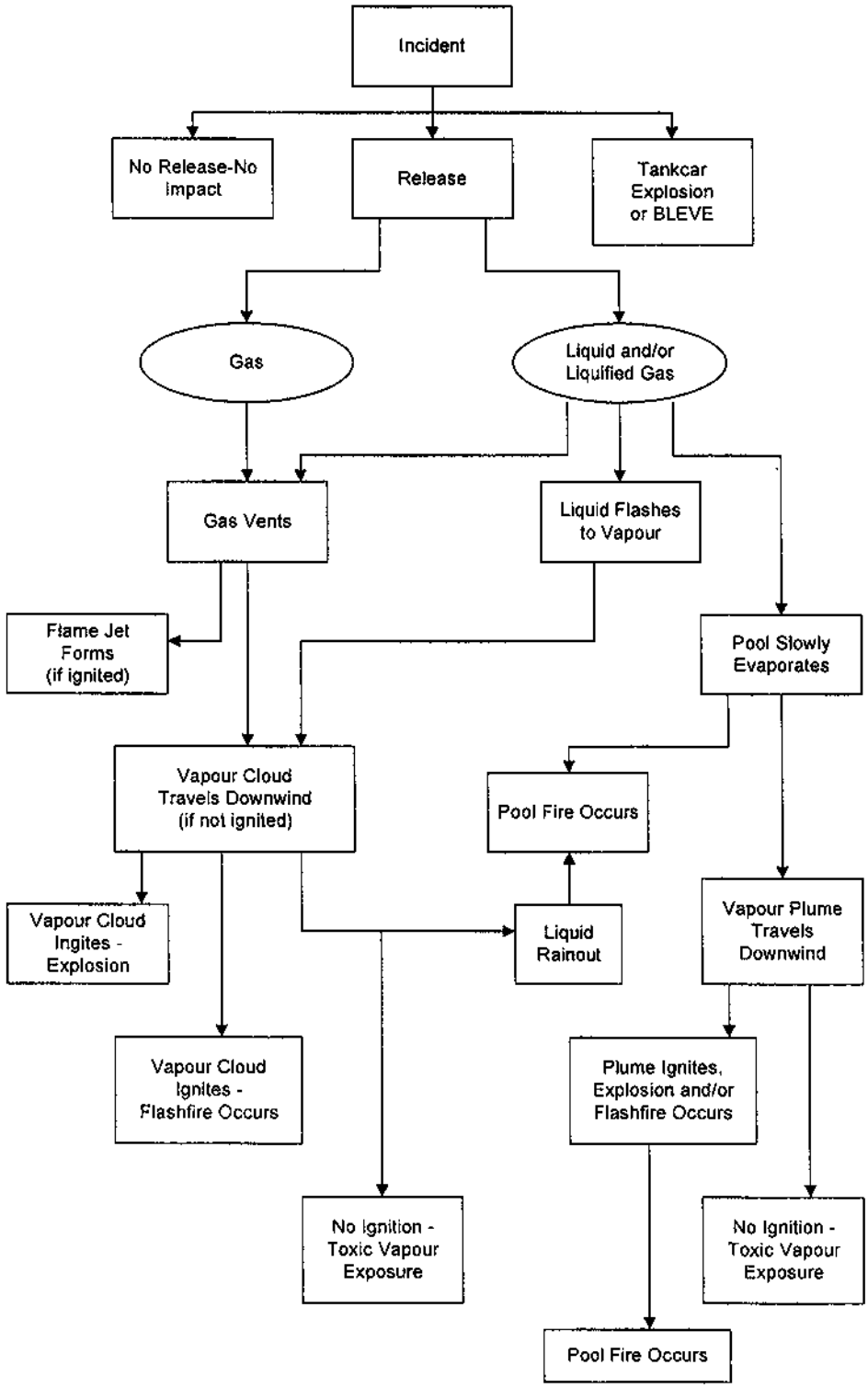

Figure 4
Typical spill event tree showing potential incident outcomes

The starting point for the source term / discharge modelling is to define the conditions (temperature, pressure, composition, phase) to which the material is subjected at the time that the release occurs. From this point of view, the CCPS guidelines define two different types of release:

- Emergency, engineered releases (e.g. – through pressure relief valves).
- Emergency, unplanned failures (e.g. – containment failures).

In the former case, the release conditions will normally be defined by the design parameters for the relief system. In the latter case, the release conditions are usually taken to be the normal process operating conditions at that point.

2.1.6 Frequency Analysis

The likelihood of each undesired event recognised at the hazard identification stage is estimated using Frequency Analysis. Both the British Standard and the CCPS guidelines describe three common approaches:

- Use of relevant historical data.
- Derivation of event frequencies using analytical or simulation techniques (such as fault tree analysis or event tree analysis).
- Use of expert judgement.

One particular type of historical data, generic failure frequency data, is commonly used in QRA studies and the implications of this are discussed in more detail in the next section.

2.1.7 Risk Estimation

As mentioned in the Introduction, risk is the chance of something adverse happening (HSE 1995). Risk estimation is therefore the combination of frequency (chance) and consequences (something adverse). There are numerous ways of presenting risk results, including:

- Risk indices (such as Fatal Accident Rate).
- Individual risk. Individual risk is defined as "the risk of some specified event or agent harming a statistical (or a hypothetical) person assumed to have representative characteristics" (HSE 1995). It may be related to a hypothetical individual, the most exposed individual or an individual in a particular worker group or at a particular location. It may be expressed as a point value, as a transect (a plot of individual risk against distance) or as contours overlaid on a map.
- Societal risk. Societal risk is defined as "the risk of widespread or large scale detriment from the realisation of a defined hazard" (HSE 1995). Typically, it expresses the frequency with which different numbers of people within a population could be affected It is commonly expressed in the form of an F-N curve, where F is the frequency with which N or more people are affected.

Since risk is a combination of frequency and consequences, the risk estimates produced will be influenced by the assumptions made and results produced at earlier stages in the process.

3. USE OF GENERIC FAILURE DATA IN QRA

Use of historical data in Frequency Analysis may take place at the event level (e.g. – the frequency of large fires in a particular type of process unit) or at the component failure level (e.g. – the frequency of leakage from pipes). In either case, the data should be appropriate to the system under consideration. Derivation of event frequencies from historical data requires sufficient and accurate records drawn from a population large enough to lend the data statistical significance.

In the ideal case the failure frequency data would be collected from the plant under investigation. Such data would be specific to the equipment present and would reflect the practices, environmental factors and other influences at that particular site. However, in reality, specific data satisfying QRA requirements are not usually available. The population (in terms of the number of equipment items and the period of observation) is often inadequate to develop failure frequencies with any degree of statistical significance. Resort may then be made to generic failure data, which are drawn from records of failures across different plants, process environments and equipment types.

Generic data, whilst representing a loss of specificity relative to single plant data, provide a greater pool of records and population of equipment experience upon which to base frequency estimates. There are a number of assumptions inherent in the use of generic data (CCPS 1989, IAEA 1998):

- Completeness: That all events of relevance are contained within the historical record (i.e. that there has been no under-reporting).
- Relevance: That the population from which the incidents are drawn is appropriate.
- Significance: That the population from which the incidents are drawn is sufficiently large for the data to be statistically significant.
- Inclusiveness: That the record of reported occurrences includes all of the significant failure causes for the system under investigation (such as human factors, management systems etc.).

Two of these assumptions, relevance and inclusiveness, are discussed further below.

3.1 RELEVANCE

As mentioned above, the use of generic failure frequency data represents a loss of specificity. The generic data may be regarded as an average across different operating environments, processes, management systems etc.

However, in a particular QRA study, the system under investigation may be considered to differ from the 'average' in certain respects, which would influence the frequency of events. For example, the process fluids may be relatively benign, presenting fewer corrosion problems. The management of safety might be considered to be particularly poor, indicating that events would be more likely than the average. In order to address such perceived differences (i.e. – in an attempt to re-introduce a level of specificity), the generic failure frequencies may be subjected to adjustment factors (CCPS 1989).

Adjustment factors may be applied in one of two ways:

1. To the overall generic figure, as a multiplier or series of multipliers.
2. To each specific contributor to the overall generic figure.

The first of these methods is applied as follows:

$$\lambda_A = \lambda_G \prod_{i=1}^{n} f_i$$

Where:

λ_A	=	Adjusted failure frequency
λ_G	=	Generic failure frequency
f_i	=	Adjustment factor i (i=1 to n)
n	=	Number of adjustment factors that apply

The CCPS guidelines give, for illustrative purposes, a set of factors which are in turn taken from Du Pont's Process Safety Management Reference Manual (Du Pont, 1987). The factors are reproduced below in Table 2.

Table 2
Generic failure rate adjustment factors

Equipment failure rate influences	Adjustment factors	
	Instruments	Valves
Process medium factors		
Corrosion	1.07	1.14
Erosion	1.14	1.28
Fouling, plugging	1.07	1.14
Pulsating flow	1.14	1.07
Temperature extremes	1.07	1.07
External environmental factors		
Vibration	1.42	1.21
Corrosive atmosphere	1.21	1.21
Dirty atmosphere	1.07	1.07
High temperature and/or humidity	1.07	1.07
Location factors		
Exposed mechanical damage	1.07	1.07
Inaccessible for inspection	1.07	1.07

In the second of the two methods, the generic failure frequency is broken down into a set of contributors. The example given in the CCPS guidelines is of pipeline leakage frequency, which may be broken down into contributions from material defects, corrosion, external impact, natural hazards and other causes. For each contributor, a factor is then determined (usually on the basis of expert judgement), the value of which depends on whether the system under analysis is considered to be 'better' or 'worse' than the average. Each contribution is then multiplied by the corresponding factor and the products summed to give a revised failure frequency.

The adjustment of generic frequencies to account for differences in human factors and safety management systems has been an area of particular research interest on the part of the Health and Safety Executive (Hurst et al. 1991, Hurst 1991, Bellamy et al. 1989, Anderson, M and Gould, J H 1997, Gould J H and Anderson, M 2000) and others (Pitblado et al., 1990).

The HSE research (Bellamy et al. 1989, Hurst et al. 1991, Hurst 1991) examined the contribution made by human and sociotechnical errors to failure frequencies for pipes and pressure vessels. A classification scheme for failures was developed and used to analyse recorded incidents of equipment failures. This scheme included direct (immediate) causes of

failure (e.g. – operator error), the origins of the failure (basic or underlying causes, e.g. – bad design) and failure to take preventative action to recover unsafe conditions (e.g. – task checking not carried out).

The research considered records of over 900 incidents of pipe failures, of which approximately 500 gave sufficient information for the analysis to be conducted. In the case of pressure vessel failures, records of 230 incidents, where the immediate causes were known, were considered. The results are summarised in Table 3 below (Hurst 1991).

Table 3
Summary of pipework and vessel failure data showing main causal contributions as a percentage of known contributions

Description	Pipework	Vessels
Human contribution to direct cause of failure	41%	32.8%
Known direct causes	Operating error (30.9%)	Overpressure (45.2%)
	Overpressure (20.5%)	Operating error (24.5%)
	Corrosion (15.6%)	Temperature (11.2%)
Major underlying cause of failure	Maintenance (38.7%)	Operating (32.0%)
	Design (26.7%)	Design (29.5%)
	Operating (13.7%)	Maintenance (22.2%)
Major recovery failure (preventive mechanism)	Human factors (29.5%)	HAZOP (37%)
	HAZOP (25.4%)	Human factors (30.2%)
	Checking (24.4%)	Not recoverable (13.5%)
Matrix analysis (combination of underlying cause / preventive failure	Design/Hazard Review (24.5%)	Design/Hazard Review (29.0%)
	Maintenance/human factors (14.5%)	Operations/human factors (24.5%)
	Maintenance/checking (12.7%)	Domino/non-recoverable (11.9%)

The authors suggest that adjustment factors could be applied to generic failure rates in order to account for human and sociotechnical influences at a particular site. They also proposed that such adjustment factors could be linked to the results of audits, particularly audits that are structured to reflect the hierarchy of causes.

The use of safety management audit results to modify generic failure frequencies was considered further in the development of the MANAGER technique (Slater 1988, Pitblado et al. 1990). Initially, the structure and content of the MANAGER questionnaire was influenced by the concept of Performance Shaping Factors (PSFs). These factors are routinely used in human factors studies in a range of industries. They are those influences that are present in the design, operation and human interaction in complex technological systems. Subsequently, the questionnaire was restructured to provide greater emphasis on established loss prevention (safety management) principles whilst retaining the human factors influences. The scoring system was also revised. This scoring system is used to generate a 'management factor', which is applied to the generic failure frequencies used in a QRA. Pitblado et al. (1990) reported that, at that time the technique had been used on around 30 occasions. The management factors obtained ranged between 0.5 (best) and 8.0 (worst), a range of 16. A case study describing the application of the tool is presented by Pitblado (1996).

In research carried out under the CEC Environment Programme 1993-94 and described by Hurst et al. (1996), a safety attitude survey questionnaire (SAQ) and a process safety

management audit tool (called PRIMA) were applied at six major hazard sites located in four European countries. The tools provided quantitative measures of safety attitudes and safety management system performance respectively. One of the outputs of the PRIMA tool was a 'modification factor', which could be applied to generic failure frequencies for use in a QRA. Modification factors were calculated for each of the sites involved in the study. It was found that there was a poor correlation between the modification factor obtained from PRIMA and either Lost Time Injury (LTI) or Loss of Containment Rate (LCR) data for the site concerned. This was judged to be due to the poor quality of the LTI and LCR data available. However, a good correlation was observed between the PRIMA modification factors and the self-reported accident rates (the percentage of respondents who reported being involved in an accident of any kind in the 12 months previous to the survey) as evaluated through the SAQ process.

The modification factor was defined as the ratio of the adjusted failure rate to the generic failure rate. For the sites studied the modification factors varied from 0.4 (best) to 6.6 (worst), a range of about 16.

3.2 INCLUSIVENESS

As mentioned above, in using generic failure frequency data it is assumed that the record of reported occurrences includes all of the significant failure causes for the system under investigation (such as human factors, management systems etc.). In order to test this assumption, generic failure data sources for pipework and pressure vessels have been studied. The data were also examined for information concerning the plant state at the time of failure. Where possible, primary sources were consulted. A number of these sources arise in industries other than the onshore process industry, but the data they present have nevertheless found use in onshore process QRA studies. The results are presented below.

3.2.1 Generic Failure Frequency Data for Pipework

General Electric Data

General Electric (GEAP 1964) obtained data on 399 failures prior to 1964 from a variety of installations, including electrical utilities and petroleum refineries. In total 94 companies took part in the survey. Approximately 74% of the 399 failures arose in the utilities industry.

Table 4 summarises findings of the study.

Table 4
Causes of piping failures

Primary cause of failure		No of cases	Cases total	Percent of total	% Total
Design	Mechanical fatigue	18		4.5	
	Expansion/flexibility	10		2.5	
	Section transition	2		0.5	
	Support	2		0.5	
	Design-operation (thermal fatigue)	32		8.0	
	Miscellaneous	9	73	2.3	18.3
Material Selection	Misapplication	9		2.3	
	Metallurgical - type 347 stainless steel	59		14.8	
	Metallurgical - graphitization	41		10.3	
	Metallurgical - stress rupture	5		1.2	
	Metallurgical - '885' embrittlement	2		0.5	
	Miscellaneous	4	120	1.0	30.1
Manufacturing	Wrong material supplied	5		1.2	
	Base material defects	31		7.8	
	Weld defects	1		0.3	
	Associated with welding	4		1.0	
	Miscellaneous	1	42	0.3	10.6
Fabrication - Erection	Weld defects	27		6.8	
	Associated with welding	10		2.5	
	Wrong material used	4		1.0	
	Miscellaneous	9	50	2.3	12.6
Operation - Service	Mis - operation	9		2.3	
	Thermal shock and shock	6		1.5	
	Corrosion and/or erosion	94	109	23.4	27.2
Unknown		5	5	1.2	1.2
Total		399	399	100	100

Of interest is the proportion of failures occurring in Operation-Service (27.2%). Only a small proportion of these failures arose from mis-operation (2%). This indicates that the level of human contribution to failures may have been smaller than that observed by Hurst (1991, see Table 3). This may be because the data arise predominantly from the utilities industry as opposed to the process industry.

WASH-1400 Data

The report (USNRC 1975), known as the Reactor Safety Study, presents data on leaks from pipes on the 17 US nuclear plants operating in 1972.

The Reactor Safety Study is a report describing the estimated accident risks to the public from commercial nuclear power plants of the type then in use. The study compares the estimated risks from nuclear power plants to those which result from other man caused and natural events.

The pipe rupture assessments were obtained from examination of nuclear data sources, industrial data sources and a number of other data sources. Various pipe sizes were included in the evaluations and the rupture data were categorised into different sizes. In general, the

basic pipe data could be broken into two general categories, ruptures occurring in pipes less than 4" in diameter and ruptures occurring in pipes having diameter greater than 4". Ruptures were categorised as major leaks or severance. Minor leaks were not included in the assessment of ruptures.

The report contains much quantitative data on failure rates and breakdowns of failure modes with corresponding failure rates. However, failure causation is not given.

GRI Data

These data are based on a survey of LNG plant operators and were compiled for the US Gas Research Institute. There were only 2 reported incidents of cryogenic piping failure, both due to poor quality welds at branch connections.

This source was not examined further.

HSE Onshore Data

Piping failure frequency data are reported by Pape & Nussey (1985). The frequencies are said to be based on aggregated data from several sources, modified by judgement. No breakdown of the data is provided.

HSE Offshore Data

The HSE (1997) hydrocarbon release database covers a total of 257 leaks from process pipes on offshore platforms in the UK Sector over the period October 1992 to March 1997. The raw data are contained in a database that is confidential to the HSE and contributing operators. Although the data are offshore and not onshore related, the report does give some useful information on the causes of failures.

Table 5 shows a summary of the reported data.

Table 5
Summary of failure causation data found in HSE (1997)

Causation factors		Totals	
Design Fault			180
Equipment Failure	Corrosion/Erosion	145	726
	Mechanical defect	485	
	Material defect	48	
	Other	48	
Operational Fault	Incorrectly fitted	153	636
	Improper operation	274	
	Dropped/Impact	21	
	Left open/Opened	126	
	Other	62	
Procedural Fault	Non-compliance	124	356
	Deficient procedure	217	
	Other	15	
Operating Mode in Area at Time of Accident	Drilling/Well operation	106	1097
	Normal production	496	
	Shutdown/Blowdown	83	
	Pig/Flush/Clean/Inspect	47	
	Maintenance/Construction	99	
	Testing/Sampling	45	
	Reinstatement/Start-up	221	
Total No. of Releases		1097	

The assignment of multiple causes to incidents makes comparison with other data sources difficult. However, the large numbers of incidents having causation factors such as 'Improper Operation' indicates the importance of human error.

Also of interest is the distribution of failures according to Operating Mode. Approximately 45% of the failures were reported as occurring during normal operation, with the remainder occurring during various activities, particularly Reinstatement / Start-up, Drilling / Well operation and Maintenance / Construction.

Blything & Parry (1988)

Historical incident data were gathered from different sources and classified into four plant categories: Chemical, Refinery, Nuclear and Steam. The incident data were analysed to determine failure cause and root causes. Failure cause was defined as the principal mechanism responsible for failure. Root cause was defined as the principal activity responsible for initiating failure. The report gives a detailed breakdown of each plant category and the number of plants involved in the survey. The authors describe the information presented as being indicative and not statistically significant.

Table 6 shows a summary of the mechanical failures for the five chemical plants and Tables 7 to 9 summarise the failure cause and root cause for each plant category. Human error was identified as a dominant factor in many failures. These errors occurred across a range of functions, including design, installation, operation and maintenance.

Table 6
Summaries of mechanical failures for the chemical plant category

	No.	Proportion (%)
Weld failure	45	33.1
Stress rupture	30	22.1
Bending stress	2	1.5
Fatigue	3	2.2
External load	4	2.9
Bellows failure	3	2.2
Valve failure	27	19.9
Seal failure	15	11.0
Miscellaneous	7	5.1
Total	136	100

Table 7
Root cause - failure cause matrix table for all CHEM data sources

Root Cause \ Failure cause	Corrosion (external)	Corrosion (internal)	Corrosion (stress)	Erosion	Restrained	Vibration	Mechanical	Material	Freezing	Thermal fatigue	Water ammer	Work systems	Unknown	Un specified	Totals	%
Design	17	14	15	2		8	23	3	10	2	2	6		1	103	28.7
Installation	4	1		1	2	1	9	7	1	1	1	4		1	33	9.2
Design/installation		2	1		4	3	4	9			1				24	6.7
Operation	2	1				1	11		2	1	4	18		3	43	12.0
Maintenance	4	1		1			11	4				34		3	58	16.2
Manufacture		1					15	1		1					18	5.0
Unknown							2						9		11	3.1
Unspecified	1	3				1	21	5	1	1		2	1	33	69	19.2
Total	28	23	16	4	6	14	96	29	14	6	8	64	10	41	359	100

Table 8
Root cause - failure cause matrix table for all REFIN data sources

Root Cause \ Failure cause	Corrosion (external)	Corrosion (internal)	Corrosion (stress)	Erosion	Restrained	Vibration	Mechanical	Material	Freezing	Thermal fatigue	Water hammer	Work systems	Unknown	Un specified	Totals	%
Design	1	42			1	1	5	2	3						55	27.9
Installation	4						1								5	2.5
Design/installation							1	1				36		13	51	25.9
Operation										1		29			30	15.2
Maintenance							1					15			16	8.1
Manufacture							3	1							4	2.0
Unknown													20		20	10.2
Unspecified								16							16	8.1
Total	5	42	0	0	1	1	11	20	3	1	0	80	20	13	197	100

Table 9
Root cause - failure cause matrix table for all STEAM data sources

Root Cause \ Failure cause	Corrosion (External)	Corrosion (internal)	Corrosion (stress)	Erosion	Restrained	Vibration	Mechanical	Material	Freezing	Thermal fatigue	Water hammer	Work Systems	Unknown	Un specified	Totals	%
Design		16	5	13	2	7	11	3	1	7					65	32.2
Installation						1	6					2			9	4.5
Design/installation					2							1			3	1.5
Operation		14		53			4				2				73	36.1
Maintenance							1								1	0.5
Manufacture		1	1	1			22	14		3				4	46	22.8
Unknown							1						4		5	2.5
Unspecified															0	0
Total	-	31	6	67	4	8	45	17	1	10	2	3	4	4	202	100

3.2.2 Generic Failure Frequency Data for Pressure Vessels

As with the pipework data, a number of primary data sources have been reviewed. The details are presented below.

HSE Offshore Data

The HSE (1997) hydrocarbon release database covers a total of 37 leaks from pressure vessels on offshore platforms in the UK Sector over the period October 1992 to March 1997. The published report presents leak frequencies for 14 different types of vessels, but no summary information. The raw data are contained in a database that is confidential to the HSE and contributing operators. Information on pipework failure causes is presented in ***GIR Data***. Failure causes specific to pressure vessels are not discussed in the document.

Davenport (1991)

Previous surveys carried out jointly by the Safety and Reliability Directorate (SRD) and the Associated Offices Technical Committee (AOTC) have been reported by Smith and Warwick (1981, 1974) and Phillips and Warwick (1967). This reference source is based on a later series of data and reports on data for a survey carried out over a five year period from 1983 to 1988.

A breakdown of the population figures for the individual vessel categories is shown in Table 10.

Table 10
Average population figures over 5 year period of survey

Vessel type	Number of Vessels	%
Boilers	28800	8.0
Steam receivers	24840	6.9
Air receivers	260280	72.3
Other pressure vessels	46080	12.3
Total	360000	100

A summary of the failure statistics, broken down by both vessel and failure type, is given in Table 11. A total of 92 failures were identified in the survey.

Table 11
Number of failures for vessel and failure type

Vessel Type	Failure Type					
	Inspect	Leakage	Deformation	Disruptive	Total	%
Air receivers	21	12	2	2	37	40.2
Steam receivers	19	5	6	0	30	32.6
Boiler	10	6	0	0	16	17.4
Other vessels	2	3	2	2	9	9.8
All vessels	52	26	10	4	92	100

Inspect: Potential failure resulting in no release of contents.
Leakage: Potential failure resulting in release of small amount of contents.
Deformation: Catastrophic failure resulting in gross distortion of vessel, with or without release of contents.
Disruptive: Catastrophic failure resulting in forcible release of contents.

Fatigue and corrosion both dominated the causes of inspection failure. Fatigue alone was the major cause of leakage failure, accounting for 65% of cases. 'Maloperation' only appears to have given rise to failures in the two catastrophic failure categories (deformation and disruption).

3.2.3 Smith & Warwick (1981)

Smith & Warwick (1981) includes a detailed list of events/failures from which Table 12 to Table 14 were compiled.

The data have been gathered from three five-yearly surveys covering the 100300 vessel years of the first survey 1962-1967, 105400 vessel years of the second survey 1968-1973 and 104320 vessel years since 1973. Some 20000 pressure vessels have been reviewed and it is their service experience which formed the basis of this report.

The type of plant selected for inclusion in the survey included:

- Welded or forged unfired pressure vessels and boiler shells and drums not subjected to flame impingement, above 9.5mm thick with a stipulated working pressure in excess of 725 kpa and constructed to the Class 1 requirements of recognised design codes.
- An age range of less than 40 years.
- Plant in which unrepaired defects are being monitored during service.
- Some pipework built to comparable pressure vessel standards, but not related to the total pipework involved.

A breakdown of the types of vessels considered in the survey is not given, although inspection of Table 1 of the report indicates that most were for steam / water service.

The two categories of failures were defined as follows:

- Catastrophic - this implies destruction of the vessel or component, or a failure so severe as to necessitate major repair, or replacement.
- Potentially dangerous - this is a defect, which requires remedial action where continued working conditions could result in a dangerous extension to the defect.

The survey reviews experience from conventional plant in the UK and from similar plant registered with the National Board of Boiler and Pressure Vessel Inspectors (NBBPVI) in the USA. Reference is also made to typical defects in both UK and USA nuclear plant. A more detailed breakdown of vessel service is not given.

The distribution of failures by cause and number for the period 1962-1978 is listed in Table 12.

Table 12
Causes of failures

Cause	No. of Cases	%
Crack propagation	216	94.3
Defects existing prior to commissioning	5	2.2
Corrosion	1	0.44
Mal-operation - human error etc.	3	1.31
Creep	3	1.31
Not ascertained	1	0.44
Total	229	100

Distribution of causes of cracks is shown in Table 13.

Table 13
Causes of cracks

Cause	No. of cases	%
Fatigue	52	24
Corrosion	30	14
Defects existing prior to service	63	29
Not ascertained	61	28
Miscellaneous (creep, mal-operation etc.)	10	5
Total	216	100

Inspection of vessels covered by the survey usually consisted of a visual examination with non-destructive examination (NDE) techniques being adopted when it was considered necessary. This is reflected in Table 14 showing the numbers of failures and the method by which they were found:

Table 14
Method of detection

Method	No. of cases	%
Visual inspection	88	38
NDE	49	21
Leakage	76	33
Hydro test	3	2
Catastrophic (in service)	13	6
Total	229	100

Hence the majority of failures (61%) were identified during the inspection process, presumably when the vessel had been taken out of service. In-service failures constituted the remaining 39%. Therefore, on the basis of the information presented, it is difficult to make any observations concerning the plant state at the time of the failure.

3.2.4 Bush (1975, 1988)

The American Boiler Manufacturing Association survey reported by Bush (1988) obtained responses covering 15% of registered pressure vessels in the USA. There is no failure cause information arising from this survey. In his earlier work (Bush 1975) failure cause was dealt with in more detail.

Some information on failure causes, which was taken from Kellermann & Seipal (1967) was presented and is summarised in Table 15.

Table 15
Failures in pressure vessels

Causes of failure	Total reported	%
Design	101	18.5
Safety devices design	33	6.0
Safety devices operation	76	13.9
Material	67	12.2
Manufacturing	55	10.1
Ageing	11	2.0
Stress corrosion	16	2.9
Overload	52	9.5
Corrosion inside	63	11.5
Corrosion outside	17	3.1
Vibrations	56	10.2
Total	547	100

3.2.5 Arulanantham & Lees (1981)

Arulanantham & Lees (1981) presented a survey of failures of pressure equipment in a plant handling toxic chemicals (Plant E) and 4 olefins plants (Plant A, B, C, and D) at a single works during the period 1950-80. It covered a population of 16000 pressure vessel years of all types. Tables 3.15 to 3.19 show various data from this source. Pressure vessels included in the survey were process pressure vessels, pressure storage vessels and heat exchangers. The data were then used to estimate failure frequencies. Information on causes of failure is relatively limited.

Failure was defined as a condition in which a crack, leak or other defect has developed in the pressure containing components of the vessel so that repair or replacement of the vessel is required.

Table 16
Pressure equipment failure rates: all equipment on all plants

Vessels	Plant	Number at risk	Service (vessel years)	Number of failures	% Number of failures for vessel type
Process pressure vessels	A	80	1360	1	1.8
	B	59	678.5	10	17.9
	C	159	2385	1	1.8
	D	117	1111.5	3	5.4
	A-D	415	5535	15	26.9
	E	131	1572	41	73.2
	A-E	546	7107	56	100
Pressure storage vessels	A	-	-	-	-
	B	-	-	-	-
	C	2	30	-	-
	D	2	19	-	-
	A-D	4	49	-	-
	E	1	12	-	-
	A-E	5	61	-	-
Non-pressure storage vessels	A	10	170	-	-
	B	8	92	-	-
	C	9	135	-	-
	D	9	85.5	-	-
	A-D	36	482.5	-	-
	E	42	504	1	100
	A-E	78	986.5	1	100
Heat exchangers	A	96	1632	3	30
	B	84	966	2	20
	C	150	2250	3	30
	D	116	1102	2	20
	A-D	446	5950	10	100
	E	95	1140	-	-
	A-E	541	7090	10	100
Fired heaters	A	5	85	36	19.9
	B	5	57.5	36	19.9
	C	10	150	34	18.8
	D	15	142.5	75	41.4
	A-D	35	435	181	100
	E	1	12	-	-
	A-E	36	447	181	100

Plants A, B, C, D, and E had service lives of 17, 11.5, 15, 9.5 and 12 years, respectively, at the time of the survey.

Table 17
Effect of operating conditions on failure rates of pressure equipment: all equipment

Operating conditions	Plant	Number at risk	Service (vessel years)	Number of failures
High temperature	A	18	306	39
	B	17	195.5	36
	C	31	465	36
	D	27	256.5	76
	A-D	93	1223	187
Low temperature	A	34	578	-
	B	32	368	1
	C	41	615	-
	D	40	380	2
	A-D	147	1941	3
Other	A	124	2108	1
	B	92	1058	11
	C	233	3495	2
	D	150	1425	2
	A-D	599	8086	16
Unknown	A	15	255	-
	B	15	172.5	-
	C	25	375	-
	D	42	399	-
	A-D	97	1201.5	-
High temperature	E	17	204	7
Vessel in corrosive duty	E	45	540	21
Vessel subject to stress corrosion	E	49	588	12
Other	E	82	984	2
Unknown	E	77	924	-

Table 18
Effect of operating conditions on failure rates of pressure equipment: process pressure vessels

Operating conditions	Plant	Number at risk	Service (vessel years)	Number of failures
High temperature	A-D	22	326	1
Low temperature	A-D	53	666	1
Others	A-D	340	4543	13
Total	A-D	415	5535	15
High temperature	E	12	144	7
Corrosion	E	39	468	21
Stress corrosion	E	29	348	12
Other	E	51	612	2
Total	E	131	1572	41

Table 19
Effect of operating conditions on failure rates of pressure equipment: heat exchangers

Operating conditions	Plant	Number at risk	Service (vessel years)	Number of failures
High temperature	A-D	36	462	5
Low temperature	A-D	94	1275	2
Others	A-D	316	4213	3
Total	A-D	446	5950	10
High temperature	E	-	-	-
Corrosion	E	5	60	-
Stress corrosion	E	19	228	-
Other	E	71	852	-
Total	E	95	1140	-

Table 20
Causes of failure of pressure equipment

Cause of failure	Plant	Proportion of failures (%)
Cracks	A	78
	B	75
	C	71
	D	85
	A-D	79
	E	38
Corrosion	A	10
	B	17
	C	26
	D	5
	A-D	13
	E	52
Maloperation	A	-
	B	2
	C	-
	D	2.5
	A-D	1
	E	10
Creep	A	12
	B	6
	C	3
	D	7.5
	A-D	7
	E	-

3.3 DISCUSSION

On the basis of the survey, some comments on the data sources examined are presented in Table 21.

Table 21
Comments on sources of generic frequency data

Equipment item	Source	Comment
Pipes	GEAP 1964	74% of the failures analysed occurred in the utilities industry. Only 7.5% were from petroleum refineries and there were none from the chemical industry.
	USNRC 1975 (WASH 1400)	Data from pipe leaks on US nuclear power plants.
	Pape and Nussey (1985) (HSE Onshore)	Basis unknown.
	HSE 1997 (HSE Offshore)	Leaks from process pipes offshore.
	Blything and Parry 1988	Range of industries considered including chemical and refinery. Data indicative and not statistically significant.
Pressure Vessels	Davenport 1991	More than 87% of the vessels considered were air receivers, steam receivers or boilers.
	Smith and Warwick 1981	Survey based on Class I pressure vessels in premises subject to the Factories Act. Proportions of different vessel types are not given, but majority appear to have been for steam / water service.
	Arulanantham and Lees 1981	Survey based on a variety of vessels in olefins plants and a plant handling toxic chemicals. The number of vessel-years of experience covered was considerably less than either Davenport (1991) or Smith and Warwick (1981).

It was found that few of the sources consulted contained information of direct relevance to the onshore process industry. Data sources which draw predominantly on information collected on equipment in steam, water or air service are unlikely to include some of the failure causes which are of concern within the onshore process industry. Hence there is a strong possibility that should these generic failure frequency data be used in a QRA, the assumption that all relevant failure causes will be 'included' in the generic frequency would be incorrect.

A number of sources (including Blything & Parry 1988, HSE 1997) have indicated the importance of the human error-related element of the frequency data. This corresponds with the findings of Hurst (1991). The occurrence of human error is clearly influenced by the quality of safety management and other performance shaping factors, many of which are specific to the system under study. Attempts to address this within QRA by application of modification factors have been reported (Pitblado et al. 1990, Hurst et al. 1996). Hurst et al. identified a correlation between the modification factor derived from an auditing tool and self-report accident rates as obtained from safety attitude surveys at six European major hazard sites.

Information on the plant state at the time of failure is sparse. However, where it is given (HSE 1997) it indicates that failures occurring during 'non-standard' conditions (maintenance, start-up etc.) form a significant proportion of the total (perhaps 50% or more).

4. UNCERTAINTY AND QUALITY IN QRA

As the use of QRA in various fields increased, concern was expressed about the uncertainties present in the various methods used at each stage of a study (see for example Okrent et al. 1982). As stated in the introduction, uncertainty in QRA can take various forms. This study is concerned with the uncertainty associated with knowing which events or phenomena to attempt to model within a QRA. From the discussion in Section 2, it can be seen that within the overall QRA process, the Hazard Identification, Incident Enumeration and Incident Selection stages determine the content of the QRA, in terms of the events modelled. If the Hazard Identification stage is incomplete (in that it fails to identify all of the relevant hazards), then clearly the missing events will not be considered within the QRA. If the Incident Enumeration and Selection process fails to extract all of the relevant hazards from the hazard identification results, then, again, events will be missing from the QRA. Such issues have been studied under the broad heading of quality in QRA.

4.1 STUDIES OF THE QUALITY OF HAZARD IDENTIFICATION METHODS

Taylor (1982) evaluated the quality of a range of risk analysis (actually hazard identification) techniques in terms of their completeness and discrimination. The techniques studied were:

- A version of HAZOP.
- Action error mode analysis and cause – consequence analysis, aimed at identifying potential operator errors.
- Generic fault tree analysis.
- A commissioning review checklist.
- Action error mechanism analysis (similar to action error mode analysis but concentrating on the operator, rather than the machine interface).
- Automatic fault tree construction.
- A 'unit level' method of analysis used by an insurance company.

'Completeness' was defined as the extent to which a technique identifies all of the possible hazards in a system. Absolute 'completeness' was seen as being unlikely to be achieved in practice. The reasons for this were said to include:

- A lack of engineering or scientific knowledge.
- Errors or omissions in the conduct of the study.
- Deliberate exclusion of some hazards in order to reduce the effort involved.
- Limitations of the hazard identification technique used (i.e. – it may only be capable of addressing certain classes of hazard).

A number of practical measures of completeness were proposed. Historical completeness is defined as:

$$\text{Historical Completeness} = \frac{\text{Number of hazards identified by a particular method}}{\text{Number of hazards which can be identified from a list of case histories}}$$

One difficulty with this measure is that rare events may not be included within the available case histories. An alternative proposed was relative completeness, which is defined as:

$$\text{Relative Completeness} = \frac{\text{Number of hazards identified by a particular method}}{\text{Total number of hazards identified by all methods studied}}$$

The third measure of completeness suggested was to compare the hazards identified at the design stage with the problems identified during commissioning. All three measures were employed during the study.

Discrimination was described as the extent to which a given technique identifies hazards that can actually occur within the system under study. The example given is that of exothermic reaction runaway, which may be identified during an analysis. Whether or not runaway is actually possible will depend on a number of factors, such as that reaction kinetics, the rate of heat release and the cooling capacity available. To decide whether the hazard is 'real' would require further effort in the form of calculations or even experiments. Alternatively, the analysis team may make a judgement about whether or not the hazard can be realised within the system under investigation. The use of judgement introduces scope for error – hazards may be omitted wrongly, or hazards may be included which cannot be realised in practice. The following measure of discrimination was proposed:

$$\text{Discrimination} = \frac{\text{Number of hazards identified which can actually occur}}{\text{Total number of hazards identified}}$$

The desire for a high degree of completeness was seen to conflict with the desire for a high degree of discrimination. The experience of the analysis team was also recognised as a key factor in achieving a high level of discrimination.

The different techniques were applied to a batch distillation system and analysed for completeness and discrimination. The main conclusion of the study was that a thorough analysis (i.e. – a high degree of completeness) required a combination of hazard identification methods.

Further work by Taylor et al. (1986) proposed a 'design review approach' to safety assessment. This approach involves conducting a detailed, thorough analysis of 'standard' process units using a range of techniques (including HAZOP, action-error analysis, fault tree analysis, a design review and comparison with the accident record). When dealing with a new process unit, the experience gained from the detailed study (in the form of a question set or checklist) of the standard unit is used to assess the new unit. Where differences in design are found, the design of the unit could be changed to bring it in line with the 'standard', or the implications of the difference could be assessed in detail before making a decision. The method could be facilitated by use of a computer-based system. The method was found to work well, but limitations included a poor ability to identify complex interactions between process units and the fact that the method could only be applied to units which were reasonably close in design to the 'standard'.

Suokas (1985) studied a range of safety analysis (again, actually hazard identification) methods in terms of their reliability, validity and coverage. Reliability was described as an indication of the accuracy of a measurement. The reliability of the various techniques studied was tested by arranging for different analysts (or teams of analysts) to apply the same technique to the same object at different times. The reliability, or more specifically the inter-analyst reliability, was calculated by dividing the total number of hazards identified by a test person (or team) by the total number of hazards identified by all persons (or teams) during the test.

The concept of validity was discussed and described as having several meanings. Broadly speaking, validity expresses how well an instrument or method measures the property under analysis. Three 'types' of validity were discussed:

- predictive validity: for example, the capability of the method, when used at the design stage, to predict the risks associated with the system. alternatively, predictive validity could mean the ability of the method to estimate the effect of suggested safety improvements on the risk arising from the system studied.
- content validity: for example, the extent to which hazards and their contributors have been identified. content validity can be evaluated by comparing the information obtained from the analysis with information obtained from the accident record. it is therefore similar to the concept of historical completeness as defined by taylor (1982). this form of concept validity was then simply referred to as 'validity' throughout the study. alternatively, content validity may be determined by comparing the results of the analysis with the results yielded by other methods, when applied to the same object. this measure of content validity is therefore similar to the concept of relative completeness as defined by taylor (1982). this form of concept validity was also termed 'coverage' by suokas.
- construct validity: this is related to the concepts employed to interpret the analysis results. in the present context, construct validity could be interpreted as the relationship between safety analysis and accident theories, specifically the ability of the analysis method to identify factors influencing the accident process as described in accident theories.

The experiments conducted by Suokas focussed on the content validity ('validity' and 'coverage') of the methods studied.

A useful definition of quality in the context of safety analysis was also presented:

"The quality of a safety analysis can be expressed as its fitness for use...i.e. to what extent a safety analysis, including its boundaries, the assumptions employed and results achieved, satisfies the explicitly formulated goals and requirements relating to the intended use of the analysis."

The experimental work conducted by Suokas was divided into three studies. In the first, five analysis methods were applied to the same object in order to investigate the kind of information elicited by the different techniques. The second and third studies investigated the reliability, coverage and validity of two methods (Work Safety Analysis and HAZOP) in more detail.

The five analysis methods employed in the first study were:

1. Potential problem analysis (PBA).
2. HAZOP.
3. Action error analysis (AEA).
4. Work safety analysis (WSA).
5. Management oversight and risk tree (MORT).

The object was a liquor recovery plant.

It was found that PBA and HAZOP concentrated predominantly on hardware failures (failures in the physical sub-system – pumps, valves, pipes etc.) and identified hazards associated with contact with chemicals, excessive temperature or excessive pressure.

WSA also concentrated on the physical sub-system but tended to identify hazards that could be described as categorised as 'slips, trips and falls'. Furthermore, HAZOP tended to identify

hazards that could affect numbers of people whereas WSA tended to identify hazards which could affect only one person at any one time.

AEA identified hazards across a range of hazard types. MORT did not explicitly identify hazards, but did reveal deficiencies in the management and information sub-systems.

In summary, the findings of this first study supported those of Taylor (1982) in recommending that a combination of methods be utilised in analysing any given system.

The second study, focussing on WSA, used a number of operations associated with paper manufacturing machinery as the objects. The average inter-analyst reliability was around 0.6, but varied widely from analyst to analyst. The coverage of WSA, when employed alongside FMEA was 0.89. A comparison with the available accident record yielded a validity of 0.7. Some suggestions for improving the quality of WSA were made.

The third study, on HAZOP, consisted of a number of sub-studies. Firstly, the inter-analyst reliability was assessed by having two study teams analyse the same object (a treatment system for toxic waste). Secondly, the coverage of HAZOP relative to a number of other techniques (WSA, AEA and automated fault tree construction) was evaluated. Finally, HAZOP validity was determined by comparison with the available accident record. For the second and third sub-studies, the objects were a sulphur dioxide loading and storage facility, and an ammonia storage and unloading facility.

In the assessment of inter-analyst reliability, a reliability of 1 was obtained (i.e. – both teams identified the same hazards), although a comparison of the deviations identified which could lead to those hazards showed a lower reliability (of around 0.7).

In the second sub-study it was found that the coverage of HAZOP relative to the AEA and WSA methods employed was around 0.8. Again, HAZOP focussed more on hazards that could be classified as contact with chemicals or contact with excessive pressure. WSA in particular identified more hazards of the 'slips, trips and falls' type. HAZOP identified 77 accident contributors in total. AEA and WSA increased this figure by 23 new contributors. The new contributors identified only by AEA or WSA included items such as the opening or closing of valves, exchange of information between operators in the control room and the storage area and locking of rails to prevent inadvertent arrival of a train at the loading point.

Had the scope of the analyses been restricted to major releases of hazardous substances (i.e. – releases equivalent to or larger than those resulting from a ruptured loading arm or pipe), then the differences would have been slightly reduced. For such events HAZOP identified 27 accident contributors, AEA adding 5 new ones. Quantification of the results by fault tree analysis showed that the additional contributors provided by AEA increased the total frequency of major releases by 30-40%.

A comparison with relevant accident records (10 in total) obtained from the TNO FACTS database yielded a validity of 0.7.

The author notes that the numerical values of reliability, coverage and validity should be treated with caution since the numbers of test analysts and objects were small, as was the number of accident records available for comparison with the HAZOP findings. Overall, the study made a number of recommendations, including:

- The concept and content of safety analysis should be defined more explicitly, through the development of standards, for example.
- The analysis procedures used within the different methods should be defined more explicitly.
- Training of new analysts should include work on practical examples.
- The development of computer programmes (including expert systems) to assist in the analysis process.
- The use of several methods in the study of a given object.
- Monitoring and review of the analysis results once the study is complete (i.e. – the study should be regarded as 'living' and not a one-off exercise).

Later work by Suokas and Pyy (1988) evaluated the validity (as defined in Suokas (1985)) of hazard identification methods when compared with information derived from accident / incident investigations. Their report presents a useful cause-consequence diagram, first developed by Rouhiainen (1987), illustrating the sources of uncertainty within a risk analysis. This diagram is reproduced as Figure 5.

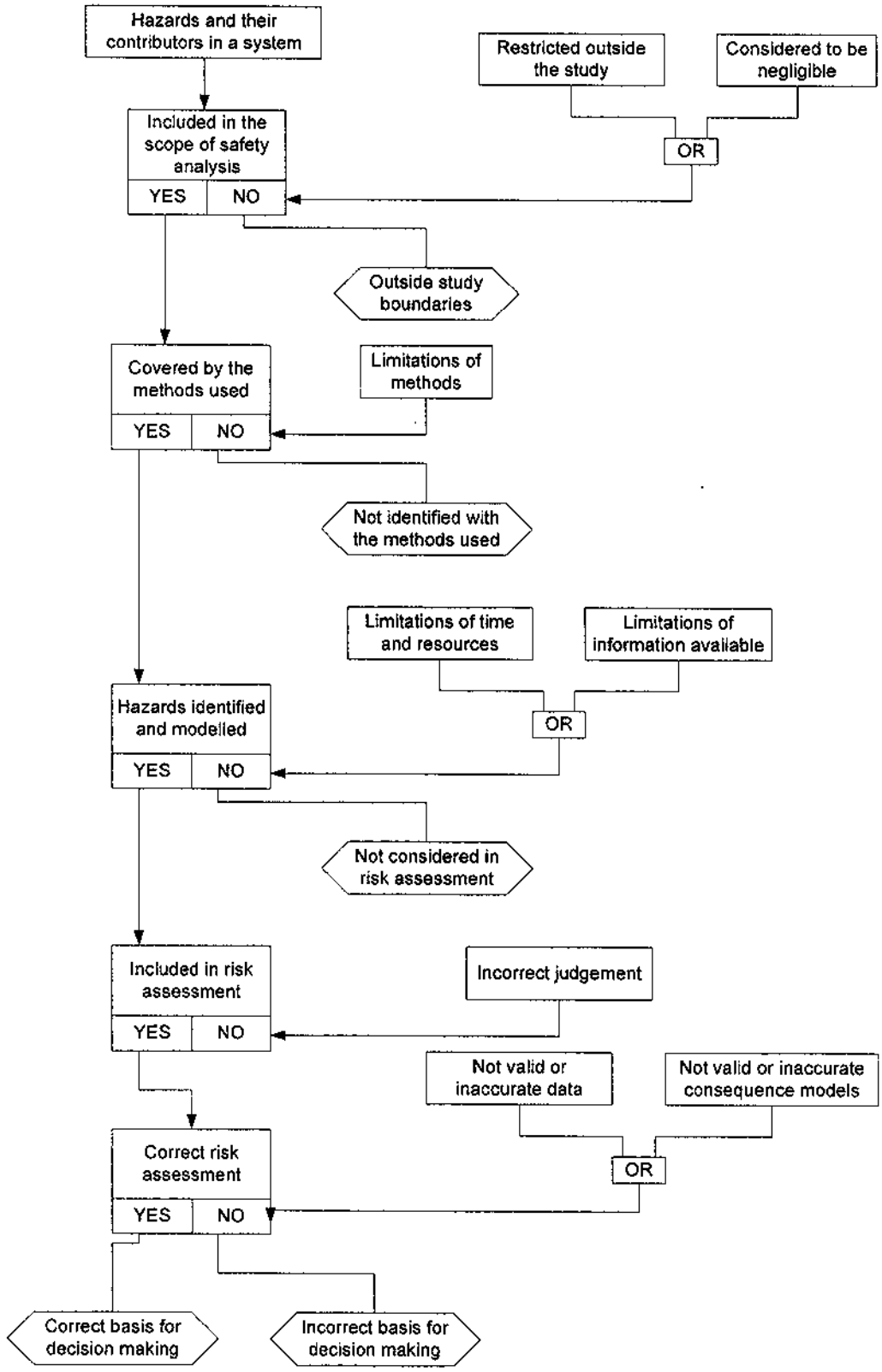

Figure 5
Main sources of uncertainty in a risk analysis

Information was collected regarding 51 incidents on seven process plants. Only a few of the incidents had resulted in any injury to personnel. The contributing factors to each of the incidents were determined by conducting interviews with shift supervisors, operators and other plant personnel. This information was supplemented by analysis of accident records obtained from the TNO FACTS database. This process identified a total of 157 contributors to the incidents / accidents studied.

Four hazard identification methods (HAZOP, AEA, FMEA and MORT) were then considered in turn. For each method, a judgement was made concerning whether or not a given accident / incident contributor (as identified above) fell within the scope of the search procedure used by that method. The analysis was performed independently, by different persons or teams.

It was found that, of the 157 contributors obtained from the accident / incident analysis, 56 fell within the search procedure of HAZOP, 33 within that of AEA, 26 within that of FMEA, and 10 within that of MORT. Some of the contributors fell within the search procedures of several methods. Overall, the methods were expected to identify 86 of the 157 contributors (a validity of 55%). The contributors not expected to be identified by the methods included those with a maintenance origin, human contributors and information / management factors.

When considering the contributors arising from different sub-systems, the validity was highest in the physical sub-system (66% overall). The kind of factors thought to be only occasionally covered or outside the scope of the methods were divided into three groups:

1. Material flow: particularly unexpected reactions or phenomena.
2. Common cause failures in the control and alarm system.
3. External factors (the example given being gas entering the air conditioning system).

The overall validity for contributors arising in the human sub-system was 49%. Contributors relating to operating tasks were well covered. Contributors relating to diagnosis of process state, considered to be an important area, were not. The most important group of contributors evaluated to be occasionally identified or not covered by the methods was associated with maintenance. However, the authors point out that this arose because the basis for the evaluation was application of the methods at a plant-wide level. Had the basis been application of the methods specifically to maintenance tasks, the validity would have been considerably higher.

Contributors belonging to the information and management sub-system were expected to be outside the scope of HAZOP, AEA and FMEA. MORT was expected to systematically cover a third of such contributors, with the remainder covered at a general level or only occasionally. Examples of the contributors only expected to be addressed occasionally were:

- Information exchange (e.g. – between shifts).
- Training and experience (e.g. – dealing with abnormal conditions).
- Wrong instructions.
- Integration of safety in operational decisions.

The authors concluded that:

- It is important to supplement site-wide analyses with more detailed studies of important human activities (such as maintenance) and technical sub-systems.
- The use of several methods to analyse the same object gives improved validity.
- There is a need to develop new approaches to cover some areas, such as analysing the diagnosis of process state.

Problem areas highlighted included availability of information to the analysis team (e.g. – for a new plant design, operator tasks and maintenance activities may not have been defined) and the treatment of batch operations.

The use of operational experience (including the findings of incident investigations) to complement safety analysis was recommended, as was the development of more user-friendly documentation of analysis results.

4.2 THE DEVELOPMENT OF TOOLS TO ASSESS THE QUALITY OF A RISK ANALYSIS

The usefulness of QRA results as an input to a decision-making process is strongly dependent on the quality of the analysis, a property that may not be immediately obvious from the QRA documentation. Rouhiainen and Suokas (1989) suggested that the quality problems associated with risk analysis could be summarised as three questions:

1. How well has the analysis identified hazards and their contributors?
2. How accurately has the analysis estimated the risks of a system?
3. How well are the results achieved in balance with the resources used?

In theory, an analysis could be said to have quality when it reflects reality. However, in the case of risk analysis, this is extremely difficult to measure. Hence the authors proposed that an analysis could be said to possess quality when:

- The insights or risk profiles produced reflect the appropriate use of safety analysis methods as well as the information about the plant and site.
- The resulting documentation clearly and accurately conveys the resulting insights and risk profiles as well as their bases.

Four different approaches for evaluating the quality of an analysis were identified:

- Carrying out a complete parallel analysis on the same system.
- Carrying out a parallel analysis on some parts of the same system.
- Comparing the analysis with experience, including descriptions of accidents which have occurred in similar systems and/or the system under consideration.
- Examining the process used to conduct the analysis.

The authors presented a chart illustrating the level of resource required by each of the four approaches. This is reproduced at Figure 6.

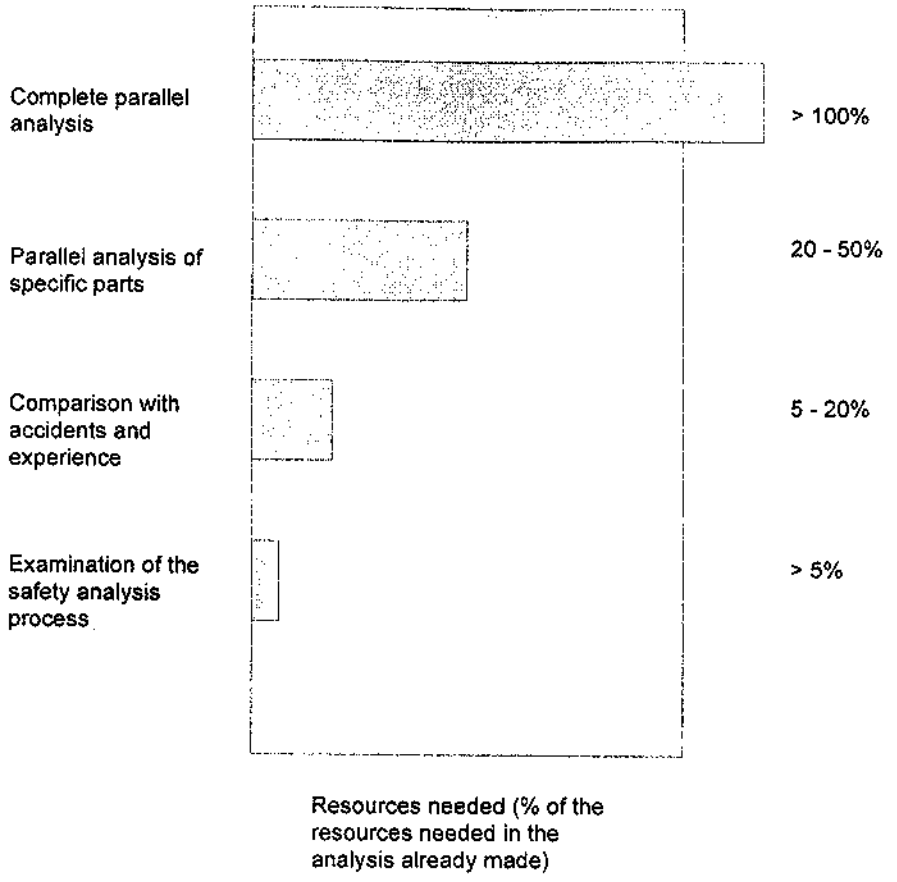

Figure 6
Comparison of resources required for the different approaches to the assessment of the quality of a safety analysis

An example of the first approach is the benchmarking exercise reported by Contini et al. (1991). The additional resources required are at least as great as those used to perform the original analysis.

The second approach has found use within the nuclear industry where probabilistic safety analysis (PSA) is used for licensing purposes. The additional effort required is less than that required to perform the original analysis, but may still be significant.

In terms of a comparison with information from accidents and incidents, the third approach has been utilised in a number of studies, including those described in the previous section. The resource requirements are less than those of the first two methods. However, problems include the lack of information on accidents in systems of interest, the lack of detail in accident reports and the fact that rare accidents may not be included within the available records.

A variation on the third approach was to compare the results of the analysis with the knowledge and experience of other experts, through a process of peer review. Evaluations of this type have been proposed within the nuclear sector (Garrick 1982, Apostolakis et al. 1983).

The fourth approach is analogous to evaluation of the quality policies and procedures of a supplier instead of testing samples of their product. It is the least demanding in terms of resources of all the approaches listed. The method developed by the authors falls into this category.

The method consists of a checklist, which may be used when scrutinising the documentation of a QRA that has been performed. Alternatively, and perhaps more usefully, the checklist may be applied by the analysts as the study progresses, as a form of quality assurance. The different sections of the checklist correspond to the different phases of a risk analysis. The method was then used to evaluate safety analyses that had been performed on the following systems:

- A new pulp manufacturing process.
- Storage and handling of chlorine in a chlorine plant.
- A pressure vessel in a nuclear power plant.
- An LNG storage facility.
- A chemical plant.
- A control room in a chemical storage area.

These studies revealed some deficiencies in the checklist, which was subsequently revised. A number of problems associated with the use of the checklist were identified, including:

- Familiarisation with the checklist on the part of the person conducting the assessment (the checklist was 23 pages long).
- The risk analysis documentation was not sufficiently detailed to allow completion of the checklist on the basis of a scrutiny of the documentation alone – discussions had to be held with the risk analysis teams.
- Collection of operational experience from the plant or relevant incident data (in order to validate the risk analysis) was time consuming and difficult. The amount of information available for validation remained quite limited.

The checklist approach for the evaluation of quality of a safety analysis was developed further (Rouhiainen 1990, 1992, 1993) and was designated QUASA (Quality Assessment of Safety Analysis). The QUASA method was used in a number of case studies. One of these studies (Rouhiainen 1990) involved an evaluation of the Canvey study (HSE 1978). The findings included a concern that a systematic means of hazard identification did not appear to have been employed. Hence the study may not have identified all relevant event sequences or dealt adequately with common-cause failures.

The section of the QUASA checklist dealing with identification of hazards contains questions to evaluate the extent to which abnormal plant conditions, management and human factors have been covered. The checklist also has sections relating to frequency analysis and consequence analysis. However, there is no section that deals explicitly with the process of incident enumeration and incident selection.

4.3 DISCUSSION

The review of the literature summarised above has highlighted a number of areas that are pertinent to this study:

- When compared with studies performed on the same system by other analysts, or when compared with information on accident contributors extracted from the available accident record, hazard identification studies are rarely capable of identifying all of the hazards present. This problem can be addressed, in part, by performing two or more studies of the same system using different, complementary techniques. In some cases the accident contributors that remain unidentified can still be significant. Hazards and accident scenarios that escape identification will subsequently be omitted from the latter stages of the QRA, resulting in an underestimate of risk.
- The hazard identification techniques studied were shown to be particularly weak in addressing certain areas. These included the exchange of information (between shifts or between operators at different locations) and the diagnosis of the plant state.
- Hazard identification studies carried out on a 'plant wide' basis or at a high level should be supplemented by more detailed investigations of particular operator actions such as maintenance tasks.
- Several approaches have been proposed for addressing these problems, including benchmark studies involving repeating all or part of a given analysis, comparisons with accident experience, peer review and subjecting the analysis process to quality assurance through the use of checklists. The last of these approaches is thought to be the least resource intensive.
- The published version of the QUASA checklist (Rouhiainen 1990) is quite comprehensive, but does not deal explicitly with the process of incident selection and enumeration.

5. QRA STUDIES

Published onshore process industry QRA studies have been examined to determine how the methodology outlined in Section 2 has been applied in practice.

5.1 CANVEY ISLAND

The Canvey study was carried out by the UKAEA Safety and Reliability Directorate, on behalf of the Health & Safety Executive. The study was performed in two stages. Following the original report (HMSO 1978) further work was commissioned which utilised a revised methodology and reflected improvements to plant, equipment and methods of operation which had been made since the original study was completed (HMSO 1981).

The Canvey complex consisted of a number of installations:

- A LNG terminal.
- Storage of petroleum products.
- Storage of a wide range of toxic and flammable substances.
- Two oil refineries.
- A terminal for filling of LPG cylinders.
- An ammonium nitrate plant.
- Trans-shipment of explosives.

The study was initiated following a public inquiry into the possible revocation of planning permission for the development of a further oil refinery in the area. The terms of reference for the study were:

> *'In the light of the proposal by United Refineries Limited to construct an additional refinery on Canvey Island, to investigate and determine the overall risks to health and safety arising from any possible major interactions between existing or proposed installations in the area, where significant quantities of dangerous substances are manufactured, stored, handled, processed and transported or used, including the loading and unloading of such substances to and from vessels moored at jetties; to assess the risks; and to report to the Commission.'*

The focus of attention was therefore on accidents where a serious loss of containment could result in production of large clouds of flammable or toxic substances. The general method adopted was as follows:

- To identify potentially hazardous materials and establish maximum total inventories and locations. This information was gathered through conducting visits to each of the installations involved and holding discussions with site personnel.
- To consider the behaviour of the dangerous substances on release, on the basis of information on material properties and process / storage conditions.
- To identify ways in which serious losses of containment could occur, presenting a hazard to the local population.
- To quantify the probability and consequences of selected failure events.

In considering the routes by which selected failures could occur, a number of contributory factors were taken into account, including:

- Operator errors.
- Metallurgical fatigue or ageing of materials.
- Internal or external corrosion.
- Loss of process control.
- Overfilling.
- Introduction of impurities.
- Fire and/or explosion.
- Missiles.
- Flooding.

The kind of failure events considered included leakage from pipes and vessels, together with some consideration of events that could result from an escalation of an event on the same installation or from a neighbouring installation. The scenarios considered in the original study are listed in Table 22.

Table 22
Scenarios considered in original Canvey study (HMSO 1978)

Installation	Major hazard scenarios identified
Shell UK Oil	Ammonia release to estuary from a ship collision
	Ammonia release at the jetties
	Ammonia release from site pipework
	HF release from the alkylation unit
	LPG release to the estuary after a ship collision
	LPG release at the jetties
	LPG release from the site
Mobil Oil Co Ltd	LPG release to the estuary after a ship collision
	LPG release at the jetties
	LPG release from the site
	HF release from the new alkylation unit
Fisons Ltd	Ammonia release from the storage sphere
	Ammonia release from rail cars, couplings and pipework
	Ammonium nitrate explosion
United Refineries Ltd (planned)	LPG release to the estuary after a ship collision
	LPG release at the jetties
	LPG release from the site
	Massive spill of hydrocarbon liquid resulting in widespread fires
London and Coastal Wharves Ltd	Massive spill of hydrocarbon liquid resulting in widespread fires
Texaco Ltd	
British Gas Corporation	LNG release to the estuary after a ship collision
	LNG release during ship to shore transfer operations
	LNG release from above ground tanks
	LNG release from in-ground pits
	LPG release from above ground tanks
	LPG release from pipeline
	LNG release from ship commissioning
Calor Gas Ltd	Fire leading to missile generation
Occidental Refineries Ltd (planned)	LPG release to the estuary after a ship collision
	LPG release at the jetties
	LPG release from the site
	HF release from the site
Shipping	LNG, LPG or ammonia release to the estuary (collision in transit)
	LNG, LPG or ammonia release at the jetties

Releases of hydrogen fluoride (HF) from alkylation units on the refineries as a result of a loss of process control were discussed, but not analysed in detail. A frequency of such events was estimated using expert judgement. It appears that these releases were subsequently treated in the same way as other releases of hydrogen fluoride.

Hazards from the manufacture of ammonium nitrate were also addressed and subsequently dismissed because the continuous process used resulted in a small inventory of material being

present in the reactor at any one time. The events included within the study related to the storage of ammonium nitrate only.

At the time of the study British Gas operated a service whereby owners of LNG carriers could arrange for newly constructed vessels to be commissioned at the British Gas jetty. The possibility of a range of hazardous events arising from this activity was discussed in some detail, but the risks were not quantified.

In general terms, then, the study was of the 'top down' type discussed in Section 2.1.4. Use of this approach was chiefly as a result of the magnitude of the scope of the study – clearly it would have been impracticable to examine in detail every possible failure mode from each installation considered. The probabilities were largely derived from historical data, combined with expert judgement. It should also be remembered that the study was one of the earliest applications of QRA within the onshore process industry environment and consequently many of the models and approaches now available were not in existence.

5.2 RIJNMOND STUDY

The Rijnmond study (Rijnmond Public Authority 1982) was commissioned by the Rijnmond Public Authority and conducted by Cremer and Warner. The work aimed to evaluate the application of risk assessment methodology to industrial installations, as a necessary prelude to using such assessments in the formulation of safety policy.

The Rijnmond area lies adjacent to the mouth of the Rhine, between Rotterdam and the North Sea. The area houses a vast complex of oil, petrochemical and chemical installations including five oil refineries and three major petrochemicals complexes. The study focussed on six installations within this complex:

- Acrylonitrile storage.
- Ammonia storage.
- Chlorine storage.
- LNG storage.
- Propylene storage.
- A hydrodesulphuriser.

The identification of the failure cases (or accident scenarios) to be modelled within the analysis was conducted by using what was termed a 'checklist'. This was essentially the same as the 'top down' approach as described in Section 2.1.4, but was supplemented by a consideration of the material properties. If the material properties indicated a potential for self-polymerisation, for example, then this was considered as an additional scenario.

The Rijnmond Study is one of the earliest published examples of the use of the top down approach. Indeed, some authors have referred to the top down approach as 'the Rijnmond Approach'.

For some of the installations (the acrylonitrile storage and the hydrodesulphuriser), a HAZOP study was conducted as well as using the checklist. However, for these installations, the findings of the HAZOP did not add significantly to what had been obtained using the checklist.

Where a catastrophic loss of containment was included, fault tree analysis was used to produce an event frequency. The fault trees contained some events arising from abnormal operations or conditions, such as over-pressurisation, overfilling, internal explosion and introduction of the wrong material followed by chemical reaction.

5.3 THE FIRST BENCHMARK EXERCISE ON MAJOR HAZARD ANALYSIS

This study was commissioned by the Joint Research Centre of the European Community (EC 1991). The aim was to assess the state of the art in risk analysis. 11 teams took part, representing regulators, research organisations, engineering companies and industry. The teams were also drawn from a range of nationalities. Each team was invited to conduct a risk analysis of an existing ammonia storage plant, placed in a hypothetical location. The study was comprised of two phases. The first phase aimed to compare the different approaches to risk analysis. On the basis of the results of the first phase, the second phase sought to identify the elements contributing to the differences in results observed.

Following the first phase, it was observed that the approaches used by the teams divided into two groups. Users of what was designated the 'first approach' followed the 'top down' method as described in Section 2.1.4. In some cases this was supplemented by a more detailed consideration of certain parts of the plant where the 'top down' approach was not judged to be appropriate. Users of the 'second approach' adopted a methodology that was described as being closer to that used within the nuclear industry. This involved application of a structured hazard identification technique (such as FMEA or HAZOP), followed by screening of the outputs by expert judgement. This resulted in a relatively small set of accident scenarios, which were then subjected to detailed analysis and quantification. By contrast, users of the 'first approach' generated extensive lists of scenarios for inclusion at the quantification stage. Many of the teams, regardless of whether they used the first or second approach, supplemented the analysis with a consideration of historical experience on similar plants. The approaches used are summarised in Table 23.

Table 23
Methodologies applied for hazard identification

Methodology Applied	Team Label										
	1	2	3	4	5	6	7	8	9	10	11
Historical experience											
- case history review	X	X				X	X		X	X	
- release frequency data bases						X	X		X		X
Previous experience with hazop studies	X										
Master logic diagram or fault tree					X		X	X		X	
FMEA			X								
HAZOP		X		X	X					X	
Check list				X						X	
Event tree					X	X*	X		X	X	X*
Action error analysis	X				X				X		
Systematic account of possible ruptures					X°	X	X		X		X

Note:

* = built-in in the computational tool adopted
o = passive components only

Some comparison of the lists of scenarios modelled was made within the study report. The combined list of all of the scenarios obtained from the 'second approach' was compared with the scenarios used by each team. This is shown in Table 24. Hence Table 24 does not include all of the scenarios modelled by users of the 'first approach'. Had it done so the table would have been several pages in length. Within Table 24, the scenarios have been grouped according to the plant area on which they arise, as follows:

1. The breasting island (jetty).
2. The import pipeline.
3. The refrigerated storage and associated facilities.
4. The cross country pipeline.
5. The pressurised storage.

Table 24
Main accidents identified as important for quantification

Accident identified	Plant area ID. number	Team label										
		Second approach							First approach			
		1	2	3	4	5	8	10	6	7	9	11
Catastrophic failure of the vessel	5	X	X		X (5)	X	X	X	X	X	X	X
Non catastrophic failure of the vessel (o)	5		X		X (5)			-	X	X	X	X
Rupture of the bottom pipe of the vessel	5			X		X		-	X	X	X	X
Rupture of the level indicator	5				X (6)	X (6)		-	X (1)		X (1)	?
Rupture of the feed line flange	5					X		-	X	X	X	X
Damage of cross country pipeline (underground)	4	X	X	X	X	X	X (4)	-	X	X	X	X
Rupture of 12" pipe upstream HV04	3			X	X	X	X		X	X	X (3)	X
DK101 burst at or near the base due to overpressure	3			X (5)	X				X (2)	X		?
Rupture of the roof of DK101	3	X	X		X	X	X	X	X	X	X	?
Release from safety valves	3	X	X				X (4)	X	X	X	X	
Rupture of pipe P1001 (from HV04 to pumps)	3					X		-	X	X	X (3)	X
Rupture of pipe P1007 between pumps 3 and BH101 heater	3	X		X		X		X	X	X	X	X
Rupture of P1008 downstream pre-heater (above ground)	4	X		X (5)	X	X		X	X	X	X	X
Damage of the inner tank DK101	3	X	X	X					X	X	X	X
Damage of the outer and inner tanks (external causes)	3	X			X				X	X	X	
Rupture of a condenser ET101/2	3	X							X (3)		X	?
Release from safety valve of a condenser	3	X										
Explosion inside the tank DK101	3	X	X									
Rupture of flange L09 (4") outside concrete tank	3					X						
Rupture or disconnection of loading arm	1	X (5)	X	X	X	X	X (4)	-	X	X	X	X
Rupture of P1004 to DK101 (undersea underground)	2	X		X		X	X (4)	-	X	X	X (3)	X
Rupture of P1004 in the sea side storage (above ground)	2			X		X		X	X	X	X (3)	X

Note:

(1) rupture of sight glass.
(2) catastrophic failure considered.
(3) leak, not full rupture.
(4) contribution considered negligible.
(5) not quantified.
(6) rupture of the bottom flange.
(o) different size rupture assumed.
(-) considered outside the plant boundaries.
(?) probably automatically generated by the computational tool, but not clearly documented in the reports.

It was observed that the scenario lists generated by users of the first approach showed a greater degree of agreement than those generated by the second approach. Also, the first approach appeared to generate all but a few of the scenarios produced by the second approach. The concept of 'coverage' as developed by Suokas (1985) (see Section 4.1) can be used to illustrate the differences observed. The total number of scenarios generated by all users of the second approach, as listed in Table 24, was 22. The coverage achieved by each of the teams, relative to this total, has been calculated and is shown in Table 25.

Table 25
Coverage achieved by study teams

Approach	Team	Coverage (%)
First	6	86
	7	77
	9	82
	11	59-77*
Second	1	59
	2	36
	3	45
	4	45
	5	64
	8	32
	10	27

Note:
* Some scenarios probably generated automatically by computerised tool used, but not clearly documented in report.

Hence teams using the first approach generally achieved a higher coverage (59-86%) compared to teams using the second approach (27-64%).

A review of historical data on accidents involving ammonia was also conducted. The HSE MHIDAS and TNO FACTS databases were interrogated. Other sources consulted included the Community Documentation Centre on Industrial Risk (CDCIR) and the European Communities Databank for Environmental Chemicals (ECDIN). A lack of detail in the accident records retrieved prevented detailed comparisons with the analyses performed.

Inspection of the accident information presented in the study report indicates that the kind of accidents found in the historical record were, in general, addressed by the study teams. For example, records of a number of incidents involving overfilling or over-pressurisation of storage vessels were found. Events of this type would appear to be addressed by the following events listed in Table 24:

- Catastrophic / non-catastrophic failure of the vessel.
- DK101 burst at or near the base due to overpressure.
- Rupture of the roof of DK101.
- Release from safety valves.

In terms of the effect of the approach used on the calculated risks, comparisons are difficult since there was a range of factors (differences in assumptions, differences in modelling, differences in presentation of results) which influenced the results. However it was observed that in general the risks calculated using the first approach were higher in the near-field than those obtained using the second approach. This was thought to be due to the fact that the second approach focussed on a small set of events that had been selected for their potential for large-scale consequences. In contrast, the first approach includes a whole range of events, from the relatively minor to the catastrophic.

6. QRA AND ACCIDENT THEORY

Section 3 described research that linked the use of generic failure rate data in QRA with schemes of accident causation. Section 5 discussed studies of quality in QRA and in particular definitions of validity. One definition of validity described was that of construct validity. Construct validity is related to the concepts employed to interpret the analysis results. In the context of the present study, this could be interpreted as the relationship between QRA and accident theories, and specifically the capability of the QRA to identify factors influencing the accident process as described in accident theories.

The purpose of this section of the report is to provide a brief review of the literature on accident theory, and to consider the relationship between models of accident causation and QRA methodology.

There is a wealth of literature available on accident theory and therefore the report describes only some key features and issues which are most pertinent to the point in question. Some of the most commonly used models that are associated with accident causation and prevention are described.

6.1 WHAT IS AN ACCIDENT?

Reason (1998) clarifies the description of an 'accident' very succinctly in that there are two types of accident that can occur. Firstly, there are accidents that happen to the individual. Typically these types of accidents are large in number and are not normally considered to be within the scope of QRA. Secondly there are organisational accidents, that fortunately are relatively rare but which have a large-scale impact on populations.

The UK has been witness to a number of such organisational accidents, including Flixborough (1974), Herald of Free Enterprise (1987), Kings Cross (1987), Piper Alpha (1988) and Clapham Junction (1988). Such accidents are characterised by multiple causes and numerous interactions between different elements of the system in question. The results of the investigations into these incidents highlight a number of key issues with respect to accident initiation, mitigation and prevention. However for the purposes of this study two issues of particular relevance are:

- An investigation of 19 UK public inquiry reports on major accidents (Turner and Toft, 1988) found 80% of recommendations were concerned with organisational and procedural matters rather than technical, hardware issues.
- "Traditionally, major accident investigations have focused on identifying the operator and technical failures... However, experts in the field are becoming increasingly concerned that an understanding of the management/organisational failures is of even greater importance if we are to make an impact on reducing the frequency of major disasters" Batstone, (1989).

6.2 MODELS OF 'ACCIDENTS'

Different types of accident model exist. Broadly speaking, these models may be divided into three categories, as follows:

- Those which describe a sequential model of accident development.
- Those which describe the conditions that are typically prevailing when accidents occur.
- Those which, typically, are used to investigate accident causation.

A useful description of a number of analytical frameworks is partly reproduced from Hoyos and Zimolong (1988) in Table 26. The reader is referred to the original reference for further details on each of the approaches.

Table 26
Types of accident model

Approach		Method
Systems Theory	Systems ergonomics	Failure modes and effects analysis
		Fault tree analysis
		Incidental Factor analysis
	Industrial engineering systems	Management oversight and risk trees
	Energy exchange model	Rank order of measures to eliminate hazard and danger
Sequential models	Sequence of events (Domino)	Sequential analysis
	Multi-linear events sequencing	
	Human information processing	Behavioural studies
	Incidents and near misses	Critical incident technique
		Incident reporting*
		Root cause analysis*
		(*these elements are additions to the original table)
Integrative models	Perturbation concept	Systems safety analysis
		Sequential analysis
	Deviation concept	Ergonomic and behavioural methods
Epidemiological approach	(This is more of a description of a hazard than accident)	Description of host factors, agent and environment

A more modern list of 'Models of Accident Causation and Theoretical Approaches' is given in Hurst (1998). This list includes:

- Engineering considerations.
- Human error.
- Safety culture and attitudes to safety.
- Safety management systems.
- Sociotechnical systems.
- Latent and active failures.
- High reliability theory and normal accidents.
- Subjective/objective debate.
- Risk perception and acceptable risk.

A few of the more commonly used models are now described in order to present an illustration of the types and variety of models that are available.

6.2.1 Disaster Lifecycle

At the societal and cultural level Turner (1978) describes six stages in a disaster lifecycle. This framework is described below:

1. Notionally normal starting points:
   a. Initial culturally accepted beliefs about the world and its hazards.
   b. Associated precautionary norms set out in laws, codes of practice, traditions and folkways.
2. Incubation period:
   a. The accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance.
3. Precipitating event:
   a. Forces itself to the attention and transforms general perceptions of stage 2.
4. Onset:
   a. The immediate collapse of cultural precautions becomes apparent.
5. Rescue and salvage – first stage of adjustment:
   a. The immediate post-collapse situation is recognised in ad hoc adjustment which permit the work of rescue and salvage to be started.
6. Full cultural readjustment:
   a. An inquiry or assessment is carried out and beliefs and precautionary norms are adjusted to fit the newly gained understanding of the world.

6.2.2 Sociotechnical Model

Section 3 described work by Hurst et al. (1991) which classified failures of piping and pressure vessels in order to investigate the influence of human factors and management systems on generic failure rates. The classification scheme was considered in the context of a hierarchical scheme of accident causation, which is shown in
Figure 7. The immediate causes are seen as the symptoms of underlying problems in the sociotechnical system.

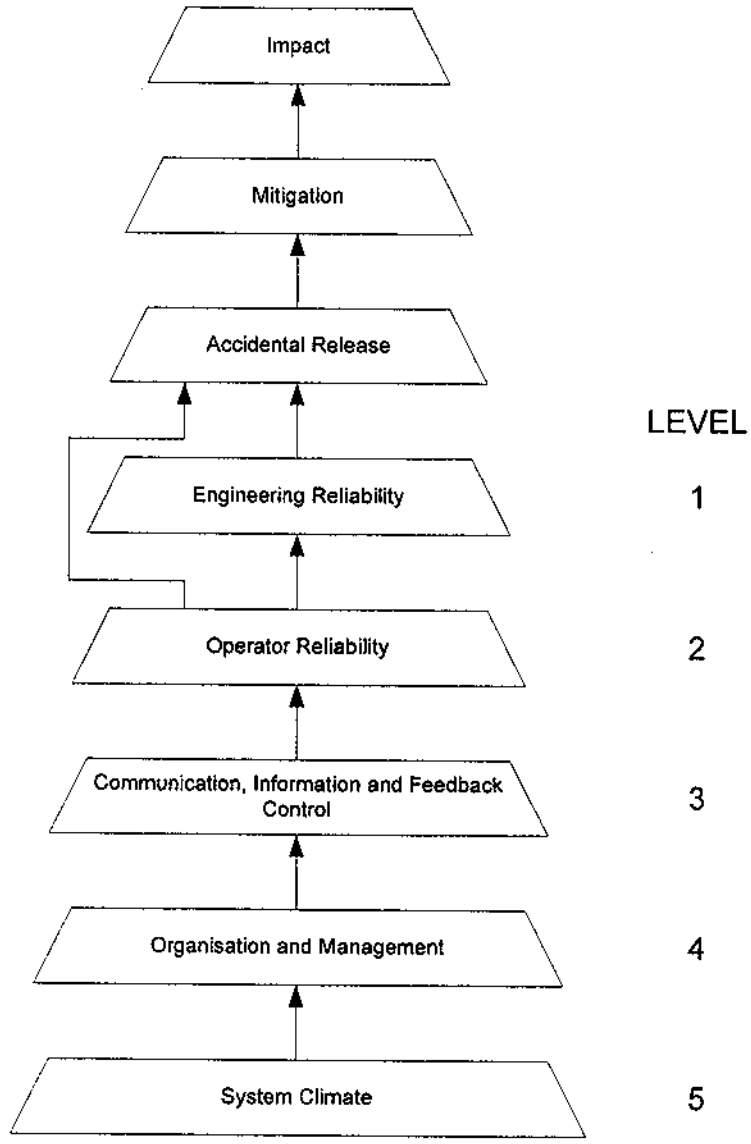

Figure 7
Hierarchical scheme of accident causation

The hierarchy shows levels of causes that are increasingly remote from the accident itself. This is remoteness in terms of levels of cause and effect, not remoteness in time. The example given is of an operator erroneously opening a valve and causing a release. The error on the part of the operator and the release are directly connected. However, the event may have occurred because the operator was not provided with an appropriate procedure, or because there had been a failure in communication, or because the operator was not adequately trained. These causes are more remote from the release event. Still more remote is, for example, the case where management may not have allocated sufficient resources for training, due to inadequacies in prioritising brought about by severe production pressures.

The different levels of the hierarchy are described in Table 27.

Table 27
Levels in the hierarchical scheme

Level	Description
1	Engineering reliability. This concerns the design of the hardware of a plant and the its operating limits. It excludes aspects such as the man-machine interface (MMI) which impinge directly on operator reliability. It includes aspects of the engineering design that might mitigate the effects of an accidental release.
2	Operator reliability. This encompasses all aspects of human factors that directly influence operator performance, including the MMI, training, experience, procedure design, etc.
3	Communication, information and feedback control. This level concerns information dissemination through documentation, instructions, logs, reporting systems etc. and the feedback systems whereby it can be verified that the appropriate communication has taken place and been acted upon.
4	Organisation and management. This level refers to the organisational structure and management system, e.g. – for the management of safety. It includes factors such as the setting of standards, priorities and targets, decision-making functions and the establishment of organisational groups, processes and personnel roles to meet the functional requirements of the system.
5	System climate. This level considers the wider system (regulatory requirements, economic pressures, public opinion, technical knowledge) within which the system itself operates.

It is theoretically possible to trace the causes through the different levels of the hierarchy to the immediate cause and the accident. The hierarchy can then be applied to the underlying causes and failures of preventative measures considered in the classification scheme. For example:

- For underlying causes of failure, problems in organisation and management (level 4) may lead to design errors. Design errors could lead to operator reliability problems at level 2 or engineering problems at level 1.
- For preventive measures, pressures in meeting production deadlines (level 5) may prevent a hazard study being carried out. Lack of a hazard study (level 4) may prevent hardware problems from being identified at level 1.

Hence the immediate causes at level 1 or 2 are manifestations of deficiencies at deeper levels.

6.2.3 Sequential Models

At an organisational level there are a number of sequential models that are based on the domino theory proposed by Heinrich and further developed by Bird. One such model, the DNV Loss Causation model, is described in Figure 8.

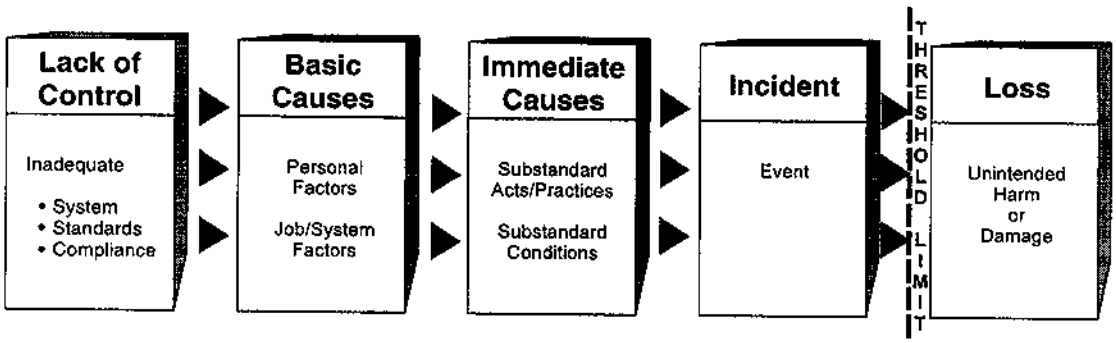

Figure 8
The DNV loss causation model

A more recent and now commonly used model is that proposed by Reason (1998). In this model Reason talks about active and latent failures, which together can open an accident trajectory through an organisation's defences. This is illustrated in Figure 9. An advantage of this model is that it can encompass the issue of the organisation being in a dynamic environment and therefore as some weaknesses in defences are identified and corrected, others become apparent.

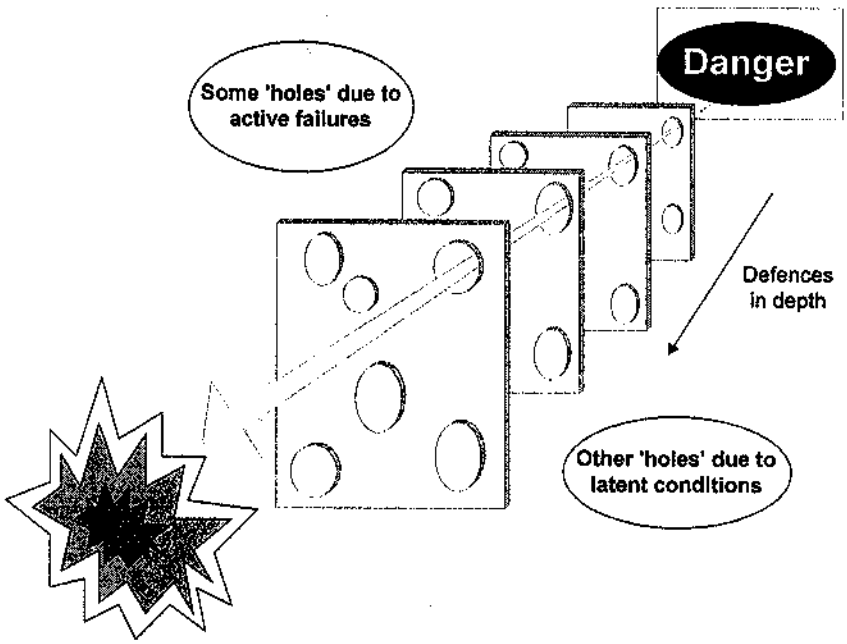

Figure 9
An accident trajectory

These models are based on the traditional approach of accidents being caused through unsafe acts and unsafe conditions. However, there has also been some attempt to explain accidents from the sociological perspective. An example of this approach to looking at accident causation is described below.

6.2.4 Sociological Models

The sociological explanation of accidents differs from the traditional hypothesis on which the majority of modern safety practices are based, which reduce accident causes to unsafe acts and conditions. In this case the underlying hypothesis is that accidents are produced by social relations at work.

One such model is put forward by Dwyer & Raftery (1991), who propose the view that accidents are produced at each of three levels of social relations of work (rewards, command and organisation), and also non-socially at the individual level.

At the reward level work is produced through the manipulation of recompense, whether monetary or symbolic, in return for effort. At this level it is proposed that accidents are produced through factors such as financial incentives, long working hours, working beyond physical capabilities etc.

At the command level work is produced through the use of power. This power may be overt and resisted (e.g. authoritarianism) or covert and accepted (such as when risks are accepted as part of normal practice). This level is reported as not traditionally being seen as having an important weight within accident production. However, the acceptance of risk taking behaviour as part of normal practice is acknowledged in some management literature as a problem that must be overcome. Some evidence of a lack of union power resulting in an employer being very authoritarian is also quoted.

At the organisational level work is produced through employer control over the division of labour. This translates into task structure, relationships between tasks, task demands, the knowledge workers have of these tasks and the capacity to react independently of the influence of social relations at other levels. This area is seen as a major contributor to

accidents with monotony and boredom being significant factors. Additionally strong evidence suggests that 'unusual' tasks are also a source of accidents and the under qualification of workers is often seen as a contributory factor. Incidents such as Three Mile Island and the Challenger disaster are related to this area.

6.3 COMPARISON WITH QRA METHODOLOGY

As the discussion above illustrates, comparison of QRA methodology with certain accident models (such as the sociological explanation of accident causation) is difficult. However, some comparison with the sequential and hierarchical models is possible.

Considering the DNV Loss Causation Model (Figure 8) and the hierarchical model proposed by Hurst et al. (
Figure 7), it can be seen that typically QRA studies address certain levels within these models. This is summarised in Table 28 below. The parallels drawn between the different levels of the two model are considered to be crude and not definitive.

Table 28
Comparison of accident models with QRA

Level within loss causation model	Level within hierarchical model	QRA methodology
Immediate Causes	1: Engineering Reliability	Addressed by standard QRA techniques including use of generic data and / or fault tree analysis etc.
	2: Operator Reliability	Tools exist to address within QRA either crudely (through use of generic human failure data) or in more detail (through use of task analysis etc.).
Basic Causes	3: Communication, Information and Feedback Control	May be addressed through linking of audit results to generic failure rate data (using MANAGER or PRIMA for example), but infrequently used.
Lack of Control	4. Organisation and Management	
	5. System Climate	Not currently addressed.

Hence it can be seen that a QRA which uses a purely 'top down' approach (as described in Section 2.1.4) will address Level 1 / Immediate Causes. It is assumed that Level 2 is also addressed, at least to some extent, since it is assumed the generic failure rate data used include some element of operator error. However, deeper levels expressed within the accident models will not be addressed.

Tools currently exist to enable QRA studies to be performed which attempt to address the full range of levels described within the accident models, with the exception of Level 5 (System Climate).

A recent development has been the concept of safety culture. A good definition of safety culture is that produced by The Advisory Committee on the Safety of Nuclear Installations (ACSNI 1993). This definition is, 'the safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management'.

There are now a number of tools available to measure safety culture or 'safety climate'. One of the most popular being the HSE Safety Climate Survey Tool. This tool is based on the use of a questionnaire that uses Likert scales as a means of measuring response to specific questions. There are a total of 71 questions which are grouped into ten factors including; organisational commitment and communication, line management commitment, supervisor's role, personal role, workmate's influence, competence, risk taking behaviour and some contributory influences, some obstacles to safe behaviour, permit-to-work systems and reporting of accidents and near misses. Whilst it is possible to statistically analyse the responses to identify areas of strengths and weakness there is currently no provision to attempt link the analysis directly to the any form of formal safety assessment.

7. ANALYSIS OF MAJOR ACCIDENTS

During the course of this study the following accident databases were interrogated:

- The Major Hazard Incident Data Service (MHIDAS) operated by AEA Technology on behalf of the Health and Safety Executive.
- The Accident Database operated by the Institution of Chemical Engineers (IChemE).
- The Major Accident Reporting System (MARS) operated by the EC Joint Research Centre.

A brief description of each of these databases is provided below.

7.1 MHIDAS

MHIDAS has been created to record details of those incidents involving hazardous materials that resulted in, or had the potential to produce, a significant impact on the public at large. Incidents involving nuclear materials are excluded from MHIDAS.

MHIDAS contains incidents from over 95 countries throughout the world, and particularly the USA, UK, Canada, Germany, France, and India. The database was started in the early 1980s, but there are references to incidents going back to the early years of the 20th century, and the database is continuously being updated. The data included in MHIDAS have been selected and indexed by professional engineers.

Each main record in MHIDAS refers to a hazardous material involved in a major incident, and is divided into the following fields, listed in the order in which they appear in records.

AN	MHIDAS Record Number
ME	Multiple Entry
CR	Contributor
DA	Date of Incident*
PD	Population Density
LO	Location
MN	Material Name
MT	Material Type
MH	Material Hazard
MC	Material Code
IT	Incident Type
OG	Origin
NP	Number of People Affected*
DG	Damage (US Dollars)*
GC	General Cause
SC	Specific Cause
QY	Quantity (Tonnes)*
IG	Ignition Time (Seconds)
IS	Ignition Source
KW	Keywords
AB	Abstract
RA	References Available
ID	Inverted Incident Date
KR	Killed**
IR	Injured**
ER	Evacuated**
DR	Damage**
QR	Quantity**

One peculiarity of MHIDAS is that, if an accident involved a number of dangerous substances, then several records for that accident appear in the database, one for each dangerous substance involved.

7.2 IChemE ACCIDENT DATABASE

The Accident Database has a much broader focus than either MHIDAS or MARS. It covers accidents of all sizes (i.e. – not just major accidents) as well as near misses. The database contains over 12,000 records.

7.3 MARS

The following information on MARS was abstracted from the JRC web site:

MARS was established to handle the information on 'major accidents' submitted by Member States of the European Union to the European Commission in accordance with the provisions of the 'Seveso Directive'.

Currently, MARS holds data on about 370 major accident events.

Information submitted to MARS may, where national provisions so require, be kept confidential if it calls into question, for example, the confidentiality of the deliberations of the Competent Authorities and the Commission, public security, personal data and/or files,

commercial and industrial secrets, etc. However, without violating these aspects, access to the register and information system shall be open to government departments of the Member States, industry or trade associations, trade unions, non-governmental organisations in the field of the protection of the environment and other international or research organisations working in this field.

As a result of an iterative process, two reporting forms have been established: the 'short report' is intended for use for immediate notification of an accident, and the "full report" is prepared when the accident has been fully investigated, and the causes, the evolution of the accident, and the consequences are fully understood. In certain cases further information comes to light - for example in the course of judicial proceedings - and there is provision for the 'full report' information to be further modified.

The 'short report' gives essential information concerning the accident, in a free-text format, under the following headings:

- Accident type.
- Substances directly involved.
- Immediate sources of accident.
- Immediate causes.
- Immediate effects.
- Emergency measures taken.
- Immediate lessons learnt.

Statistical type of information on short report data currently stored in MARS can be found by simply clicking on one of the above short report headings.

The 'full report' is much more analytic, and involves more work in its preparation. While there are always free-text fields available to describe facts connected with an accident, a great deal of effort has been put into the definition of descriptive codes, for the accident itself and for associated information, to enable the MARS database to be searched under almost 200 different headings (data variables).

The short reports may be accessed via the Internet. Access to the full reports is via JRC.

7.4 GENERAL SEARCH CRITERIA

A set of general criteria were applied in order to limit the searches to accidents that:

- Occurred in the UK.
- Occurred since 1984.
- Were at fixed installations (i.e. – not transport accidents).
- Did not involve cross-country pipelines.

In addition to these general criteria, it was also necessary to apply other criteria that were specific to the database being searched, because of the differing database structures.

7.5 MHIDAS SEARCH

The initial MHIDAS search, using the criteria outlined above, was refined further by:

- Removing duplicate records relating to the same accident (but different dangerous substances).
- Removing records where the General and Specific Causes were not given.
- Removing records of accidents that obviously did not occur at major hazard installations.
- Removing accidents involving relatively less hazardous materials that would not normally be subjected to QRA. These substances included:
  - Sulphuric acid (but not oleum).
  - Nitric acid.
  - Hydrochloric acid (but not anhydrous hydrogen chloride or hydrogen chloride produced by chemical reaction following release of another material).

This resulted in a total of 265 records of accidents, which were subjected to analysis.

7.6 ANALYSIS OF MHIDAS DATA

The 265 records produced by the search were initially analysed by origin (process plant, storage, warehousing, etc.) and general cause. Each major general cause was then broken down by specific cause.

This did not reveal a great deal of information concerning the state of the plant at the time the accident occurred. Furthermore, this information is not specified in any of the MHIDAS fields. Hence the abstracts accompanying the records were studied and, where it was possible to determine the plant state at the time of the accident, one of several key words was applied. Most of the key words are self explanatory, but definitions are listed below:

- CONTAMINATION: This was used to describe accidents where incompatible materials had been brought together, or where materials had been mixed in the wrong proportions.
- DEMOLITION: This was used to describe accidents that occurred when plant was being demolished.
- MAINTENANCE: This was used to describe accidents that occurred when plant was undergoing maintenance. It should be noted that the distinction between a normal or abnormal plant state is somewhat blurred in this case, since it is quite common for maintenance to take place on some equipment (e.g. – a pump that is installed in parallel with another) while the rest of the plant continues to operate normally.
- NORMAL: This was used to describe accidents that occurred when plant was operating normally.
- OTHER: This was used to describe accidents that occurred when plant was in an abnormal condition that was otherwise difficult to categorise.
- OVERHEATING: This was used to describe accidents that occurred when plant was subject to overheating.
- OVERPRESSURE: This was used to describe accidents that occurred when plant was subject to excess pressure.
- SHUTDOWN: This was used to describe accidents that occurred when plant was shut down.
- STARTUP: This was used to describe accidents that occurred when plant was undergoing start-up.
- UNKNOWN: This was applied when the plant condition at the time of the accident could not be determined from the abstract in the MHIDAS record.
- UPSET: This was used to describe accidents that occurred when plant was known to be in an upset condition.

Breakdowns of the data by plant state at the time of the accident were then performed.

7.7 RESULTS OF ANALYSIS OF MHIDAS DATA

7.7.1 Breakdown by Origin

The results are shown in Table 29 and Figure 10.

Table 29
Results of breakdown by origin

Origin type	Number of records	% of total
Domestic/Commercial	2	0.8
Process	117	44.2
Storage	85	32.1
Transfer	51	19.2
Warehouse	10	3.8
Total	265	100.0

The largest number of accidents originated in process plant (44%) with significant numbers also occurring in storage facilities (32%) or during transfer operations (19%).

7.7.2 Breakdown by Cause

The results of the analysis by General Cause is shown in Table 30 and Figure 11.

Table 30
Results of breakdown by general cause

General cause	Number of records	% of total
External	37	14.0
Human	64	24.2
Impact	15	5.7
Instrument	3	1.1
Mechanical	97	36.6
Procond	2	0.8
Service	3	1.1
VReaction	11	4.2
Combined Causes	33	12.5
Total	265	100

Records where more than one General Cause was given were assigned to the Combined Causes category. Mechanical failure was the dominant General Cause (37%), followed by human factors (24%). External factors (14%) and Combined Causes (13%) were also significant. The mechanical failure, human factors and external factors General Causes were then analysed according to the Specific Causes associated with them. The Combined Causes category was analysed according to the General Cause combinations found. The results are displayed in the following Tables and Figures:

- Breakdown of mechanical failure into specific causes: Table 31 and Figure 12.
- Breakdown of human factors into specific causes: Table 32 and Figure 13.
- Breakdown of external factors into specific causes: Table 33 and Figure 14; and
- Breakdown of Combined Causes into General Cause combinations: Table 34 and Figure 15.

Table 31
Breakdown of general cause mechanical failure into specific causes

Specific cause	Number of records	% of total
Accidental venting	1	1.0
Brittle failure	1	1.0
Corrosion	5	5.2
Leaking coupling or flange	7	7.2
Leaking gland or seal	3	3.1
Hose	2	2.1
Metallurgical failure	7	7.2
Overheating	8	8.2
Overloading	1	1.0
Overpressure	6	6.2
Relief valve failure	2	2.1
Valve leaking or passing valve	25	25.8
Weld failure	1	1.0
Not Given	28	28.9
Total	97	100

In a significant number of cases (29%) no Specific Causes were given. Where a specific cause had been identified, the dominating Specific Cause was a valve leaking or passing.

Table 32
Breakdown of general cause human factors into specific causes

Specific cause	Number of records	% of total
Accidental venting	1	1.6
Failure to connect or disconnect	1	1.6
Draining accident	3	4.7
General operational	16	25.0
Incompatible material and design	1	1.6
Installation error	1	1.6
Failure to isolate or drain before uncoupling	2	3.1
General maintenance	13	20.3
Management error	4	6.3
Overfilling	5	7.8
Procedures	10	15.6
Sabotage or vandalism	1	1.6
Not given	6	9.4
Total	64	100

Here, the main Specific Causes were general operational and general maintenance (25% and 20% respectively). The Specific Cause 'Procedures' was also significant (16%). In 9% of cases no Specific Cause was given.

Table 33
Breakdown of general cause external factors into specific causes

Specific cause	Number of records	% of total
Corrosion	1	2.7
Explosion	1	2.7
Fire	14	37.8
Flooding	1	2.7
High winds	1	2.7
Lightning	2	5.4
Sabotage or vandalism	11	29.7
Temperature extremes	5	13.5
Not given	1	2.7
Total	37	100

The predominant Specific Causes were fire (38%) and sabotage or vandalism (30%). The Specific Cause 'temperature extremes' was also significant (14%).

Table 34
Breakdown of combined causes into general cause combinations

General cause combination	Number of records	% of total
External-External	1	3.0
External-Human	3	9.1
External-Service	1	3.0
Human-Human	3	9.1
Human-Impact	2	6.1
Human-Inst-Procon	1	3.0
Human-Mechanical	8	24.2
Human-VReaction	5	15.2
Inst-Mechanical	3	9.1
Mechanical-External	2	6.1
Mechanical-VReaction	3	9.1
VReaction-Procond	1	3.0
Total	33	100

7.7.3 Breakdown by Plant State

Where possible, accident records were also assigned a Plant State category, using the process described above. A breakdown of the records by Plant State is presented in Table 35 and Figure 16.

Table 35
Breakdown by plant state (MHIDAS)

Plant state	Number of records	% of total
Contamination	14	5.3
Demolition	2	0.8
Maintenance	21	7.9
Normal	1	0.4
Other	3	1.1
Overheating	11	4.2
Overpressure	3	1.1
Shutdown	4	1.5
Startup	3	1.1
Unknown	199	75.1
Upset	4	1.5
Total	265	100

In the majority of cases (75%) it was not possible to determine the Plant State from the abstract. The breakdown was repeated, using only those accidents where the Plant State was identified as a basis. The results are shown in Table 36 and Figure 17.

Table 36
Breakdown of plant state for accidents where the plant state could be identified (MHIDAS)

Plant state	Number of records	% of total
Contamination	14	21.2
Demolition	2	3.0
Maintenance	21	31.8
Normal	1	1.5
Other	3	4.5
Overheating	11	16.7
Overpressure	3	4.5
Shutdown	4	6.1
Startup	3	4.5
Upset	4	6.1
Total	66	100.0

Hence, in approximately 32% of those accidents where the Plant State could be identified, the plant was undergoing maintenance at the time. Other significant Plant States were 'Contamination' (21%) and 'Overheating' (17%).

7.8 IChemE ACCIDENT DATABASE SEARCH

Initially, the general search criteria were used. The scope of the Accident Database is much broader than either MARS or MHIDAS, since it covers the full range of accidents experienced on process plants, not just major accidents. Some screening of the initial results was performed to remove accidents which were clearly not at major hazard sites or involved less hazardous substances such as hydrochloric acid. A few accidents were found which had occurred at nuclear processing or explosives sites. These were also excluded.

The records were also found to contain a few duplicates (typically the same incident reported by different authors at different times), which were also removed. This resulted in a total of 117 records for analysis.

7.9 ANALYSIS OF IChemE ACCIDENT DATABASE DATA

The amount of information within each record varied considerably. In some cases, the abstract contained only a single line of text, in others it was over a page in length. In many cases accident causes were not stated or were described by a single keyword, such as 'Leak'. In view of the fact that the MHIDAS analysis of the information on causes had revealed little concerning the Plant State at the time of the accident, an analysis of the information on causes was not carried out.

As with the MHIDAS records, an attempt was made to assign each of the accidents a 'Plant State' category, using the same set of keywords. As with MHIDAS, this information is not specified in any of the database fields.

Breakdowns of the data by plant state at the time of the accident were then performed.

7.10 RESULTS OF ANALYSIS OF IChemE ACCIDENT DATABASE DATA

The results of the analysis by Plant State are shown in Table 37 and Figure 18.

Table 37
Breakdown by plant state (IChemE)

Plant State	Number of Records	% of Total
Contamination	7	6.0
Demolition	0	0.0
Maintenance	7	6.0
Normal	3	2.6
Other	10	8.5
Overheating	7	6.0
Overpressure	5	4.3
Shutdown	5	4.3
Startup	1	0.9
Unknown	71	60.7
Upset	1	0.9
Total	117	100.0

As with the MHIDAS results, in the majority of cases (61%) it was not possible to determine the Plant State from the abstract. The breakdown was repeated, using as a basis only those accidents where the Plant State could be identified. The results are shown in Table 38 and Figure 19.

Table 38
Breakdown of plant state for accidents where the plant state could be identified (IChemE)

Plant state	Number of records	% of total
Contamination	7	15.2
Demolition	0	0.0
Maintenance	7	15.2
Normal	3	6.5
Other	10	21.7
Overheating	7	15.2
Overpressure	5	10.9
Shutdown	5	10.9
Startup	1	2.2
Upset	1	2.2
Total	46	100.0

In those accidents where the Plant State could be identified, the 'Other' category was the most common (22%). Also significant were 'Contamination', 'Maintenance' and 'Overheating' at approximately 15% each.

7.11 MARS SEARCH

With the assistance of the Health and Safety Executive, the short reports for each of the 33 incidents reported to MARS by the UK since the introduction of the database in 1993 were obtained. In view of the small number of records it was not necessary to refine the search. It should be noted that, of the three databases consulted, MARS probably has the narrowest scope since it contains only those accidents notified to the EC under the Seveso Directive (or the CIMAH Regulations in the UK). The requirements for reporting are defined within the Directive.

7.12 ANALYSIS OF THE MARS DATA

The MARS short reports contain, in the majority of case, only limited information concerning the causes of the accident. The Suspected Causes are classified as either 'Plant or Equipment', 'Human', 'Environmental' or 'Other'. This is supplemented by a brief description. In view of this, and the fact that the MHIDAS analysis of causes had revealed little of direct interest to this study, an analysis of the information on causes was not conducted.

An attempt was made to assign each of the accidents a 'Plant State' category, using the same set of keywords as applied to the MHIDAS data. As with MHIDAS, this information is not specified in any of the database fields.

Breakdowns of the data by plant state at the time of the accident were then performed.

7.13 RESULTS OF ANALYSIS OF MARS DATA

The results of the analysis by Plant State are shown in Table 39 and Figure 20.

Table 39
Breakdown by plant state

Plant state	Number of records	% of total
Contamination	1	3.0
Demolition	1	3.0
Maintenance	5	15.2
Normal	12	36.4
Other	6	18.2
Overheating	0	0.0
Overpressure	0	0.0
Shutdown	0	0.0
Startup	0	0.0
Unknown	7	21.2
Upset	1	3.0
Total	33	100.0

In a significant proportion of cases (21%) it was not possible to determine the Plant State from the record. This proportion was considerably lower than that observed for the MHIDAS analysis (75%). This is thought to be due to differences in the way information is stored within the two databases. MARS presents fewer keywords but more areas into which textual descriptions can be entered. Another difference is that the proportion of records for which the Plant State was determined to be 'Normal' was greater for the MARS analysis (36%) than for the MHIDAS analysis (0.4%). This indicates that a significant number of the 'Unknown' cases in the MHIDAS analysis may have been 'Normal'.

As with the MHIDAS analysis, the breakdown was repeated, using only those accidents where the Plant State was identified as a basis. The results are shown in Table 40 and Figure 21.

Table 40
Breakdown of plant state for accidents where the plant state could be identified

Plant state	Number of records	% of total
Contamination	1	3.8
Demolition	1	3.8
Maintenance	5	19.2
Normal	12	46.2
Other	6	23.1
Overheating	0	0.0
Overpressure	0	0.0
Shutdown	0	0.0
Startup	0	0.0
Upset	1	3.8
Total	26	100.0

In approximately 19% of cases where the Plant State could be identified, the plant was undergoing maintenance at the time. This compares with a figure of 32% obtained from MHIDAS on the same basis.

7.14 COMBINATION OF MARS AND MHIDAS DATA

An attempt was made to combine the results obtained from the various database searches. It was found that the IChemE Accident Database findings had to be excluded from this exercise, since a significant number of the records contained scant information concerning either the date or the location of the accident, or both. This made it difficult to clearly identify any overlaps between the Accident Database data set and the other data sets.

The list of records obtained from MARS was compared with the list from MHIDAS, in order to identify any duplicates. Surprisingly, only one duplicate was found. Hence the combined MHIDAS and MARS findings gave a total of 297 records. The combined records were then analysed according to Plant State at the time of the accident. The results are shown in Table 41 and Figure 22.

Table 41
Breakdown by plant state

Plant state	Number of records	% of total
Contamination	15	5.1
Demolition	3	1.0
Maintenance	26	8.8
Normal	13	4.4
Other	9	3.0
Overheating	11	3.7
Overpressure	3	1.0
Shutdown	4	1.3
Startup	3	1.0
Unknown	206	69.4
Upset	4	1.3
Total	297	100.0

Again, the breakdown was repeated, using only those records where the Plant State could be identified. The results are shown in Table 42 and Figure 23.

Table 42
Breakdown by plant state for accidents where the plant state could be identified

Plant state	Number of records	% of total
Contamination	15	16.5
Demolition	3	3.3
Maintenance	26	28.6
Normal	13	14.3
Other	9	9.9
Overheating	11	12.1
Overpressure	3	3.3
Shutdown	4	4.4
Startup	3	3.3
Upset	4	4.4
Total	91	100.0

Comparing these results with those for MHIDAS alone (Table 36), it can be seen that the proportion of 'Normal' states is somewhat higher (14% as opposed to 1.5%). This is due to the relatively high proportion of MARS records that were assigned to this category.

'Maintenance' remains a significant category, as do 'Contamination' and 'Overheating'.

7.15 DISCUSSION

7.15.1 MHIDAS Search

The largest number of accidents originated in process plant (44%) with significant numbers also occurring in storage facilities (32%) or during transfer operations (19%). A study of accident causes yielded the following information:

- Mechanical failure was the dominant General Cause (37%), followed by human factors (24%). External factors (14%) and Combined Causes (13%) were also significant.
- For Mechanical failures, in a significant number of cases (29%) no Specific Causes were given. Where a Specific Cause had been identified, a valve leaking or passing was dominant (26%).
- For Human Factors, the main Specific Causes were general operational and general maintenance (25% and 20% respectively). The Specific Cause 'Procedures' was also significant (16%). In 9% of cases no Specific Cause was given.
- For External Factors, the predominant Specific Causes were fire (38%) and sabotage or vandalism (30%). The Specific Cause 'temperature extremes' was also significant (14%).

A study of the General and Specific Causes yielded limited information concerning the plant state at the time of the accident. Some General Causes, such as violent reaction (VREACTION), imply a loss of process control. The cases involving maintenance as a Specific Cause under human factors also indicate an abnormal state.

The attempted analysis of plant state through a study of the abstract on the MHIDAS record proved problematic since in the majority of cases (75%) the Plant State could not be determined in this way. Conversely, it was possible to determine that at least approximately 25% of the accidents studied occurred when the plant was in some abnormal state.

In approximately 32% of those accidents where the Plant State could be identified, the plant was undergoing maintenance at the time. Other significant Plant States were 'Contamination' (21%) and 'Overheating' (17%).

7.15.2 IChemE Accident Database Search

As with the MHIDAS results, in a large proportion of the accidents analysed the Plant State at the time of the accident remained unidentified (61% of all cases). On removing the 'Unknown' records from the analysis, it was found that the most significant Plant States were 'Other' (22%), 'Contamination', 'Maintenance' and 'Overheating' (each with 15%). The kinds of Plant States falling into the 'Other' category were quite varied and included an unexpected decomposition of a catalyst, misconnection of delivery lines and blockages in lines, for example.

Overall, at least 27% of the accidents occurred when the plant was in some abnormal condition.

7.15.3 MARS Search

Fewer records were obtained from the MARS database compared to MHIDAS. In general the 'short reports' received contained less information on causes than the MHIDAS records. However, the reports contained several areas for descriptive text, which assisted in the identification of Plant State at the time of the accident. The proportion of accidents where the Plant State remained unknown was 21%, considerably less than for MHIDAS (75%). A significant number of the records indicated that the Plant State had been 'Normal' (36%). The occurrence of 'Maintenance' was again significant (19% of the accidents where the Plant State could be identified, as opposed to 32% for MHIDAS). As mentioned previously, the distinction between abnormal and normal plant states is somewhat blurred in the case of Maintenance. There were several accidents assigned to the 'Other' category (18% of all records). As with the IChemE database results, the kind of accidents falling into this category were quite varied and included a rollover in a LNG tank, operation of a plant outside its design limits and miscommunication of instructions resulting in overfilling of a tank.

Overall, at least 43% of the accidents occurred when the plant was in an abnormal condition.

7.15.4 Combined MHIDAS and MARS Data

On combining the MHIDAS and MARS results, it was found that only one record occurred in both data sets. This was surprising and the reasons are still under investigation. One reason for this may be that a number of accident records were excluded from the MHIDAS analysis because information on causes was not given. These may have included some of the accidents recorded in MARS. Also, MHIDAS contained no information on accidents occurring after 1997, whereas MARS records were obtained for accidents that occurred up to mid-1999.

The profile of breakdown by Plant State for the combined MHIDAS and MARS data is similar to that of the MHIDAS only data. Essentially this is because the greater number of MHIDAS records swamps the effect of introducing the MARS data. However, it was observed that the proportions of 'Normal' and 'Other' Plant States did increase noticeably. This was because these categories were quite significant for the MARS data but very small for MHIDAS. 'Maintenance' remains the most significant Plant State at around 29% of those accidents where the Plant State could be identified (9% of all accidents). Overall, at least 26% of the accidents occurred when the plant was in some abnormal condition.

7.15.5 General

Overall the analyses indicated that the proportion of accidents occurring when the plant was in some abnormal state was in the range of at least 25-43%. The analyses of the three databases did not reveal any consistent pattern in terms of the most common abnormal Plant States, other than that 'Maintenance' was significant for all three (15-32% of those accidents where the Plant State could be identified).

The significance of maintenance in relation to accidents has been the subject of previous studies by HSE (HSE 1987). This work also indicated that 30% of the incidents investigated had had the potential to present an off-site risk.

The results of these analyses should be viewed as indicative and not statistically significant. The process of assigning a Plant State category on the basis of the abstracts or text fields within the records was found to be difficult and quite subjective.

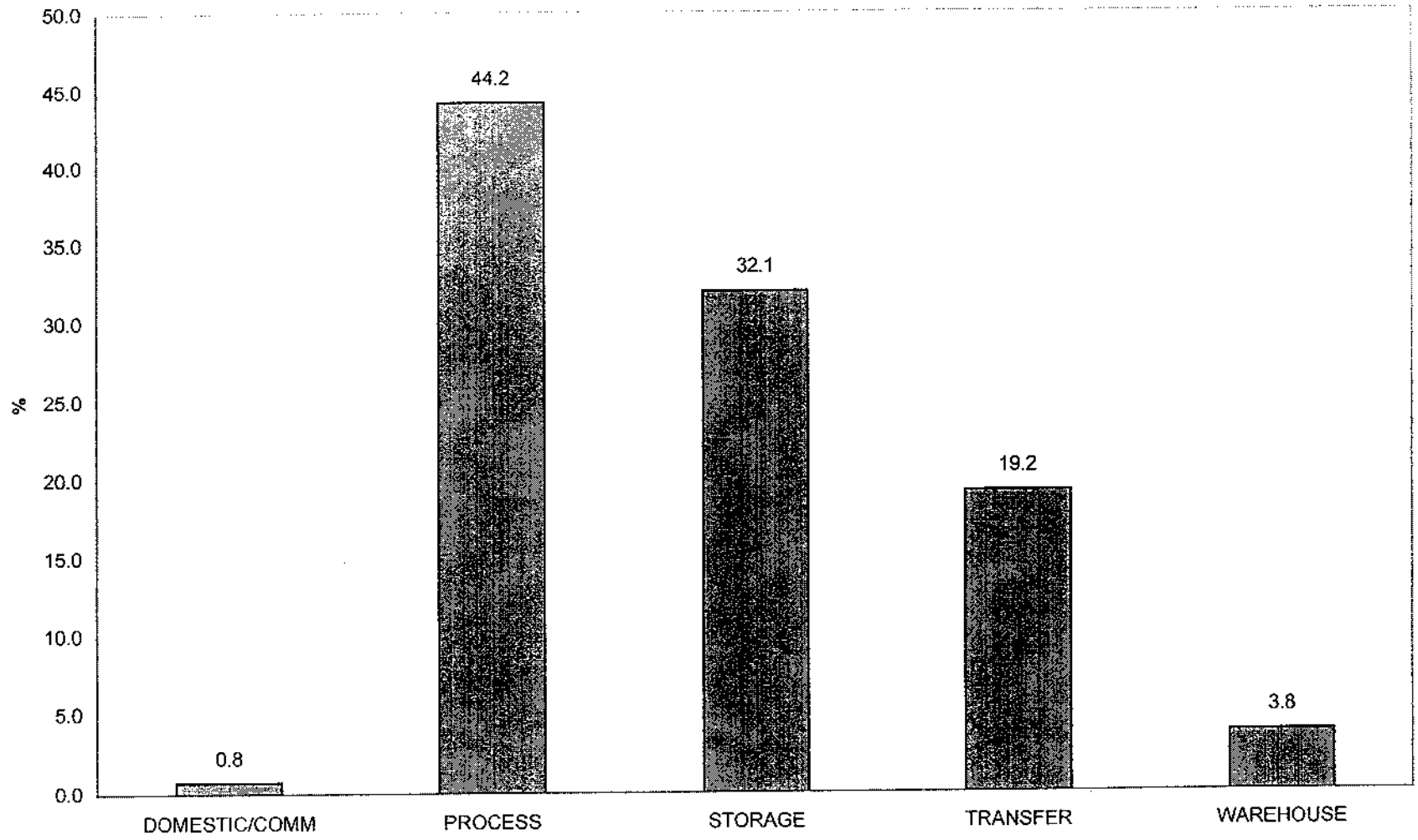

Figure 10
Results of breakdown by origin

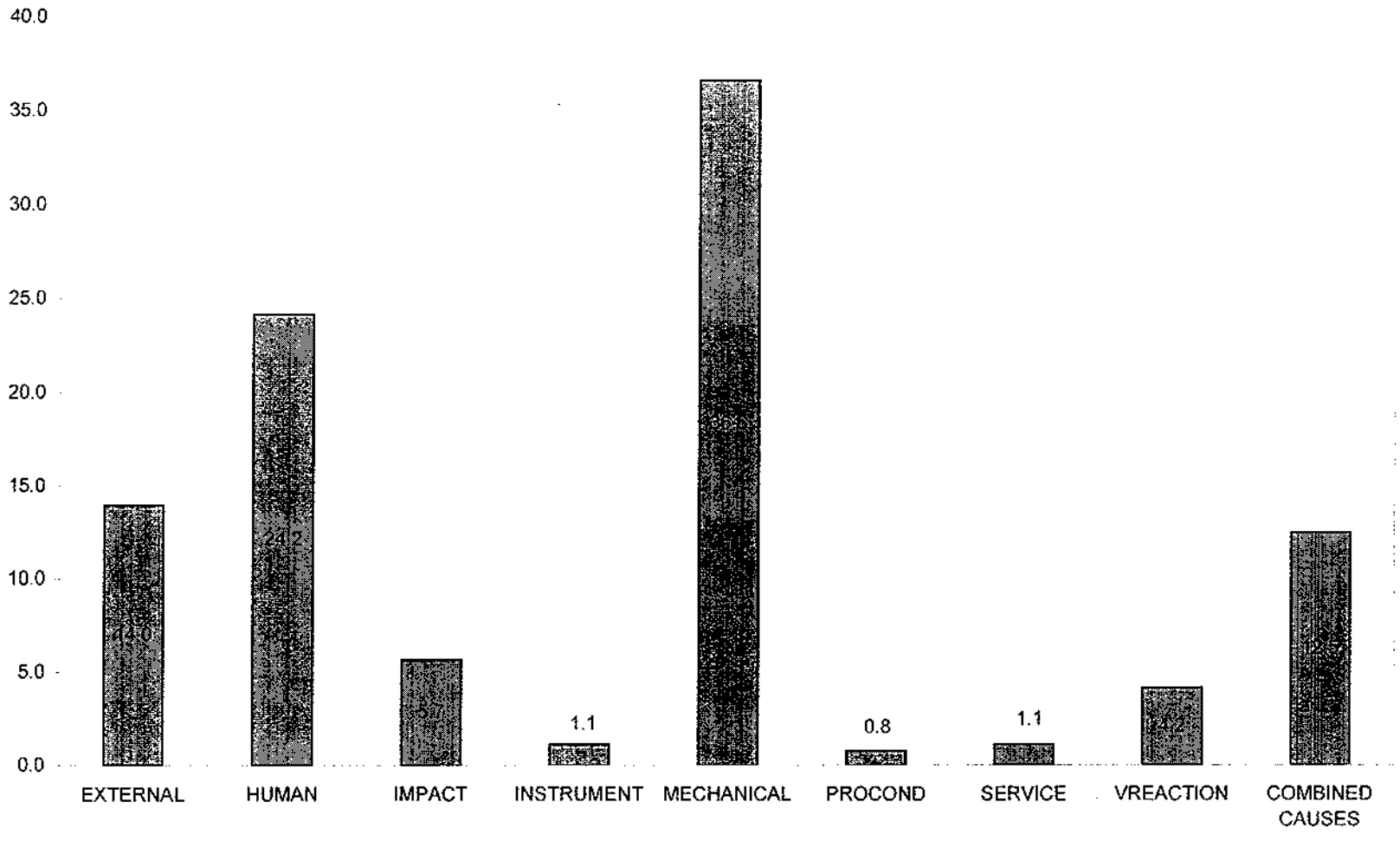

Figure 11
Results of breakdown by general cause

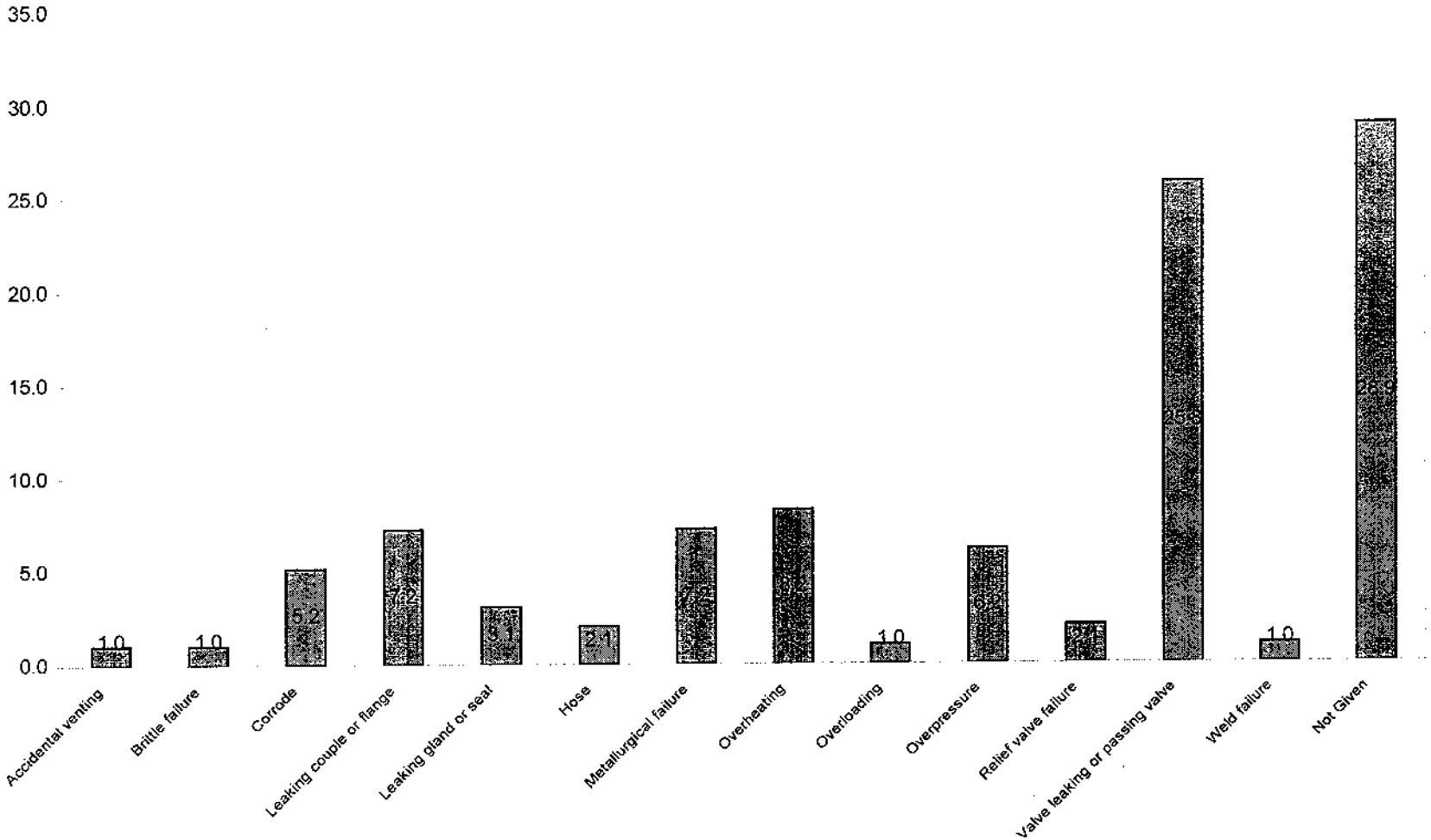

Figure 12
Breakdown of general cause mechanical failure into specific causes

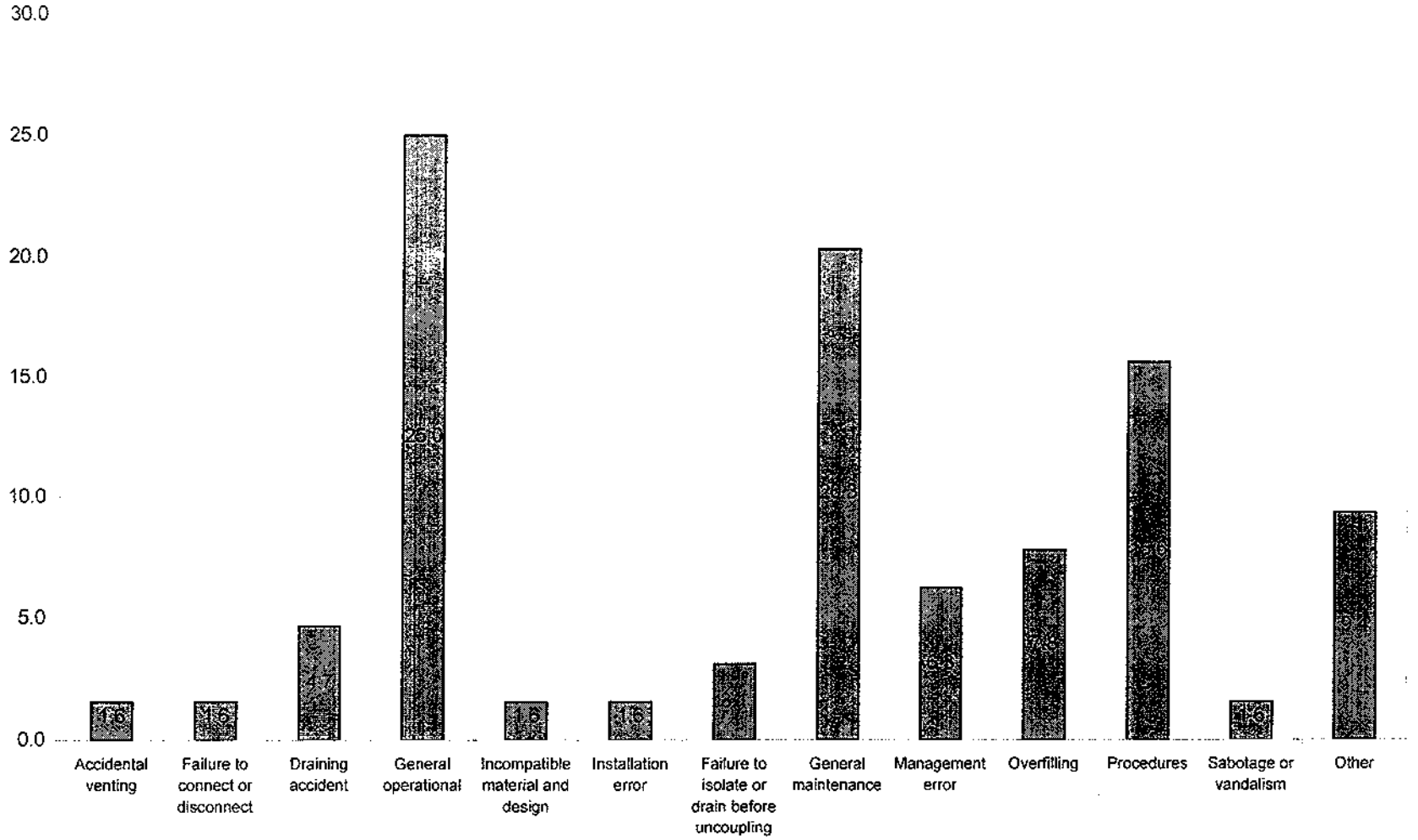

Figure 13
Breakdown of general cause human factors into specific causes

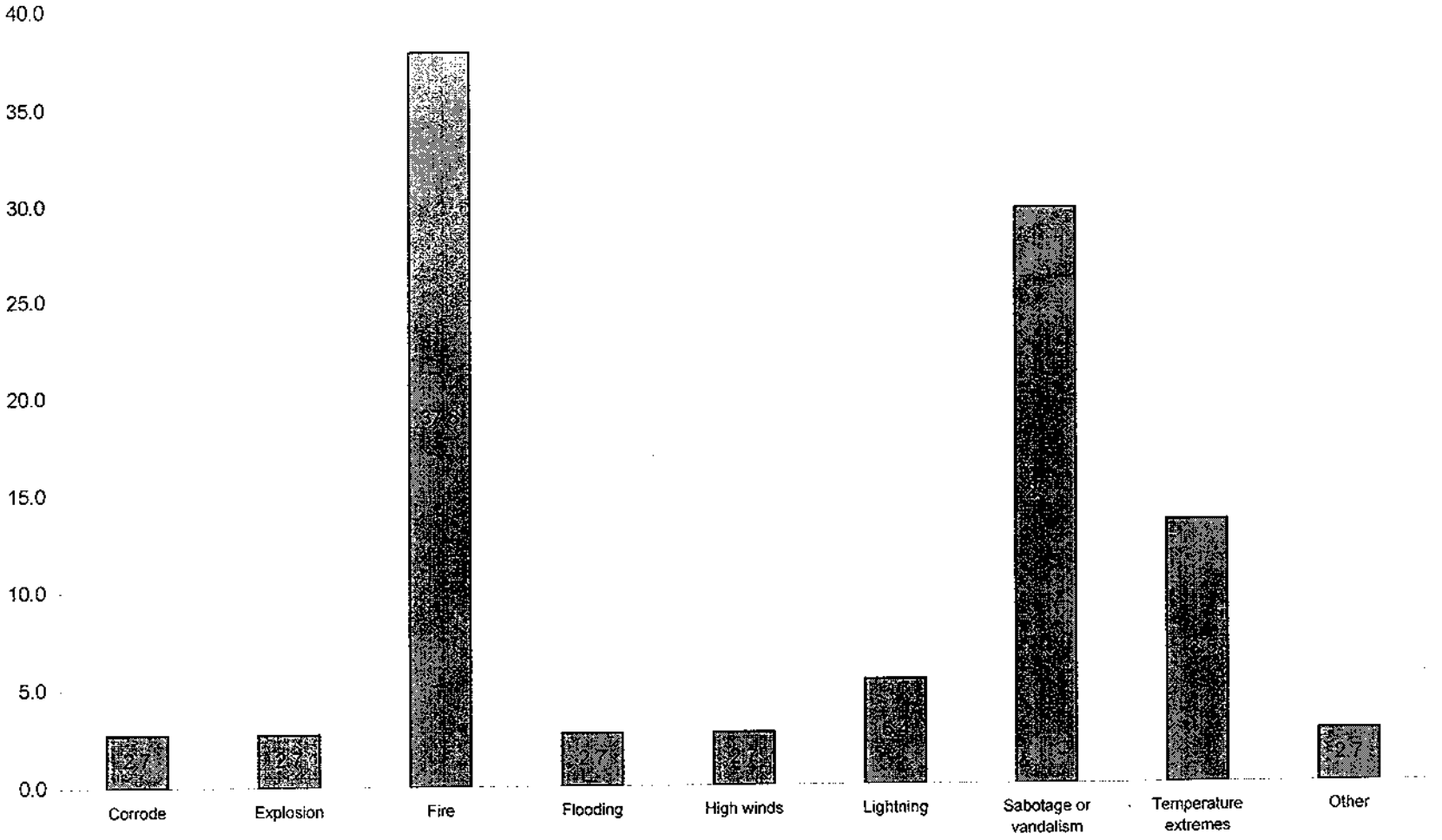

Figure 14
Breakdown of general cause external factors into specific causes

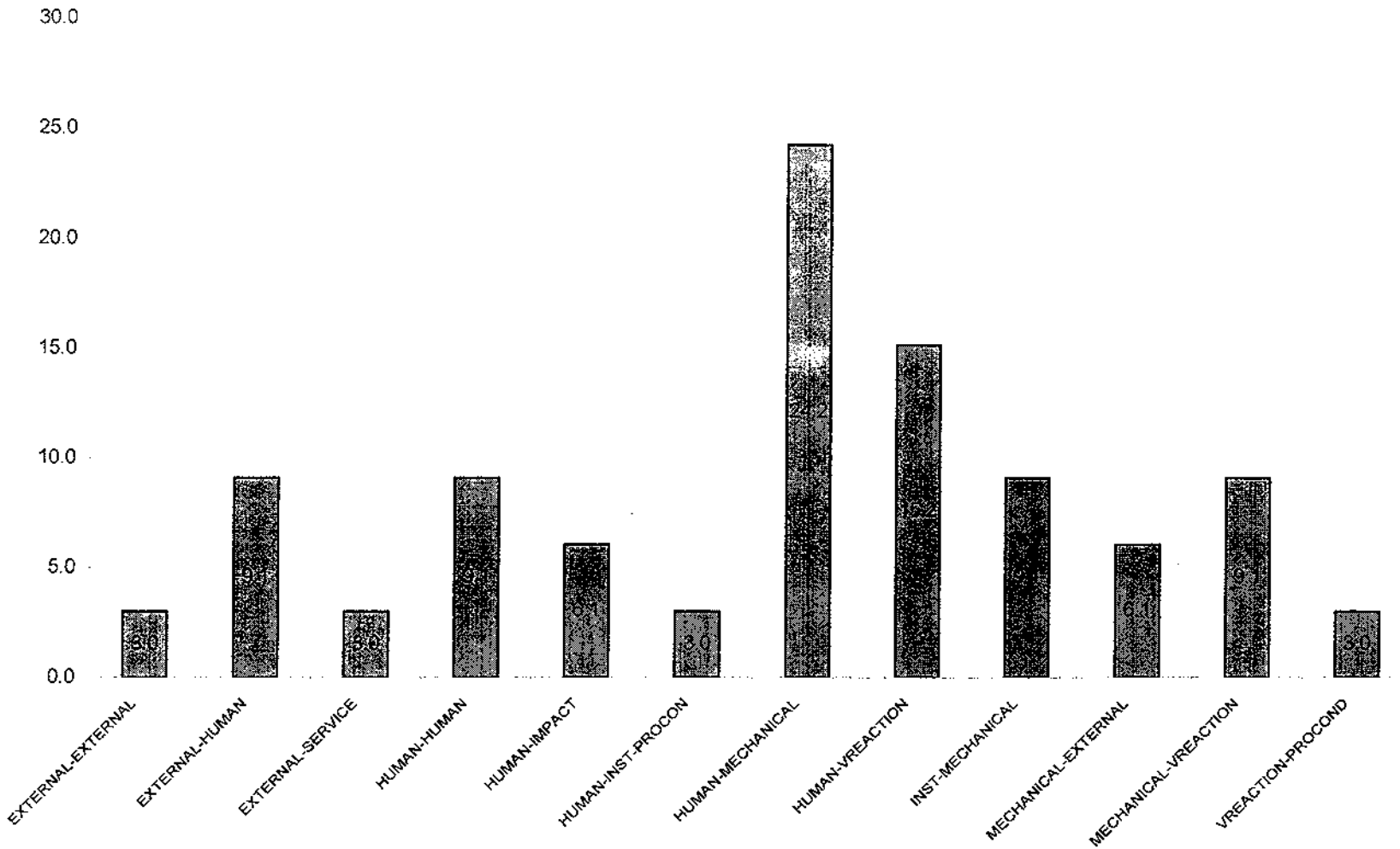

Figure 15
Breakdown of combined causes into general cause combinations

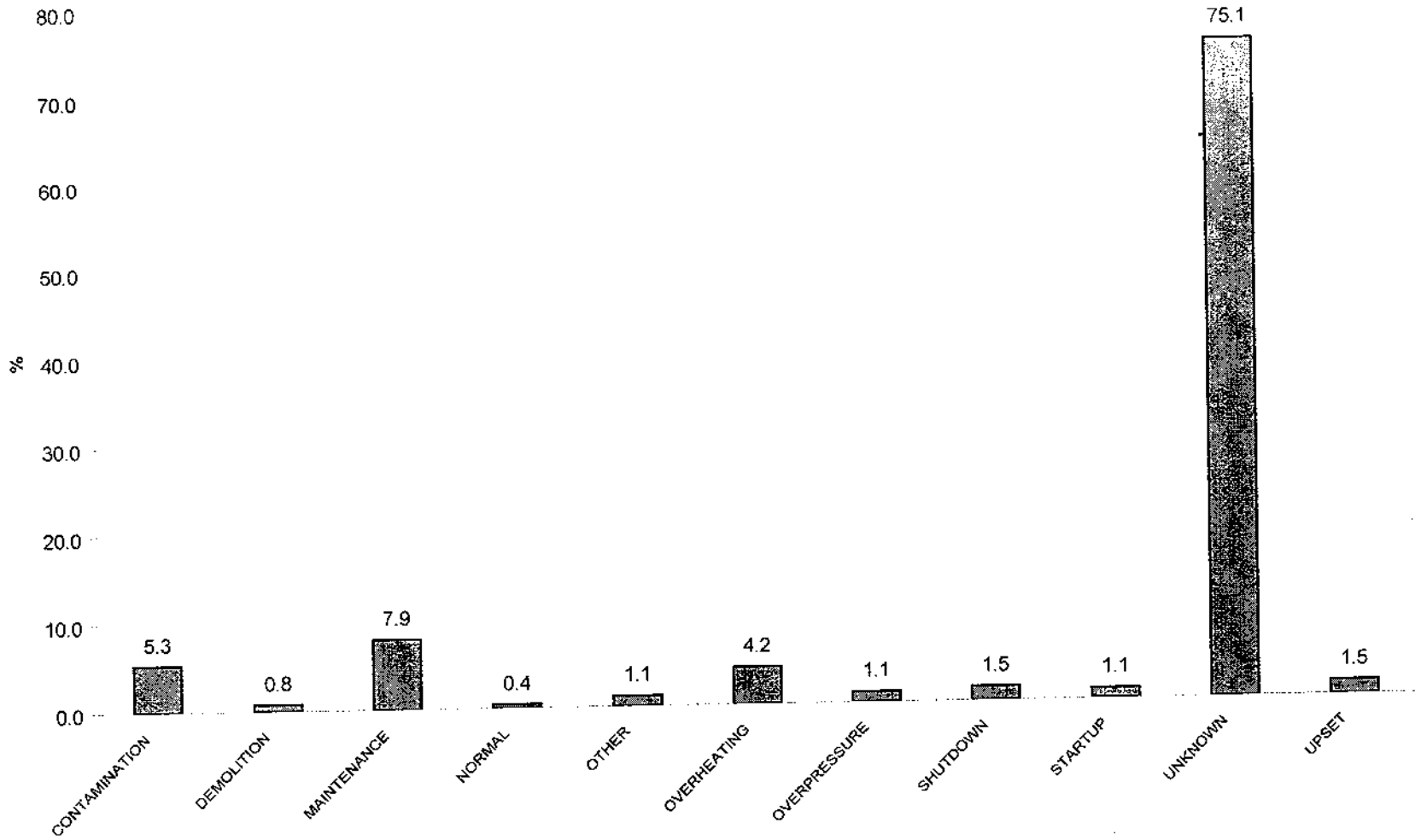

Figure 16
Breakdown by plant state (MHIDAS data)

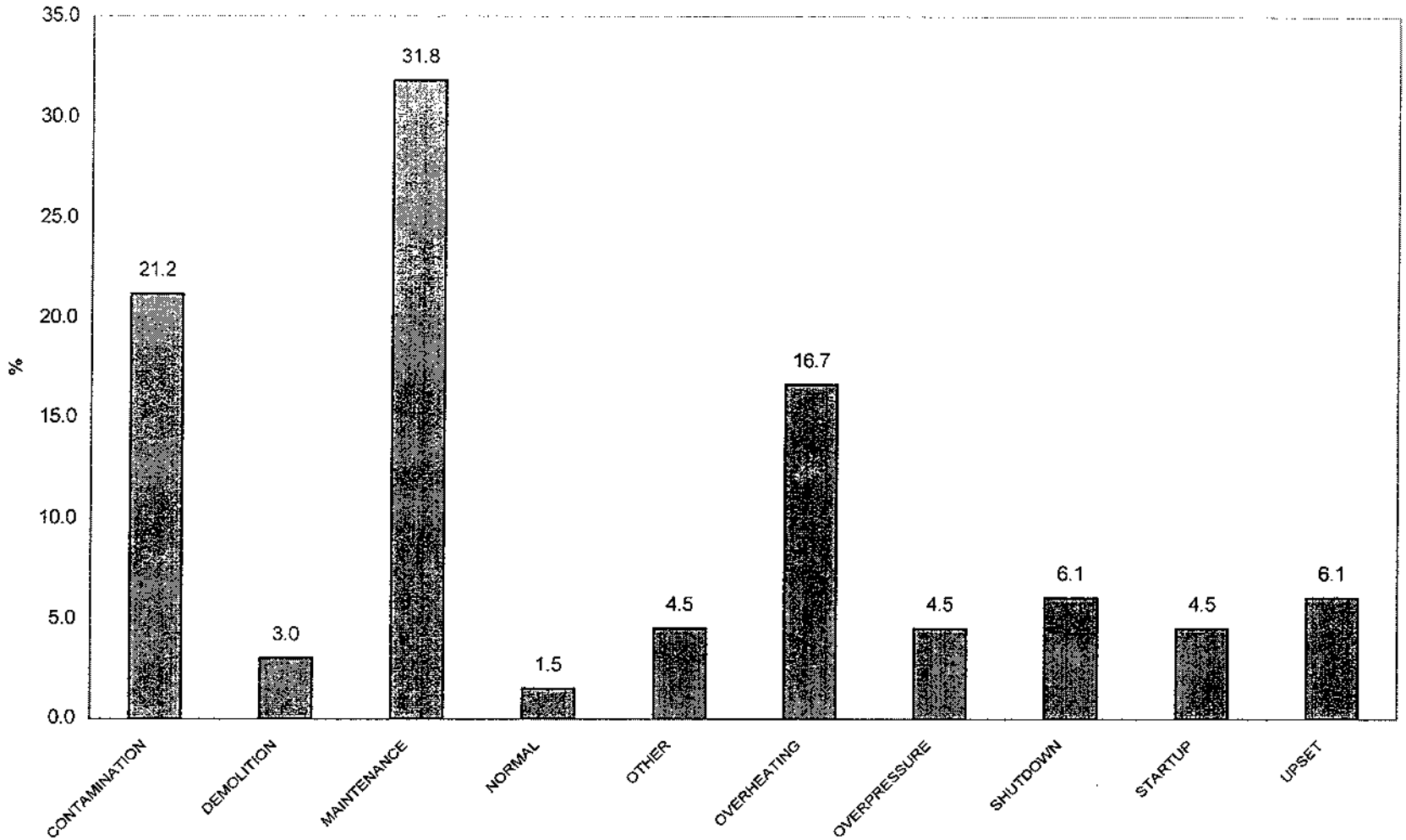

Figure 17
Breakdown of plant state for accidents where the plant state could be identified (MHIDAS Data).

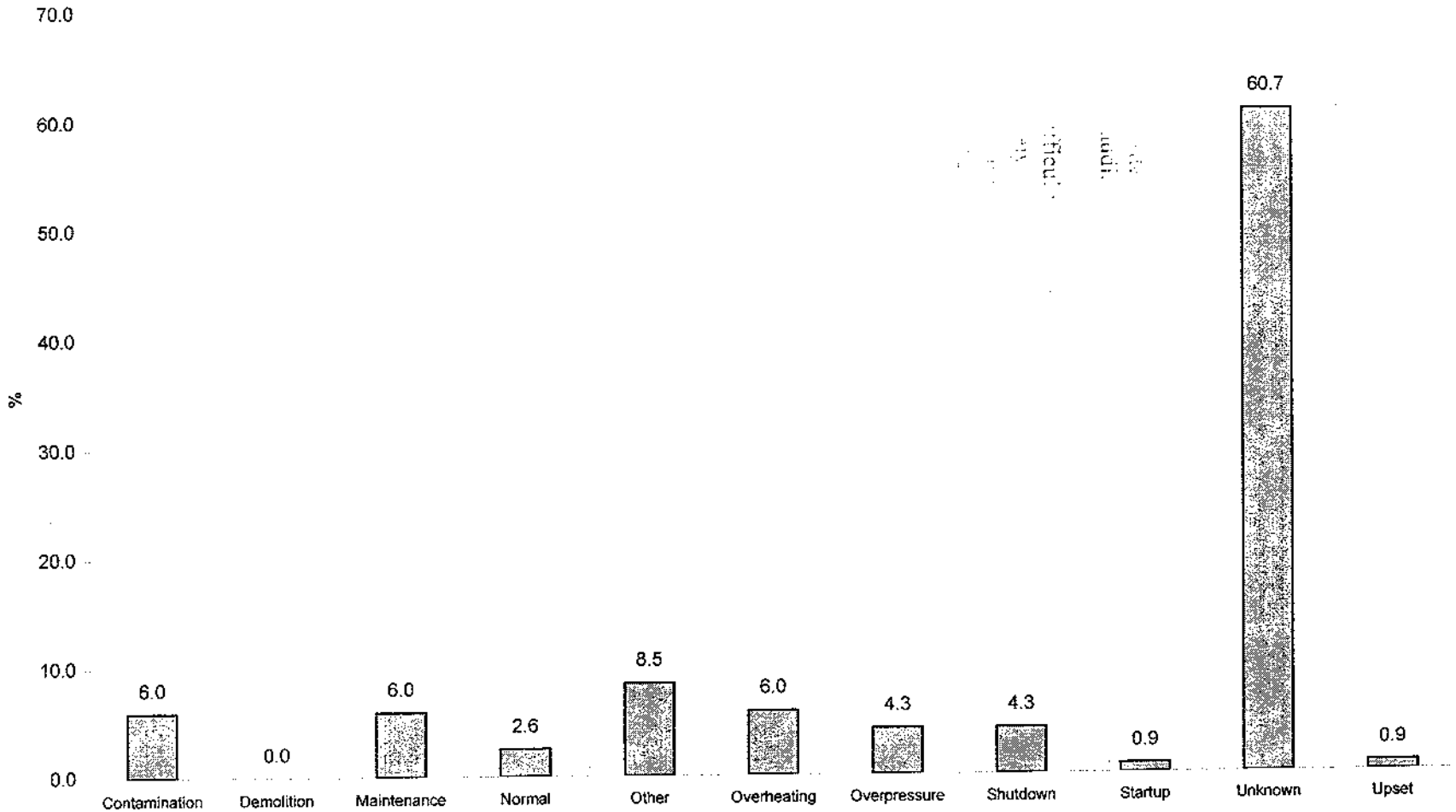

Figure 18
Breakdown by plant state (IChemE data)

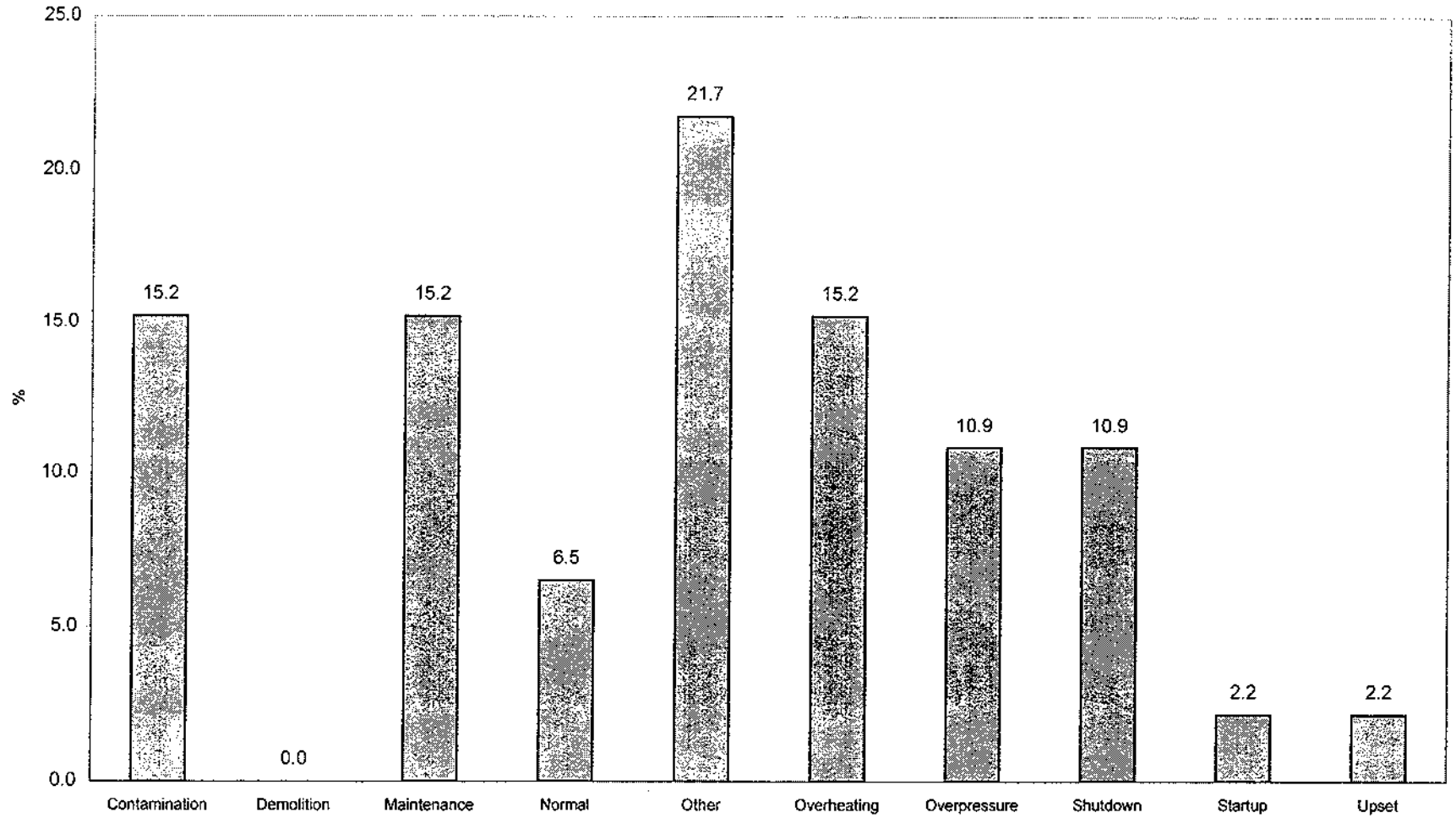

Figure 19
Breakdown by plant state for accidents where the plant state could be identified (IChemE data)

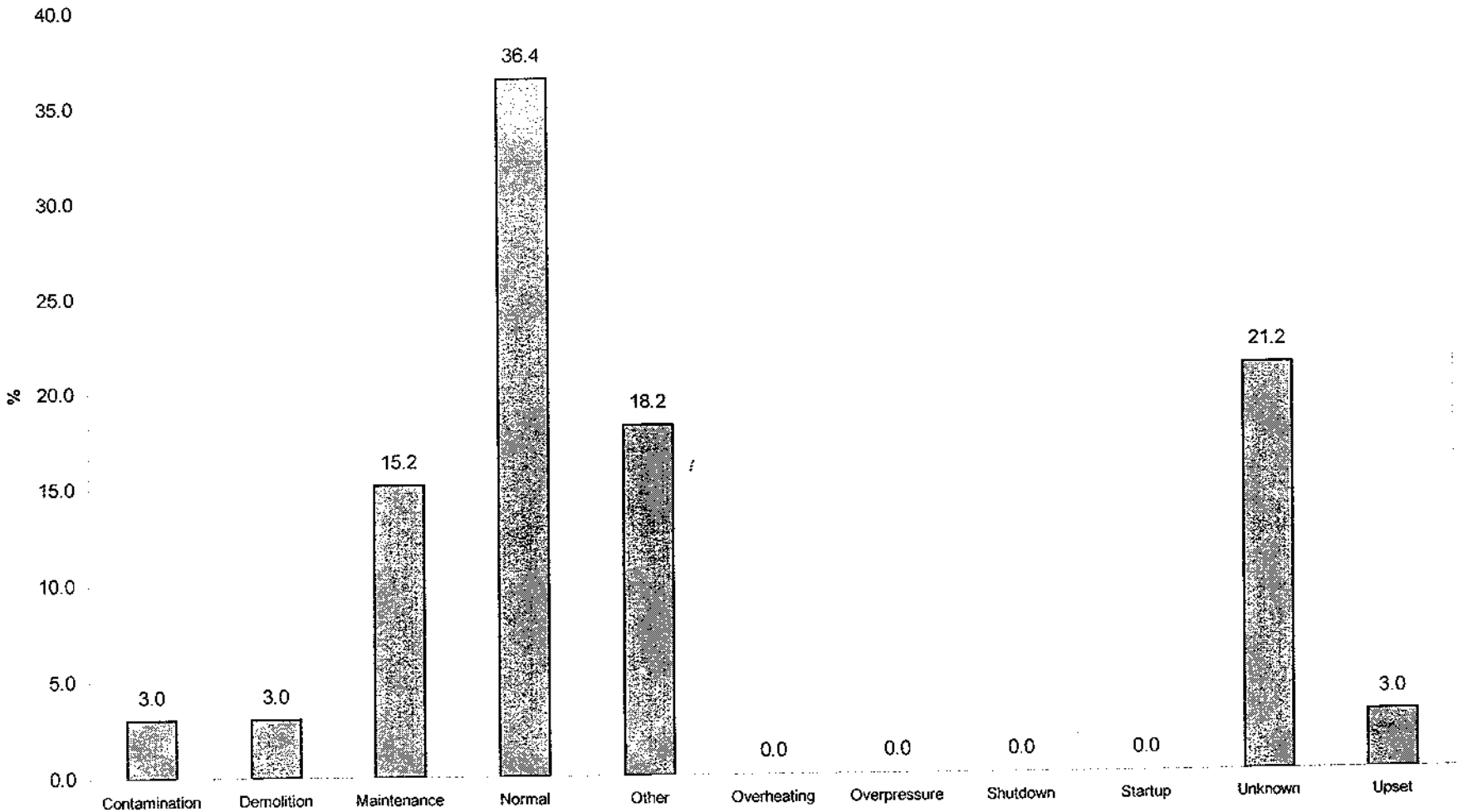

Figure 20
Breakdown by plant state (MARS data)

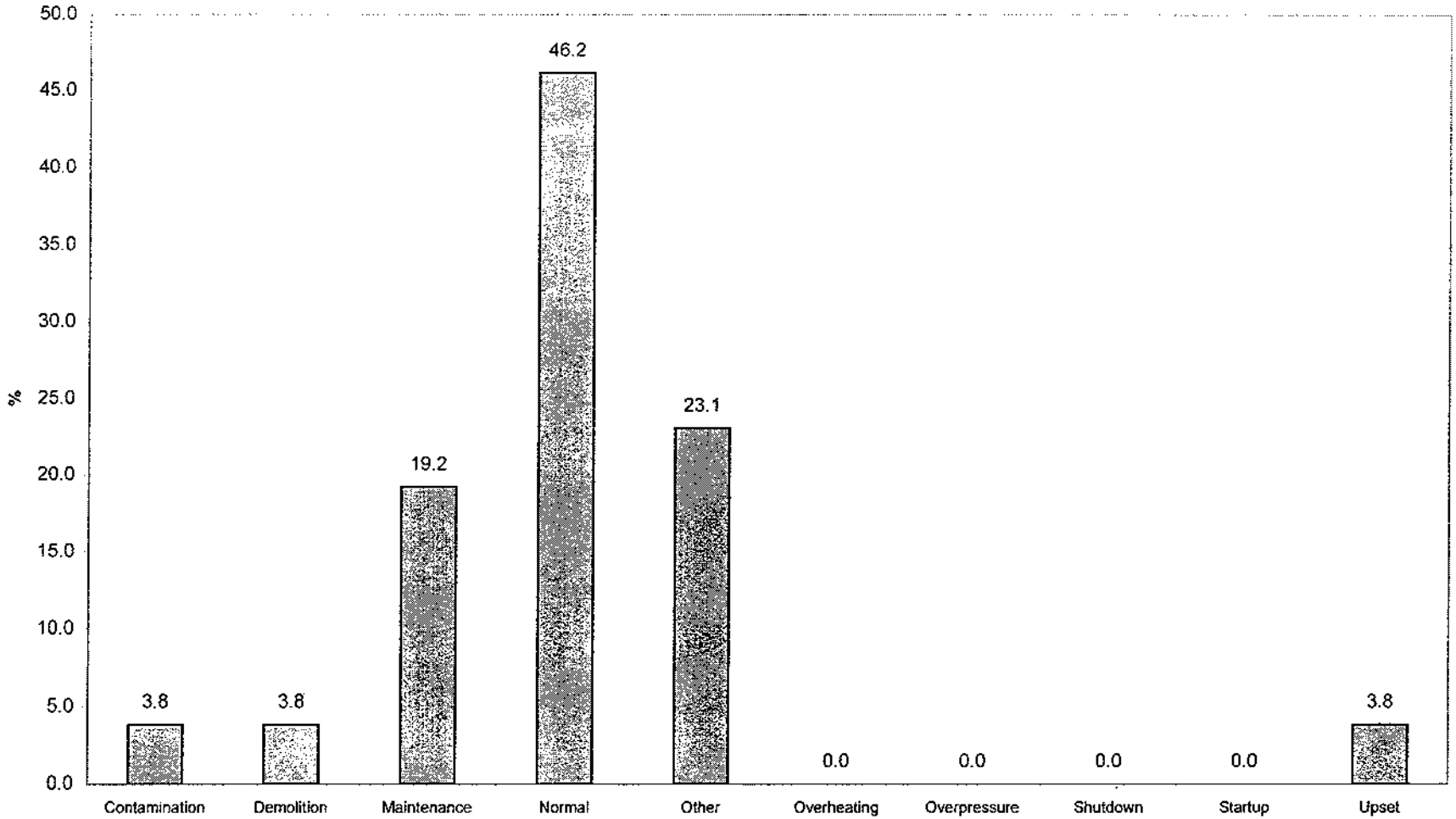

Figure 21
Breakdown by plant state for accidents where the plant state could be identified (MARS data)

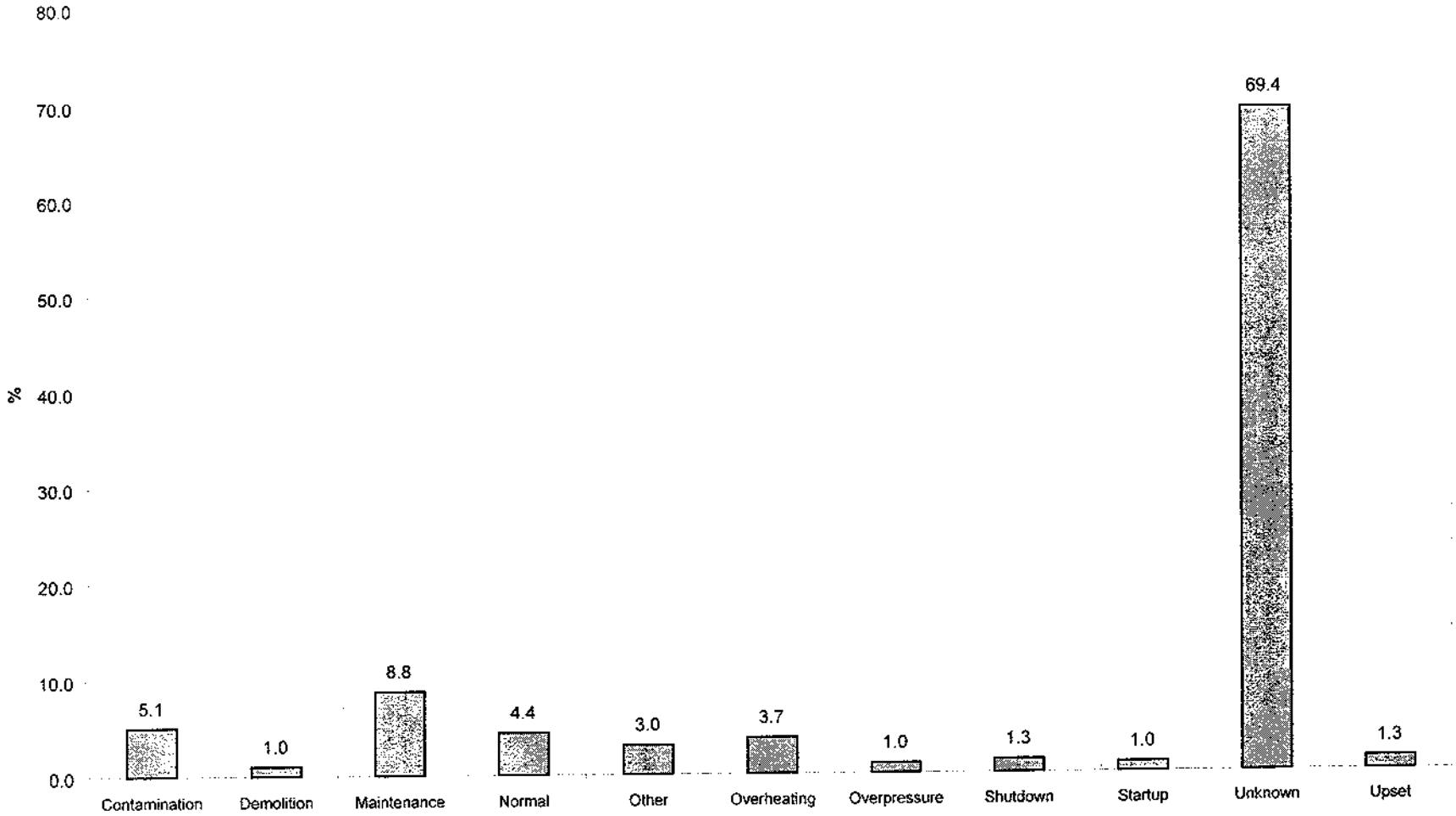

Figure 22
Breakdown by plant state (MHIDAS and MARS data)

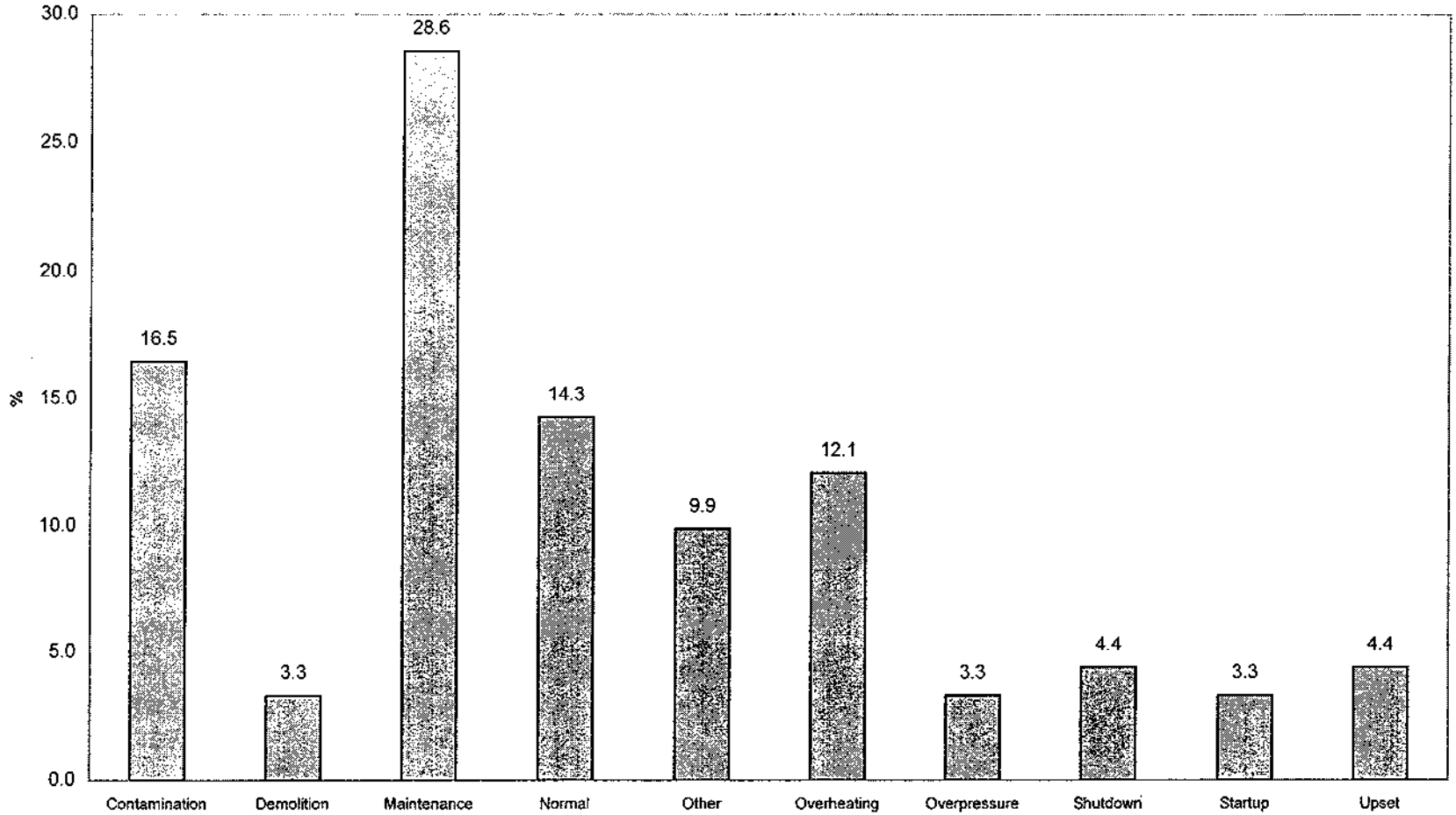

Figure 23
Breakdown by plant state for accidents where the plant state could be identified (MHIDAS and MARS data)

8. DISCUSSION

The focus within this research has been the uncertainty associated with deciding which events or phenomena to attempt to model within QRA studies of onshore process plant.

A survey of the literature on QRA methodology and an examination of published reports on QRA studies have revealed that, broadly speaking, approaches divide into two categories:

1. An approach that is similar in many respects to that adopted in the nuclear industry. This involves a hazard identification study of the plant under investigation (using techniques such as HAZOP or FMEA), selection of scenarios of interest (usually by expert judgement, and usually focussing on major events) and detailed quantification of those scenarios.
2. The so-called 'top down' approach, involving consideration of potential leaks and major releases from fractures of all process pipes, equipment and vessels. This typically generates a large number of scenarios, which may then be subjected to a selection process before producing a final list of events to be modelled. This approach usually involves the use of generic failure frequency data, since it would be impractical to use detailed techniques such as fault tree analysis to quantify the failure frequencies for the large number of scenarios produced.

The two approaches would probably converge if the hazard identification studies performed under the first approach were comprehensive and only limited screening of scenarios was performed.

A broad comparison of QRA methodology with accident theory has indicated that tools exist that would enable QRA to address most of the levels described within hierarchical or sequential accident models, although these tools are rarely used.

The hazard identification and incident selection process is critical to determining which events are modelled within a QRA study. Research has shown that hazard identification studies using the available techniques are unlikely to identify every hazard present. This situation is improved by using a combination of techniques rather than a single technique. This research also led to consideration of ways of addressing issues of uncertainty and quality in QRA. Four approaches to evaluating the quality of a given QRA were identified:

- Carrying out a complete parallel analysis on the same system.
- Carrying out a parallel analysis on some parts of the same system.
- Comparing the analysis with experience, including descriptions of accidents which have occurred in similar systems and/or the system under consideration.
- Examining the process used to conduct the analysis.

The last of these is analogous to evaluation of the quality policies and procedures of a supplier instead of testing samples of their product. It is the least demanding of resources of all of the methods listed. A checklist (known as QUASA) has been developed to assist in the evaluation. The section of the QUASA checklist dealing with identification of hazards contains questions to evaluate the extent to which abnormal plant conditions, management and human factors have been covered. The checklist also has sections relating to frequency analysis and consequence analysis. However, there is no section that deals explicitly with the process of incident enumeration and incident selection.

As stated above, the 'top down' approach to QRA usually involves the use of generic failure frequency data. The assumption made in using these data is that they 'include' contributions from all of the failure causes of interest. However, an examination of the sources of generic

failure frequency data for pipes and pressure vessels has shown that few of the sources contain information of direct relevance to the onshore process industry. Most of the data related to equipment used for steam, water or air service.

Data sources that draw predominantly upon information collected on such equipment are unlikely to include some of the failure causes that are of concern within the onshore process industry. Hence there is a strong possibility that should these generic failure frequency data be used in a QRA, the assumption that all relevant failure causes will be 'included' in the generic frequency would be incorrect.

A number of sources indicated the importance of the human error-related element of the frequency da The occurrence of human error is clearly influenced by the quality of safety management ther performance shaping factors, many of which are specific to the system under study. mpts to address this within QRA by application of modification factors derived from it results have been reported.

A further di ulty with the 'top-down' approach is that, although leak sources are comprehensi addressed, other, more complex failures may be neglected. This difficulty has not gone cognised. It is evident from published QRA studies that this problem is usually addr d by complementing the 'top-down' approach with other methods of identifying haz.rds, including:

- A consideration of the properties of the materials under investigation.
- An examination of the historical accident record for similar plant.
- More detailed hazard identification studies of particular areas of the plant.

At the consequence analysis stage, it is common practise to assume that the leak or failure occurs under otherwise normal conditions for the process. However, an analysis of three accident databases (MHIDAS, MARS and the IChemE Accident Database) has indicated that the proportion of accidents that occur when the plant is in some abnormal state may be 40% or more. A significant proportion of these 'abnormal states' appears to be associated with maintenance operations (but noting that the distinction between the normal and the abnormal is somewhat blurred in the case of maintenance). Previous studies by HSE of maintenance related accidents have indicated that 30% of such accidents had had the potential to present an off-site risk.

The extent to which the issues outlined above represent a cause for concern will depend on the scope and purpose of the QRA, as well as the level of complexity of the plant under investigation.

A QRA can never be expected to address all potential accidents at a given plant, but it should address all of those potential accidents that are relevant to the scope as defined. Thus, if the scope of the study involves calculation of the off-site risk, the QRA should consider all accidents with the potential for off-site effects. Given the results of the analyses of the accident databases and the previous HSE work on maintenance related accidents, it cannot be assumed that accidents occurring when the plant is in an abnormal state do not have the potential for off-site effects. Similarly, if the scope of the QRA study includes a calculation of on-site risk, then maintenance related accidents, for example, may clearly be of significance.

It could be argued that the range of accidents modelled within a QRA would be representative of the full range of accidents that might occur. For example, consider the situation where a vessel storing flammable liquid is analysed within a QRA. Typically, leaks or major failures of the vessel would be modelled, assuming some level of vessel contents, resulting in fires and explosions. It could then be argued that an explosion within the vessel during a

maintenance operation is 'bracketed' or adequately represented by the range of fires and explosions already modelled. This may indeed be the case, but whether or not this is satisfactory depends on the purpose of the QRA. If the QRA is simply to be used to give an estimate of the off-site risk, then the position may be satisfactory. If the QRA is to be used to make decisions concerning options for reduction of risk, then the position may not be satisfactory. The fact that events that have been modelled within the QRA assume otherwise normal conditions means that recommendations arising from the QRA are likely to relate to the normal operation of the plant. It is difficult to use the QRA to produce recommendations concerning abnormal plant operations such as upsets or maintenance, even though these areas could be significant.

It might be expected that simple plant (such as bulk storage of chlorine at water treatment works) would be less prone to accidents arising from certain abnormal states such as process upsets. No analysis of the accident records obtained from databases has been attempted in this regard.

9. CONCLUSIONS AND RECOMMENDATIONS

The analyses of accident databases indicate that the proportion of accidents occurring when the plant is in some abnormal state may be 40% or more. Maintenance appears to be a particularly important abnormal state.

Whether or not accidents occurring during maintenance or other abnormal states need to be considered explicitly within a QRA study depends to a large extent on the scope and purpose of the QRA, as well as the complexity of the plant being studied. This is thought to be particularly important for cases where the QRA is to be used for producing recommendations for risk reduction options.

Where necessary, this could be done by building upon the existing practise of supplementing the conventional 'top down' approach with other hazard identification methods. This could include a review of hazard identification studies performed for other purposes. Ultimately, as experience in performing QRA studies in this way develops, it may be possible to extend the generic lists of events used in the 'top-down' approach to include events occurring during some abnormal states.

No attempt has been made during this study to quantify the effect of excluding events occurring during abnormal plant states on the risk figures obtained from a QRA study. It is recommended that case studies be conducted to investigate this area further.

10. REFERENCES

Advisory Committee on the Safety of Nuclear Installations (ACSNI), (1993), 'Third report: Organising for Safety'. HMSO. London.

Anderson, M and Gould J H. "The Development at Site-Specific Failure rRates for Use in Risk Assessments of Major Hazard Sites". IChemE Symposium Series No. 141 Hazards XIII Process Safety – The Future 22nd-24th April 1997, Manchester.

Apostolakis G, Garrick B and Okrent D. "On Quality, Peer Review and the Achievement of Consensus in Probabilistic Risk Analysis". 1983. Nuclear Safety 24 (6) 792 – 800.

Arulanatham, D.C. and Lees, F.P. 1981. "Some Data on the Reliability of Pressure Equipment in the Chemical Plant Environment", *Int. J. Pres. Ves & Piping*, 9 (1981), pp 327-338.

Blything, K W & Parry, S T (1988), "Pipework Failures - A Review of Historical Incidents", UKAEA, SRD R441.

BS 8444: Part 3: 1996. IEC 300-3-9: 1995. "Risk Management Part 3. Guide to Risk Analysis of Technological Systems".

Bush, S.H. (1975), "Pressure Vessel Reliability", Journal of Pressure Vessel Technology, 97, 54, February.

Bush, S. H. (1988), "Statistics of Pressure Vessel and Piping Failures", Journal of Pressure Vessel Technology, 110/227, August.

CCPS. "Guidelines for Chemical Process Quantitative Risk Analysis". 1989.

CCPS. "Guidelines for Hazard Evaluation Procedures". 1992. 2nd Edition.

Clay, G A et al. "Risk Assessment for Installations where Liquefied Petroleum Gas (LPG) is Stored in Bulk Vessels Above Ground" 1988. J Haz Met. 20 (1988), 357-374.

CONCAWE Report No. 10/82, 1982. "Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry".

Conitini S et al., 1991. "Benchmark Exercise on Major Hazard Analysis", CEC Joint Research Centre, Ispra EUR13386EN.

Davenport, T.J. 1991. "A Further Survey of Pressure Vessel Failures in the UK", Reliability 91, London, June 1991.

Du Pont 1987. "Process Safety Management Reference Manual", 6th edition. E I du Pont de Nemours & Co., Inc., Wilmington DE 19898.

Dwyer, T and Raftery, A. (1991), 'Industrial accidents are produced by social relations of work: A sociological theory of industrial accidents', Applied Ergonomics 1991, 22.3, 167-178.

Garrick B J, 1982 in "On PRA Quality and Use" Ed. Okrent D, UCLA-ENG-8269.

GEAP (1964), "Survey of Piping Failures for the Reactor Primary Coolant Pipe Rupture Study", Report 4574, General Electric Atomic Power.

Gould J H and Andeson M. "Hose and Coupling Failure Rates and the Role of Human Error – Catastrophic Failure Rates. Final Report". Health and Safety Laboratory RAS/00/01. 2000.

HSE 1978. "Canvey an Investigation". HMSO.

HSE 1981. "Canvey: A Second Report". HMSO.

HSE 1987. "Dangerous Maintenance A study of maintenance accidents in the chemical industry and how to prevent them". HMSO.

HSE 1989. "Quantified Risk Assessment: Its Input to Decision Making". HMSO.

HSE 1995. "Generic Terms and Concepts in the Assessment and Regulation of Industrial Risks". Discussion Document.

HSE 1997. Data from 1/10/92-1/03/97, 'Offshore Technology Report - OTO 97 950'.

Hoyos, C. and Zimolong, B. (1988), 'Occupational Safety and Accident Prevention – Behavioural Strategies and Methods,' Elsiever.

Hurst N W 1988. "Immediate and Underlying Causes of Vessel Failures: Implications for Including Management and Organisational Factors in Quantitative Risk Assessment". IChemE Symposium Series No. 124.

Hurst, W. (1998), 'Risk Assessment – The Human Dimension', The Royal Society of Chemistry.

Hurst N W et al. 1991. "A Classification Scheme for Pipework Failures to involve Human and Sociotechnical Errors and their Contribution to Pipework Failure Frequencies". J Haz Mat 26 (1991) 159-186.

IAEA. "Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas". IAEA – TECDOC – 994. 1998.

Kellerman, O., and Seipel, H. G. (1967), "Analysis in the Improvement in Safety Obtained by a Containment and by Other Safety Devices for Water-Cooled Reactors," IAEA SM-89/8 T.P. 89.

Kletz, T. (1999), 'HAZOP and HAZAN', IChemE.

Okrent D, Apostolakis, G, Whitley, R and Garrick, BJ. "PRA Quality and Use", 1982.

Pape R P and Nassey C. "A Basic Approach for the Analysis of Risks from Major Toxic Hazards". IChemE Symposium Series No. 93. P367-388.

Pitblado R M. "International Risk Assessment Case Studies" in "Risk Assessment and Management Handbook for Environmental, Health and Safety Professionals". Eds. Kolluru R, Bosell, S, Pitblado R and Stricoff S. McGraw Hill. 1996.

Pitblado, R M, Williams, J C and Slater D H. "Quantitative Assessment of Process Safety Programs". 1990. "Quantitative Assessment of Process Safety Programs". Plant/operations Progress 9 (3), 169-175.

Reason, J. (1998), 'Managing the Risks of Organisational Accidents', Ashgate ISBN 1-84014-105-0.

Rijnmond Public Authority 1982. "Risk Analysis of Six Potentially Hazardous Objects in the Rijnmond Area, A Pilot Study". D. Reidel Publishing Company.

Rouhiainen, V 1987. "Turvallisuus – ja riskianalyysin laadun arviointi (Evaluation of the quality of safety and risk analysis)". Tampere, Tampere University of Technology (techn lic. Work).

Rouhiainen, V 1990. "Quality Assessment of Safety Analysis". VTT Publication 61.

Rouhiainen, V 1992. "QUASA: A Method for Assessing the Quality of Safety Analysis". Safety Science 15 (1992), 155-172.

Rouhiainen, V 1993. "Importance of the Quality Management of Safety Analysis". Reliability Engineering and System Safety 40 (1993) 5-16.

Rouhiainen, V and Suokas, J. "Planning and Evaluation of the Quality of Safety and Risk Analysis". 1989. 6th International Symposium Loss Prevention and Safety Promotion in the Process Industries, Oslo, Norway June 1989. Norwegian Society of Chartered Engineers.

Smith, T.A. and Warwick, R.G. 1981. "A Survey of Defects in Pressure Vessels in the UK for the Period 1962-78, and its Relevance to Nuclear Primary Circuits", UKAEA Safety and Reliability Directorate Report SRD R203.

Suokas J. "Evaluation of the Validity of Four Hazard Identification Methods with Event Descriptions". VTT Research Report 516.

Suokas, J. "On the Reliability and Validity of Safety Analysis" 1985. VTT Publications 25.

Taylor, JR 1982 "Evaluation of Costs, Quality and Benefits for Six Risk Analysis Procedures", RISØ Internal Report N 14-82.

Taylor, J R et al. "A Design Review Approach to Safety Analysis" 1986. 5th International Symposium Loss Prevention and Safety Promotion in the Process Industries.

Turner, B.A. (1978), 'Manmade Disasters', Wykeham.

USNRC (1975), "Reactor Safety Study", Appendix III - Failure Data, US Nuclear Regulatory Commission, NUREG-75/014, WASH-1400, October 1975.

World Bank Technical Paper No.. 55 1988. "Techniques for Assessing Industrial Hazards – A Manual". Technica Ltd.

Printed and published by the Health and Safety Executive
C1 10/00

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

RETAIL
HSE priced publications
are available from
good booksellers

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

CRR 293

£20.00

ISBN 0-7176-1849-8