Journal of Hazardous Materials, 26 (1991) 159–186
Elsevier Science Publishers B.V., Amsterdam

A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies

N.W. Hurst

Health and Safety Executive, Broad Lane Sheffield S3 7HQ (Great Britain)

and

L.J. Bellamy*, T.A.W. Geyer* and J.A. Astley*

Four Elements Ltd., 25 Victoria Street, London SW1 HO2X (Great Britain)

(Received March 20, 1990; accepted July 2, 1990)

Abstract

This paper analyses the contribution of human error and sociotechnical failures to pipework failure frequencies. A failure classification scheme has been developed and used to analyse about 500 reported incidents involving failures of fixed pipework on chemical and major hazard plant. An important objective of the classification scheme was to make a distinction between human error as a direct or immediate cause of failure and failures of the sociotechnical system which can be either the underlying origin of the failure or a failure of a potential preventive mechanism. This has led to the development of a three dimensional classification scheme by which the 500 accidents are analysed. Results are presented for the percentage contributions of different direct (or immediate) causes, origins of failure (underlying cause) and failures of preventive mechanisms. The results are also presented in a matrix form by which the importance of specific recovery mechanisms applied to certain types of failure can be identified. The work shows that about 90% of the analysed incidents could have potentially been prevented by suitable preventive mechanisms which in theory are within the scope of management control. In addition a hierarchical scheme of accident causation is considered in which the direct cause of the accident is the carrier or symptom of underlying problems in the sociotechnical system. The implications of the classification schemes are considered with respect to the contributions which compose the generic failure rates which are used in the calculation of risk for major hazard plant.

1. Introduction

The British Health and Safety Executive (HSE) uses the results from quantified risk assessment (QRA) calculations to provide advice to local planning authorities about land-use planning around major hazard sites. The QRA calculations are carried out using the HSE risk assessment tool (RISKAT) and make use of generic failure rates [1]. These incorporate failure rate data from

*This work was carried out while these authors were employed by Technica Ltd, Lynton House, 7/12 Tavistock Square, London WC1H 9LT.

0304-3894/91/$03.50

all causes which necessarily include human error and failures of management control. Thus human factors, in a general way, are implicitly included in QRA when the generic failure rate data are applied in a site-specific way according to details of vessel sizes, pipe sizes and process conditions [1].

The use of generic failure rate data in the calculation of risk make it important to clarify how these management, organisational and human factor issues are taken into account. Can these generic failure rates be modified in a valid way to allow the overall quality of safety management to be quantified? Would it be possible to apply a factor to the generic risk figure based on an assessment of management systems at a particular installation ? Such an approach would make transparent any judgement made about the size of these contributions to the risk figures. Of course planning decisions have consequences that are measured over years if not decades and cannot be dependent upon changes in management except within very narrow limits. Nevertheless the extent to which management, organisational and human factors contribute to the risk is not made explicit.

The HSE has started to investigate these issues by commissioning research. It is implicit that the research will look, in due course, at the validity of using audit schemes, which are designed to make a measure of the quality of management systems, for the purpose of modification of risk calculations. However, in the first instant it is important to understand how generic failure rates are made-up of components from different contributory factors. As a first step the factors involved in a limited data set have been investigated and tentative implications for future work are also developed.

This paper reports the results of a collaborative study between HSE and Technica which has analysed over 900 reported incidents involving failures of fixed pipework on chemical and major hazard plant [2]. In about 500 cases sufficient data was available to fully classify the incident using the scheme developed here. It represents a first attempt to categorise and quantify the extent to which human factors are included in generic failure rate data. An important part of the work has involved the development of a failures classification scheme, which is used to analyse recorded incident accounts. This categorisation includes not only direct (immediate) causes of failure (e.g. operating error) but also the origins of failure (basic or underlying cause) (e.g. bad design) and failure to take preventative action to recover unsafe conditions (e.g. task checking not carried out).

2. The sociotechnical system

The sociotechnical system emphasises the importance of both the human and technical components of the whole system, in this case the chemical or major hazard plant. It takes account of the individual, social and organisational aspects which affect human behaviour and which ultimately influence

system performance. Some of the early work [3,4], began with an examination of the individual, group and organisational behaviour which commonly characterised accidents.

Later came the development of human reliability techniques such as the influence diagram approach [5] which provides a method of modelling some of the major sociotechnical influences within a system which affect successful task completion.

Large scale accidents may be reported in sufficient depth to enable a detailed analysis of these sociotechnical processes and accident analysis which attempts to clarify the relevance of the sociotechnical system has highlighted a number of areas which are repeatedly involved in accident causation [6–8] for example communication problems and incompatible goals (for example between production and safety).

One characteristic of the sociotechnical system failures is that a mismatch develops between the actual status of a system and its perceived state. From the point at which a mismatch occurs, the accident "incubates" [4], sometimes for years. In a complex technological system, this mismatch can easily remain hidden [9]. Failure to deal with the causes of mismatch has the potential for repeated failures. Hence, one would expect to find that organisations with a high accident frequency have underlying problems in the sociotechnical system. Such problems may be on a large scale, for example economic pressures may be imposed by changes not directly under the control of a particular organisation. Nonetheless, these must be responded to appropriately. Alternatively, poor working practices may develop within particular groups in an organisation because the process of setting and maintaining group standards has been allowed to lapse or is not effectively enforced. Quite often, communication problems within an organisation or between different groups working on the same part of the system have provided a setting which has enabled a mismatch to develop [10].

With the increasing awareness of the importance of sociotechnical system failure in accident causation, the need is to consider both human error at the operating level and also at levels more remote from the plant operation. These more remote levels are relevant not only in terms of their effect on human reliability, but also as an influence on the reliability of plant components via design, manufacture and maintenance considerations. Recently the HSE has published a booklet [11] which begins to look at some of these important issues "Human Factors in Industrial Safety". It provides an examination of the roles of organisations, jobs and individuals in industrial safety and a practical guide to control.

3. Development of a failure classification scheme

3.1 Classifying human causes of failure

Examination of actual incidents in relation to pipework failure classification schemes which have been used in the past [12,13] suggested that a ready made

scheme for the purposes of the present study did not exist. There was confusion between the direct (immediate) cause, the origin of failure (basic/underlying cause) and any possible recovery from unsafe conditions. In addition there was an absence of transparency as to how the classifications were derived and the thinking behind them.

An important objective of the classification scheme was to make a distinction between operating error as a direct cause of failure leading to loss of containment and sociotechnical failures which may be both the underlying cause of failure or the failure of a potential preventive mechanism. This distinction is also made by the terms 'active human failures' and 'latent human failures' [14].

Operating error as a direct cause of failure, is therefore defined by incidents such as turning on the wrong valve or connecting the wrong wire. These are skill based or rule based slips or well intentioned mistakes which correspond mainly to the automatic or schematic ways of thinking [15]. These are active human failures.

There is also a need to define a range of underlying causes of failure; bad design, manufacture/assembly, construction/installation, operation and maintenance. These types of failure are defined as 'sociotechnical' failures which relate to systemic considerations, i.e. are a function of the whole system. These are latent human failures.

Also within this sociotechnical umbrella come some failures to recover: no hazard study carried out, no human factors review, task checking/testing omitted and routine checking and testing not carried out. Similarly these are latent human failures.

3.1.1 Direct or immediate human causes

The most obvious direct (immediate) human causes of a release occur as operator procedural errors e.g. opening a wrong valve or opening a line that has not been effectively isolated. In such cases, where procedural failure is the only cause of a release, pipework or in line equipment does not actually fail but a release occurs as a direct result of operating error. This is not to imply 'guilt' or ultimate responsibility for the action, simply to define a type of incident in which the immediate cause is a human one.

However, sometimes an operating error may lead directly to pipework or in line equipment failure e.g. feeding wrong materials into a process resulting in an explosion. For these incidents, operating error is a necessary condition for pipework failure, but the pipework or in-line equipment ultimately fails by some other mode, such as overpressure. Incidents of this type were classified under both operating error and the other direct cause of pipework/equipment failure (e.g. overpressure). Usually in such cases both immediate causes occur virtually simultaneously.

3.1.2 Sociotechnical failures

(a) Basic/underlying cause. Ideally, incident descriptions would describe what the underlying causes of failures were. However, because of the uncertainty reflected in the quality of the available incident data, it was generally only possible to determine the point in the life of a plant at which a failure had its origins. For example, it was possible to infer that an error occurred at some point in the design process but not why. When looking for the underlying cause of pipework failures, sociotechnical errors were therefore best classified according to the contexts in which these errors originated (e.g. design, maintenance, normal operations, installation etc.).

In breaking down immediate causes of failure (overpressure, corrosion, impact etc.) into descriptions at a more detailed level, it became easier to determine what the underlying causes of failure were likely to have been. However, tracing a failure back to its origins by examining this finer breakdown required judgement as well as an understanding of how these immediate causes of failure might arise.

Some underlying causes of failure could not be attributed to sociotechnical error, in particular unusual natural events such as earthquakes, lightning and floods. However, extreme temperature conditions were regarded as being potentially avoidable in terms of their effects on pipework – in particular freezing weather.

(b) Human failure to prevent potential release conditions developing. Failure to prevent conditions which could ultimately lead to a release is also sociotechnical error. Even if potential failure conditions have already arisen, there can be opportunities to recover these situations and return the system to a safe state. This is rarely fully considered when classifying incident causes and has never been examined systematically.

Obvious examples are checking that a task has been carried out correctly (e.g. checking the installation of equipment) and routine inspections (e.g. for visible corrosion). Designs can also be checked (e.g. by HAZOP), and man-machine interface and procedures evaluated in human factors reviews or human reliability assessments. All these recovery (preventive) mechanisms require both identification of an unsafe condition and follow-up activity to correct it.

For any release to occur it was considered that there must have been either a failure to prevent potential release conditions developing or the situation was not recoverable (as in the case of an earthquake fracturing a live pipe).

3.2 A three-way classification scheme

Because the human factors causes of failure could be classified in the three different ways described in the previous section, it was necessary to develop an

overall scheme that would accommodate this. This section gives an overview of the developed scheme. Appendix 1 and 2 describe the classification system in detail. Appendix 1 considers the immediate causes of failure, while Appendix 2 considers the underlying causes of failure and the preventive mechanisms.

Figure 1 summarises the final classification that was derived. This scheme consists of a number of layers of immediate cause. Each immediate cause was overlaid with a two-way matrix of underlying cause of failure times preventive mechanism. Essentially, this gives a 3D scheme whereby every incident is classified in three different ways, locating it at some point within the 3D space shown in Fig. 1 (e.g. corrosion due to design error, not recovered by routine inspection).

The scheme allowed contribution counts to be made in a number of different ways. For example, the vertical column indicated in Fig. 1 includes all immediate causes whose origin was domino effects with unknown recovery failures.

Any incident could be placed in more than one causal category (e.g. overpressure and operating error; design and maintenance; HAZOP and human

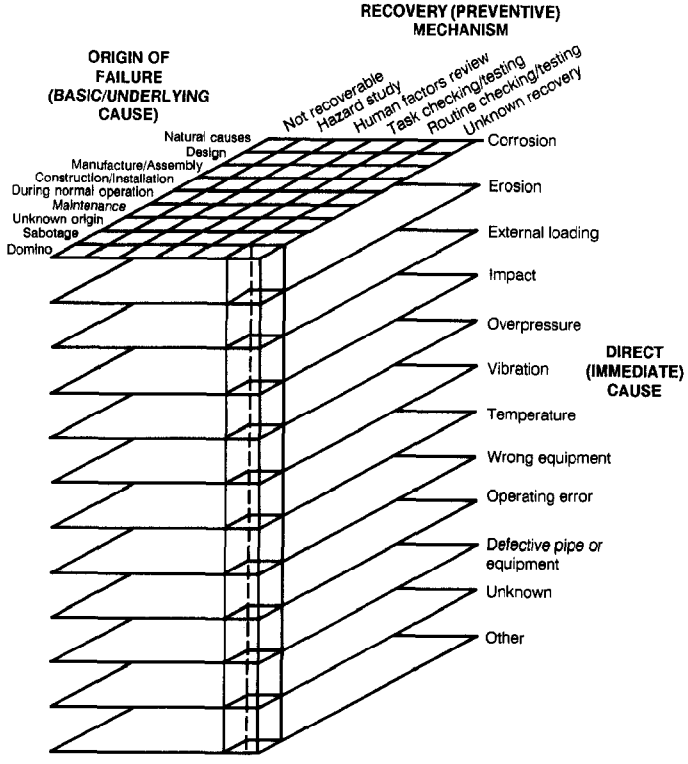

Fig. 1. Classification scheme for pipework failures. The scheme consists of a number of layers of immediate causes (e.g. corrosion). Each immediate cause is overlaid with a two-way matrix of underlying cause of failure and preventive mechanism.

factors review). For immediate causes, there were no limits to the number of alternatives. For the underlying cause times preventive mechanism matrix, the alternatives were limited to two as further numbers of alternatives were considered unnecessary.

Multiple causes were appropriately coded to enable frequency counting to be carried out. In this way, no event should be double counted. For shared causes 1/2, 1/3, 1/4 or 1/6 scores were applied as appropriate. For example if for one incident there were 3 immediate causes and 2 underlying cause × preventive mechanisms then the incident would have 6 points in the 3D space each of value 1/6.

This method ensures that counting accurately reflects the causal contribution and not the frequency of accidents to which the event contributed. The latter strategy would have constrained classification of an incident to only one point in the 3D space. Unless otherwise stated, all the data reported in this section are therefore causal contribution scores not incident frequencies.

Overall, contribution counts could be carried out as follows:

(1) Total number of incidents.
(2) Contribution of each immediate cause.
(3) Contribution of each underlying cause of failure.
(4) Contribution of each preventive mechanism.
(5) Contribution of each underlying cause of failure × preventive mechanism category (summed across all immediate causes).
(6) Contribution of each underlying cause of failure × preventive mechanism category (for each immediate cause).

The scheme developed may be compared with the 'Systematic Cause Analysis Technique' published by the International Loss Control Institute to improve accident investigations [16].

4. Application of the classification scheme

4.1 Immediate causes

Figure 2 shows a breakdown of the 'Immediate Cause' contributions to the analysed incidents. The highest contribution (31.9%) was for 'Defective Pipe or Equipment' (cause unknown), where the only information was the type of equipment that failed (pipe, valve, etc.). If this is added to the 'Unknown' category, then the total for all unknown Immediate Causes of failure is 41%. (The total number of incidents was 921, but the immediate cause was known for 543).

If these unknown causes are removed, operating error was then the largest known direct contributor to incidents (30.9% of all known causes). Overpressure (20.5%) and corrosion (15.6%) are the next largest categories of known causes. The other causes have relatively much smaller contributions, with erosion being the smallest (1.3%).

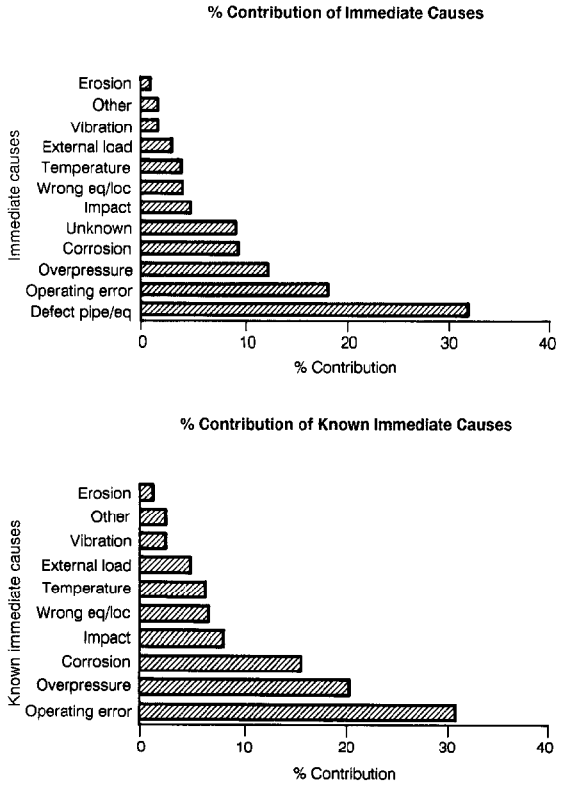

Fig. 2. Percentage contribution of immediate causes to pipework failures. Top diagram includes unknown causes and defective pipe or equipment where the only information was the type of equipment which failed. The bottom diagram is the percentage contribution of known immediate causes.

The other major areas of human contribution to immediate causes are in 'Impact' and 'Wrong In-Line Equipment or Location'. Human related 'Impact' events, mainly vehicle impact, with some human initiated dropped loads and human impact, had a contribution of 5.6% of all known causes.

For Wrong In-Line Equipment, incorrect installation at the correct site contributed another 4.5% of the known cause contributions, e.g. installing something the wrong way round, screwing something up too tightly or having it too loose, bad welding etc. Table 1 summarises these results for the human contribution to immediate causes of failure.

For many of the sub-categories of Immediate Causes (see Appendix 1), there is also a human contribution which cannot be distinguished in some cases from other Immediate Causes (e.g. unexpected reaction leading to overpressure). The value of 41% is therefore probably an underestimate.

4.2 Underlying cause of failure and preventive mechanism

The underlying cause of failure for all incidents and preventive mechanisms are shown in Fig. 3. The percentages are based on removing unknown origins

TABLE 1

Human contribution to the known immediate causes of failure

Cause	Human contribution (%)
Operating error	30.9
Human initiated impact	5.6
Incorrect installation of equipment at correct site	4.5
Total	41.0

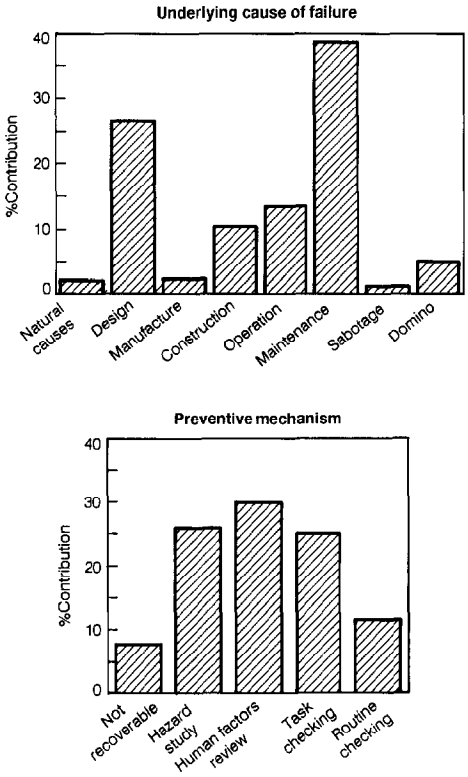

Fig. 3. Percentage contributions of underlying cause of failure and preventive mechanism for pipework failures.

of failure, leaving 502 records and removing unknown preventive mechanisms, leaving 492 records. The percentages for the complete matrix are shown in Table 2. Figure 4 illustrates the data in Table 2. It can be seen from Table 2 that the largest contributions for underlying causes of failure are Maintenance (38.7%) and Design (26.7%) and that Human Factors Review (29.5%), Hazard Study (25.4%) and Task Checking/Testing (24.4%) are all large preven-

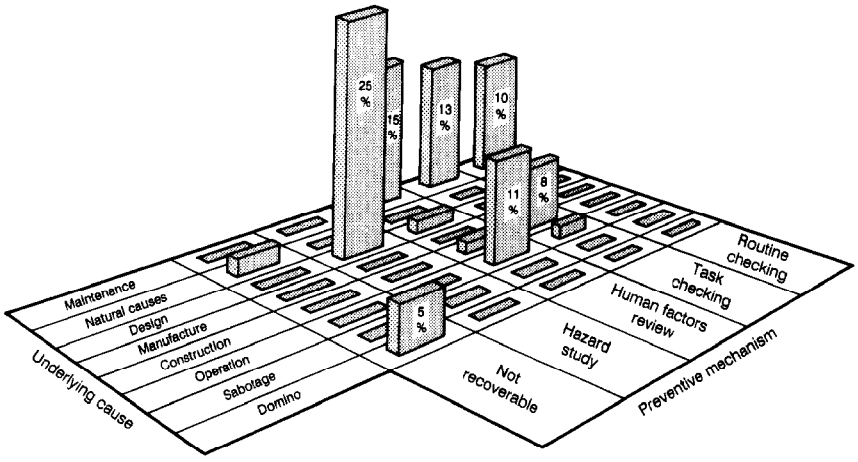

Fig. 4. Percentage contributions of pipework failures according to underlying cause of failure and preventive mechanism.

TABLE 2

Percentual contribution of failures according to origin of failure and recovery failure (unknown origin/unknown recovery cell removed) 502 records

Underlying cause of failure	Preventive mechanism						Total
	Not recoverable	Hazard study	Human factors review	Task checking	Routine checking	Unknown recovery	
Natural causes	1.8			0.2			2.0
Design		24.5	2.0		0.2		26.7
Manufacture				2.4			2.4
Construction	0.1	0.2	1.9	7.5	0.2	0.4	10.3
Operation		0.1	11.0	1.6	0.2	0.8	13.7
Maintenance		0.4	14.5	12.7	10.3	0.8	38.7
Sabotage	1.2						1.2
Domino	4.5	0.2			0.3		5.0
Total	7.6	25.4	29.5	24.4	11.1	2.0	100

tive mechanisms. In fact these 4 areas of management control (preventive actions) have the potential to prevent 90% of the analysed accidents.

Figure 4 and Table 2 show that hazard study of design could potentially recover 24.5% of failures, whilst human factors review of maintenance and operations could recover 25.5% with task checking potentially recovering a further 14.3%.

Although 41% of all known immediate causes of failures are human ones, the final barriers to failure are the preventive mechanisms and these are almost

entirely human and within the domain of management control. Only a 7.6% contribution to failure was classified as not recoverable (Table 2).

Of course, this does not take account of the fact that economic constraints may limit the use of such recovery mechanisms. Nonetheless, the emphasis on hazard studies (particularly of the design of the plant), human factors reviews (particularly of support for maintenance and operational activities) and checking of completed tasks (particularly maintenance) suggests the importance of these management control activities in reducing pipework and in-line equipment failures. Improvements in routine hardware inspection (e.g. for visible corrosion) can be expected to recover 11% of known contributors whereas these other 3 strategies in combination could, in theory, recover 80%. Clearly a broad based inspection of a plant (by, for example, regulators) which includes a systematic review of safety related management procedures such as permit to work systems, has an important part to play.

5. A hierarchical scheme of accident causation

The concept clearly illustrated by the analysis of these data and a study of the relevant literature is one of an immediate cause acting as the carrier or symptom of underlying problems in the sociotechnical system (see for example Refs. [14,17–19]. This suggests that there exists a hierarchical scale of accident causation from the most immediate causes to increasingly remote causes (see 'The ILCI loss causation model' Ref. [19]). This does not imply a sequence of events in time but illustrates the potential effects of actions or inactions at various levels within the sociotechnical system on the safety of a plant. This concept of different levels of causes is represented in Fig. 5. Thus the sociotechnical "pyramid" (Fig. 5) represents levels of increasingly remote causes from an accident event. This is not remoteness in time, rather that the connection between an event and its cause becomes more remote as the number of intervening variables increases. When an operator incorrectly opens a valve and this causes a release, the opening of the valve 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 the operator was not adequately trained, etc. These causes are more remote. Even more remote, for example, is where management may not have allocated sufficient training, and this may have been due to inadequacies in prioritising brought about by severe production pressures. It is in this sense that there is a hierarchy of causes.

The levels of the hierarchy in Fig. 5 are:

Level 1 – Engineering reliability. This concerns the design of the hardware of a plant and the limits within which it is to operate. It excludes aspects such as the man–machine interface (MMI) which directly impinge on operator re-

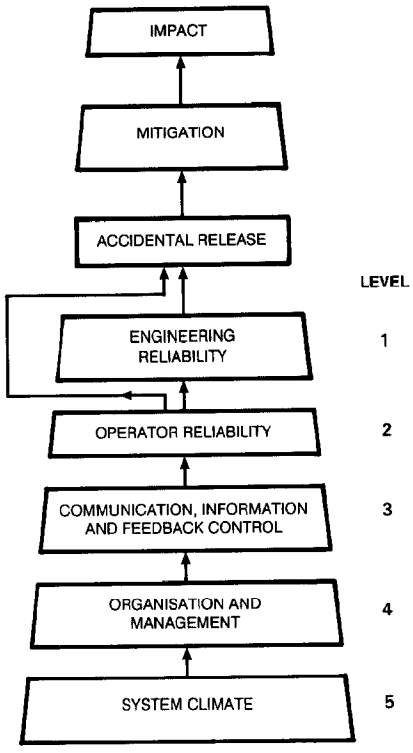

Fig. 5. A hierarchical scheme of accident causation. The figure is used to illustrate the potential effect of actions or inactions at different levels within the sociotechnical system on the safety of a plant.

liability. This level includes aspects of engineering design which might mitigate the duration of an accidental release e.g. shut-off valves and other safety systems.

Level 2 – Operator reliability. This encompasses all aspects of human factors which directly influence operator performance, including MMI, level of training and experience, procedure design, job design, workplace design etc., and other aspects of operator support.

Level 3 – Communication information and feedback control. This level concerns information dissemination through documentation, instructions, logs, reporting systems, etc. and the feedback mechanisms whereby it can be verified that the appropriate communication has taken place and been acted upon, e.g. permit-to-work procedures.

Level 4 – Organisation and management. This level refers to the organisational structure and management systems, e.g. for the management of safety. It includes factors such as the setting of standards, priorities and targets, maintaining and improving standards, decision making functions, and the estab-

lishment of organisational groups, processes and personnel roles to meet the functional requirements of the system.

Level 5 – System climate. At this level the organisation and its management overlaps and interfaces with other systems, e.g. regulatory systems, in that the system operates within a 'wider system' which includes economic pressures, public opinion, government regulations, current technical know-how, etc. The inclusion of this level is most important in comparing the way similar plants might perform in different economic circumstances and in different parts of the world.

This hierarchical concept demonstrates the levels through which it is theoretically possible to trace accident causes. At the top of the hierarchy can be seen the immediate causes of failure, either through engineering or operating failures. In the event of an accidental release action may be taken to mitigate the release parameters for example by the use of automatic shut-off valves while the impact of the release will be effected by such factors as the use of breathing apparatus and escape from toxic or thermal exposure.

In developing this hierarchical scheme we have drawn upon the similarities between other schemes [14, 17–21] and audit methods [22,23] which are used to analyse accidents or assess the state of major hazard plants. Appendix 3 shows how all the various schemes can be drawn together by the idea of the hierarchy.

The hierarchical scheme can also be applied to the matrix of underlying cause of failure and preventive mechanism. This can be done in the following way:

(1) For underlying causes of failure, problems in organisation and management (level 4), for example, may lead to design errors. Design errors could lead to operator reliability problems at level 2 or engineering problems at level 1. Alternatively failure to make operators aware of safety standards and safe practices (level 3) may cause unsafe working practices at level 2.

(2) For preventive mechanisms, problems such as pressure 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. Similarly pressures at level 4 or at level 5, may prevent a human factors review which prevents operator reliability problems at level 2 from being identified. In some cases identification of unsafe conditions at levels 1 or 2 may occur but due to problems at level 3 there may be a failure to communicate these conditions to the relevant personnel. This emphasis the importance of communication between the different levels of the hierarchy.

In this way, the underlying causes of failure or preventive mechanisms have their effect at levels 1 and 2 and are manifested as direct or immediate causes of failure. However, they arise because of problems at a deeper level.

We can see that although the immediate cause of an incident might (for

example) be classified as operator error, the operators would only be "carriers" of a problem which originated from levels 3, 4 and possibly 5. To quote Professor Reason [14]: "Rather than being the main instigators of an accident, operators tend to be the inheritors of 'pathogens' created by poor design, incorrect installation, faulty maintenance, inadequate procedures and management decisions, and the like. The operators' part is usually that of adding the final garnish to a lethal brew that has been long in the cooking. In short: unsafe acts in the 'frontline' stem in large measure from bad decisions made by the rear echelons". The data presented in this paper in fact shows that 4 areas of management control (preventive actions) have the potential to prevent 90% of the analysed accidents.

6. Generic failure rates

As explained in the introduction generic failure rates are used within RISKAT to quantify the risk from Major Hazard plant [1]. If nominally identical plants are managed, maintained and operated to significantly different standards but both are above the minimum required by the Health and Safety at Work Act then can systematic ways be found to reflect these differences? One approach may be to look at the influence that the factors identified here as important have on the generic failure rates used.

Generic failure rates must reflect the immediate causes which have given rise to the actual incidents. In other words it is the immediate cause such as corrosion which 'causes' the failure to occur. However the immediate cause is the symptom of the sociotechnical system failure which may be the underlying cause of failure or the failure of a potential preventive mechanism. Thus although the data presented here suggests that 41% of the immediate causes of pipework failure are human ones and 31% can be classified as operating error this is not a useful way to categorise the various contributions to a generic failure rate for the purposes of comparing different plants.

The results suggest that if improvements are made at a plant to, for example, maintenance procedures following a review of human-factors aspects then the incidence of failures would be expected to reduce. Operators would make fewer mistakes because the procedures would be better designed. This suggests that the more fundamental way of categorising failure rates for our purposes is in the two dimensional way described by the underlying cause of failure and preventive mechanism matrix which is used here to overlay each immediate cause. The data presented in Table 2 allows this statement to be expressed in a mathematical form:

$$x = x \sum_{ij} N_{ij} \tag{1}$$

with x the generic failure rate, where $\sum_{ij} N_{ij}=1$; N_{ij} are the individual entries in Table 2 normalised with respect to the total of the entries.

This analysis presupposes, of course, that the overall statistical distribution obtained for the pipework failure matrix represents the same data that generic failure rates for pipework are based on. In this respect the value of $\sum_{ij} N_{ij}=1$ is termed "average" for the purpose of assessment of a plant. A plant which we would call "average" should therefore show a breakdown of known underlying failure causes according to the matrix and have a "generic" failure rate for pipework failures.

If for a particular plant we would expect a 50% reduction in maintenance failures compared to average, this would reduce the maintenance contribution to pipework failures to 19.4%. In this instance $\sum_{ij} N_{ij}$ would equal 0.816, and the failure rate for pipe work for the plant would be 82% of the generic value.

7. Conclusion

This paper has proposed and developed two classification schemes which have been used to provide a detailed analysis of published incident accounts involving failures of fixed pipework on chemical and major hazard plant.

First a three dimensional scheme was developed which consists of a number of layers of immediate causes (e.g. operating errors). Each immediate cause was overlaid with a two-way matrix of underlying cause of failure (e.g. bad design) and preventive mechanism (e.g. task checking not carried out). Thus each incident is classified in three ways e.g. corrosion due to design error not recovered by routine inspection.

Operating error was the largest known immediate contributor to incidents (30.9% of all known causes). Overpressure (20.5%) and corrosion (15.6%) were the next largest categories of known immediate causes. The other major areas of human contribution to immediate causes were human initiated impact (5.6%) and incorrect installation of equipment (4.5%). The total human contribution to immediate causes was therefore about 41%.

For the underlying causes of failure, maintenance (38.7%) and design (26.7%) were the largest contributors. The largest potential preventive mechanisms were human factors review (29.5%), hazard study (25.4%) and checking and testing of completed tasks (24.4%). The hazard studies particularly of the design of the plant, human factors reviews of support for maintenance and operational activities and checking of completed tasks, particularly maintenance, are key activities in reducing pipework and in-line equipment failures. The data shows that it is potentially within the control of management to prevent 90% of the incidents analysed.

Secondly it is suggested that there exists a hierarchical scale of accident causation from the most immediate direct causes to increasingly remote causes. This does not imply a sequence of events in time but illustrates the potential effects of actions or inactions at various levels within the sociotechnical system on the safety of a plant. The levels of the hierarchy are 1 – engineering reliability, 2 – operator reliability, 3 – communication information and feedback control, 4 – organisation and management and 5 – system climate. The concept of a hierarchy of cause can be combined with the matrix of the underlying cause of a failure and a failure to recover from an unsafe condition. In this way the underlying cause of failure or a failure of a preventive mechanism have their effects at level 1 and 2 of the hierarchy and are manifested as direct causes of failure (operating error, corrosion etc.) but they arise because of problems at a deeper level i.e. the immediate causes of a failure are the carrier or symptom of underlying problems, such as bad procedures or bad design. These in turn may have resulted from deeper causes, e.g. inadequate resources.

The concepts developed above are also used to consider the nature of the generic failure rates which are used in the HSE Risk Assessment Tool RISKAT. It is used to calculate the risk from major hazard plant [1]. Generic failure rates are based on reports of accidents and incidents which have occurred in the past. No attempt is made to determine the cause of the incidents and so generic failure rates necessarily include a component for human error and failures of management control. Because of this, the risk figures calculated by RISKAT may be said to include an 'average' contribution from 'human factors', i.e. that amount which is implicitly included in the generic failure rates.

The work reported in this paper allows this 'average' contribution to the generic failure rates to be expressed in a mathematical form. Table 2, which summarises the information for all the pipework failures reported here may be normalised and the entries used, as in eqn. (1), to express a generic failure rate for pipework and in-line equipment failure as a sum of its component (two dimensional) parts. For an 'average' plant the generic failure rate will remain unaltered while for another plant the failure rate may be modified from the generic value by changes in the component parts.

The implications for any auditing scheme designed to modify risk values is that if appropriate questions are to be asked of a system, it is necessary to consider not only the types of failure causes as expressed in the three way classification but also how these arise and in what part of the system. In particular all questions should relate to the sociotechnical pyramid, i.e. be shown to have a causal relationship to failure at different levels in the sociotechnical system and questions should also tie in with the three-way classification of failure causes, particularly the matrix of underlying causes and preventive mechanisms. Future work will consider the form of the matrix for other important plant components, e.g. pressure vessels and the implication for audit question sets.

References

1 N.W. Hurst, C. Nussey, and R.P. Pape, Development and application of a risk assessment tool (RISKAT) in the Health and Safety Executive, Chem. Eng. Res. Des., 67 (1989) 362–372.

2 L.J. Bellamy, T.A.W.. Geyer and J.A. Astley, Evaluation of the Human Contribution to Pipework and In-Line Equipment Failure Frequences. Contract Research Report No. 89/15, Health and Safety Executive, Broad Lane, Sheffield S3 7HQ.

3 V. Bignell, G. Peters and C. Pym, Catastrophic Failures, Open University Press, 1977, pp. 37–65.

4 B.A. Turner, Man-Made Disasters, Wykehan Publications, London, 1978.

5 L.D. Phillips, P. Humphreys and D. Embrey, A Socio-technical Approach to Assessing Human Reliability, London School of Economics Decision Analysis Unit, Technical Report 83-4, London, July 1984.

6 L.J. Bellamy, Neglected individual, social and organisational factors in human reliability assessment, Reliability '83, Proc. 4th Natl. Reliability Conf., 6–8 July, Birmingham, Vol. 1, 1983, pp. 2B/5/1-2B/5/11.

7 L.J. Bellamy, A Literature Survey of the Effects of Individual, Social and Organisational Influence on Human Reliability. Part 1, Accident Survey, Ergonomics Development Unit, University of Aston in Birmingham, 1983, Report prepared for NCSR, UK Atomic Energy Authority, Culcheth, Warrington.

8 L.J. Bellamy, How people's behaviour shapes your plant operation, Process Eng., (1985).

9 C. Perrow, Normal Accidents - Living with High Risk Technologies, Basic Books, Inc., New York, NY, 1984.

10 L.J. Bellamy, Not waving but drowning: Problems of human communications in the design of safe systems, Ergonomics Problems in Process Operation, Institution of Chemical Engineers Symposium Series, 90 (1984) 167–177.

11 Human Factors in Industrial Safety, Health and Safety Executive HMSO, London, 1985.

12 K.W. Blything and S.T. Parry, Pipework Failures - A Review of Historical Incidents, Safety and Reliability Report SRD R 411, UK Atomic Authority, Bootle Mersegoide, January 1988.

13 E. Crooks, An Assessment of the MARCODE Databank, Health and Safety Executive Internal Report, Culcheth, Warrington, April 1986.

14 J. Reason, Human factors in nuclear power operations, pp. 238–242 in House of Lords Select Committee on Science and Technology (Subcommittee II), Research and Development in Nuclear Power, Vol. 2 - Evidence, House of Lords paper 14-II, HMSO, London, 1989.

15 D. Embrey and J. Reason, Human Factors Principles Relevant to the Modelling of Human Errors in Abnormal Conditions of Nuclear and Major Hazardous Installations, Report prepared for the European Atomic Energy Community, Vienna, under contract EC1 1164-B7221-84-UK.

16 Systematic Cause Analysis Technique, The International Loss Control Institute, 4546 Atlanta HWY, Loganville 9A30249, GA, 1989.

17 B. Bowonder and T. Miyake, Managing-Hazardous Facilities: lessons from the Bhopal accident, J. Hazardous Materials, 19 (1988) 237–269.

18 V. Bignell and J. Fortune, Understanding Systems Failures, Manchester University Press, Manchester, 1984.

19 F.E. Bird and G.L. Germain, Practical Loss Control Leadership, Institute Publ., Loganville, GA, 1988.

20 G.L. Wells and A.B. Reeves, A checklist for identifying the post causes of faults of errors on chemical plants. Int. Conf. Saf. Loss Prevention in the Chemical and Oil Processing Industries, 23–27 Oct. 1989, Singapore.

21 W.G. Johnson, MORT: The management oversight and risk tree, J. Saf. Res., 7 (1), (1975) 4–15.

22 The International Safety Rating System, Institute Publ., Loganville, GA, 1988.
23 The 'Manager' Technique, Technica, Lynton House 7/12 Tavistock Square, London WC1H 9LT.

Appendix 1

Classification of immediate causes of failure

This was a data-driven descriptive classification scheme. Using a sample of 400 incidents from the data collected, a descriptive scheme outlining direct (immediate) causes of pipework or in-line equipment failure was drawn up.

The aims of the scheme were that it should be:

- Accurate: conforming to current engineering knowledge.
- Unambiguous: categories are clear in meaning and non-overlapping.
- Comprehensive: will accommodate any pipework or in-line equipment failure.
- Hierarchical: will accommodate different levels of detail from incident descriptions. This minimises the loss of information which inevitably occurs when a unique event is classified in a category of events.
- Structured for making failure counts: events can be assigned to more than one category without double counting and events at different levels of the classification scheme will sum to the total of events in a higher category in the hierarchy.

The basic structure of the immediate cause scheme was developed through a number of iterations until a workable classification was achieved which fulfilled the aims described above. The scheme was added to and modified throughout the analysis of all the incidents. The basic structure consists of eleven categories of immediate cause, sub-categories for each of these and further sub-categories arranged in a 'tree' structure. An event could be inserted into the immediate cause scheme at any level of description, preferably the lowest level possible. If it had to be classified under two categories it was assigned a numerical value of 1/2 for each category (1/3 if inserted under 3 categories etc.). In this way, summing the number of events at each level and feeding that sum into the next level up would provide a value for the total number of events, in any category, at any level of description chosen for analysis. At the highest level, the total number of incidents analysed overall would be indicated.

The classification scheme has the following twelve categories:

(1) Corrosion

Corrosion was defined as the destructive attack of a metal, by chemical or electrochemical processes. This category referred to both internal, external and stress corrosion of a pipe and included zinc embrittlement, nitrate stress corrosion, and galvanic action.

(2) Erosion

Erosion was described as the destructive attack of a metal (or other material) by mechanical means i.e. bombardment by particles (e.g. sand) or from flowing fluids carrying small particles. This category also referred to both internal and external erosion.

(3) External loading

External loading was defined as mechanical stress induced in a pipe (or equipment) due to weight placed upon it, or the pipe having to support its own weight, e.g. due to failure of supports.

(4) Impact

Impact was defined as a collision (striking) between a pipe (or equipment) and some other object or person which causes sudden mechanical stresses leading to failure.

(5) Overpressure

Overpressure referred to a failure caused by the internal pressure in a pipe or equipment exceeding its mechanical strength. It included, for example, sudden pressure surges (water hammer), explosions inside pipework, inadequate pipe specifications for source pressures, and freezing of pipe contents.

(6) Vibration

Vibration was defined as an oscillating movement which leads to failure via fatigue of metal (or other material) or some part falling off or loosening but not actually failing, e.g. a nut gradually unscrewing.

(7) Temperature (high and low)

Temperature failures were those caused by stresses induced by excessive heat or cold, external or internal to the pipe, or by a hot–cold cycle in a pipe or equipment. It included extreme weather conditions, thermal shock and situations where inadequate allowance had been made for thermal expansion. It did *not* include freezing of contents leading to overpressure.

(8) Wrong in-line equipment or location

This category referred to situations where failure was caused by incorrect or inadequate installation of equipment (e.g. installing the wrong equipment, installing the right equipment incorrectly, installing the right equipment in the wrong place). It included cases such as bad welding and situations of insufficient equipment (e.g. no tail pipe on a valve, or inadequate valves to allow isolation).

(9) Operating error

This category included failures caused by direct human action where no pipe or equipment actually failed, (e.g. opening the wrong valve, or not isolating part of a system before working on it, leaving open ends on start-up, etc.).

(10) Defective pipe or equipment (cause of defect unknown)

This category was used to identify pipe or equipment items that were known to have failed, but when insufficient information was available to assign the failure to one of the other immediate causes.

(11) Unknown

The "unknown" category was used when a failure had occurred of an unknown component for which there was no known cause, i.e. insufficient information was available in the incident description.

(12) Other

This category was used for specific failures which could not be satisfactorily classified in any of the other categories. It was used to catch any omissions from the original 11 immediate causes (e.g. a clogged pipe leading to backflow) or to unusual events (e.g. pipe cut by weed trimmer).

Appendix 2

Classification of sociotechnical causes of failure

In the previous appendix, a classification system for immediate causes of failure was described. This appendix examines ways of classifying sociotechnical causes of failure and describes in more detail the scheme used in the current study. A detailed description of basic/underlying causes of failure and preventive mechanisms is given below.

Basic/underlying causes

(1) Natural causes

Any failure from 'natural' causes, such as failures due to lightning, flooding, subsidence, trees falling, soil conditions, wind, earthquake etc. (e.g. a crane falling onto a pipeline during a storm). It does not include those cases which are not 'natural' e.g., where subsidence was due to mining in neighbouring areas (this case would go under (7) Domino).

Where a design should reasonably be expected to withstand the environment it is included under (2) Design. This is particularly true for cases of freezing/frost. Extremes of temperature are therefore not included under natural causes: neither are dead birds or other forms of wildlife which may clog pipework.

(2) Design

This category includes errors in the design of plant, such as pipe specifications, in-line equipment specifications, layout, configuration, etc. This applies to the original design *and* to modifications.

The design category includes failures such as:

- incorrect specification of piping or equipment for the given conditions;
- omitting equipment in the design specification;
- locating equipment in the wrong place in the design specification;
- the design resulting in inappropriate process conditions (excessive temperature, pressure, etc.);
- design of layouts which facilitate failure.

This section does not apply to cases where the plant is not maintained within reasonable design assumptions.

(3) Manufacture/assembly

Cases which include defective or incorrect pipework or equipment specification could fall into this category where such cases are known to have been caused by the manufacturer, for example:

- flaws;
- not manufacturing to specification (e.g. bad materials);
- missing or defective component in assembly.

(4) Construction/installation

This category includes failure events arising out of construction/installation activities. These activities refer to the building or dismantling of plant, as opposed to maintenance or minor modifications to existing plant. It includes, for example:

- installation wrong equipment;
- installing equipment at the wrong location;
- impact during construction or demolition;
- removing or connecting equipment without knowledge of relevant personnel;
- installing equipment incorrectly.

(5) Operational activities during normal conditions

This category includes any pipe failure which arose out of operational actions during normal operating. Normal includes normal start-up and shutdown. It refers to errors arising in the day to day activities of those operating plant and monitoring process conditions, delivering chemicals, operating mobile equipment etc. Even if the event caused an unusual situation, as long as it occurred in normal day to day operations it still belongs in this category. It does not include maintenance, or installation activities or failures derived from design of plant.

The unsafe conditions which gave rise to the failure are likely to exist in the

design of the man–machine interface and of procedures for carrying out operations, in the training of personnel, and the design and use of organisational/communication systems (e.g. log books, instructions) for normal day to day operations. These unsafe conditions will often need to be inferred from the incident description.

It includes, for example:

- errors in following operating procedures or instructions;
- operating wrong equipment (valves, pumps, etc.);
- using wrong set points;
- impact during operations such as delivery tankers driving into pipework;
- inadvertent operation of controls;
- leaving pumps on/valves open;
- inappropriate design for human use (e.g. location of displays and controls, identification of equipment, procedure design, etc.).

(6) Maintenance activities

This category includes pipe failures which arose from maintenance activities. It also includes failures arising from either lack of or insufficient maintenance.

The unsafe conditions which gave rise to failure are likely to be broadly similar to those for operational activities i.e. the design of the man–machine interface and of maintenance procedures, the training of personnel and the design and use of organisational/communication systems (e.g. permit to work systems) for maintenance activities. These conditions will often need to be inferred from the incident descriptions where maintenance errors have occurred. For example:

- Working on the wrong pipe;
- Failing to lock off valves, pumps, etc. before maintenance;
- Errors in following maintenance procedures or written or verbal instructions, including permit to work systems;
- Failing to keep to maintenance schedules. Not maintaining equipment;
- Replacing equipment wrongly or using wrong equipment;
- Not adequately isolating for maintenance;
- Not using slip blinds, etc.;
- Impact during maintenance;
- Leaving equipment in the wrong status after maintenance;
- Removing or connecting equipment without knowledge of relevant personnel;
- Inadvertent operation of equipment;
- Inappropriate design for human use (e.g. location of displays and controls, identification of equipment, procedure design etc.).

It does not include design errors where, for example, isolation was not possible because the design did not include sufficient isolation valves.

(7) Domino

Any pipework or in-line equipment failure which results from an independent on-site failure (e.g. explosion, fire) or from off-site activities (e.g. car careers off road, mining causes subsidence). This also includes impact events which resulted from other failures such as the falling of higher situated plant equipment.

Domino does not include dropped loads from cranes, direct damage caused by vehicle working in the area or any sabotage events.

(8) Sabotage

Any deliberate attempt to cause a failure (e.g. bomb, starting a fire, deliberately opening valves, deliberately introducing contaminants, etc.), even if the subsequent cause of pipework failure is a domino effect.

(9) Unknown

Any failure event for which the underlying cause (origin of failure) cannot be deduced.

Detailed description of preventive mechanisms

This categorisation describes the primary recovery or preventive mechanisms which must have failed in order for a release to occur.

Some failures are not recoverable. These are also included as a sub-category of preventive mechanism.

(1) Not recoverable

When a potential failure situation first arises, if this results in a situation which is not reversible (i.e. conditions cannot be put back to a safe state before any release consequences), then the situation is not recoverable. For example, natural causes which result in an immediate release are not recoverable. Sudden events such as domino effects from explosions, or sudden unexpected reactions in the process will also be non recoverable.

(2) Appropriate hazard study of design or as-built not carried out/inadequate

Hazard and operability study (HAZOP) should recover design and, potential human errors where these could lead to the deviations considered in HAZOP. HAZOP only makes recommendations for follow-up. Some underlying causes of failure will only be recoverable at the as-built stage (e.g. certain layout aspects, wrong locations of equipment etc.). Appropriate hazard study and follow-up failure is therefore a broad category covering:

- Inadequacies or failures in conducting an appropriate hazard study of design or construction.
- Failure to follow-up recommendations of the HAZOP or other hazard study.

For example, incidents with the following characteristics would fall in this category:

- Failures caused by problems in design leading to external loading, overpressure, corrosion, impact, vibration etc., that would not be expected to be reasonably prevented by maintenance, and which could have been identified by hazard study of the design or as-built and rectified.
- Problems in safely operating a plant due to its design, which could have been identified by hazard study of the design or as-built and rectified.
- Operational errors which lead to problems (e.g. back flow, overpressure, etc.) which should have been picked up in an appropriate hazard study.

(3) Human factors review not carried out/inadequate

This category is similar to (2) but it specifically refers to cases of failure to recover those underlying causes of unsafe conditions which resulted in human errors within the man–machine system or in the following of procedures. The unrecovered errors will be information processing or action errors of the type:

- Failure to follow procedures (correctly) due to the following aspects not being recovered: poor design, poor organisation, lack of permit-to-work, inappropriate instructions, inadequate resources, inadequate or wrong communications, inadequate training or experience, lack of supervision, etc.
- Recognition failure given correct information due to lack of skills, training, lack of supervision, etc. not being recovered.
- Recognition failure given inadequate or incorrect information due to poor interface design or inadequate communication systems etc. not being recovered.
- Carrying out actions wrongly or on the wrong equipment due to man–machine interface inadequacies not being recovered.
- Accidental operation of equipment due to poor location or design of controls not being recovered.
- Inability or difficulty in carrying out actions due to poor location or design of displays or controls not being recovered (e.g. difficult to access or see).

Human factors reviews are not yet common industry practice. Nevertheless, all underlying causes of failure which could have been recovered by a human factors review should be included.

A human factors review should be expected to recover errors in the design of the man–machine interface/control room layout etc., design of procedures and job design, communication systems, organisation/planning of tasks, training and skills, and supervision inadequacies.

A human factors review would be carried out on the design and/or on the operating system. Methods would include task analysis, procedural walk-throughs, written procedure design evaluation, application of design guidance and checklists to assess MMI, and human reliability assessment, and human factors auditing techniques.

The review should evaluate the demands on, and capacities of, personnel and whether certain tasks can be reasonably organised into jobs without conflict in procedures or priorities.

The capacities of personnel will relate to their physical and information processing capacities within the context of the limiting conditions imposed by the ambient conditions of the system, such as the selection and training process, existence of stress inducing conditions, manning levels, supervision, and the provision of relevant required information, etc. (often referred to as 'performance shaping factors').

Any incident which simply states human error as a cause should also be included in this category. Ideally a human factors review should minimise all cases of human error.

(4) Task - driven recovery activities not carried out/inadequate: checking or testing

Carrying out checking/testing after tasks have been completed should identify errors such as installing equipment at the wrong location or failure to check that a system has been properly isolated and the pipe contents removed for maintenance, etc. For example, this often occurs in accident descriptions as "assumed pipe had been cleared of contents". Failure to identify and rectify such errors should be included here.

Sometimes there may appear to be overlap with other categories, e.g. should the operator have checked it was the right valve before he opened it or was it a human factors review failure? As a rule, this category applies only to checking completed activities, therefore the latter case would be classified as a human factor's review recovery failure.

(5) Routine recovery activities not carried out/inadequate: routine inspection and testing; process sampling; safety audits

These are all routine activities in the sense that they are part of a vigilance system on regular look-out for recoverable unsafe conditions in plant/process, e.g. process sampling identifies corrosion. It is similar to (4) except that it is not task driven. It also includes failure to follow-up, given identification of an unsafe condition. Evidence for events to be included in this category includes:

- equipment in a state of disrepair;
- inadequate inspection and testing;
- failure conditions which take a long time to develop but which are detectable.

(6) Unknown recovery

All failures for which there was an unknown preventive mechanism.

Appendix 3

Audit schemes and sociotechnical classifications

There are similarities between various post-accident analysis schemes, other sociotechnical classification schemes and plant audit methods. The purpose of this appendix is to draw together these similarities where possible.

In a paper analysing the Bhopal accident, Bowonder and Miyake [17] used the methodology developed by the United Nations–Asian and Pacific Centre for Transfer of Technology (APCTT). This methodology was used to classify any technology into the following areas:

- Technoware: hardware aspects of the plant (e.g. storage tanks, scrubbers, safety equipment, instruments and monitoring equipment, process control equipment, flare towers etc.).
- Humanware: human factors aspects (e.g. skills, stress, use of procedures and other person related aspects).
- Inforware: information, procedures, communication (e.g. emergency procedures documentation, toxicity data).
- Orgaware: organisational and management considerations (e.g. commitment to safety management, hazard assessment procedures).
- Climoware: climate of regulatory and technology absorption aspects (e.g. siting of facilities, expertise of safety inspectorate staff, dissemination of information relating to safe handling of hazardous facilities, public pressure, etc.).

Bowonder and Miyake gave many examples of errors which occurred under these different headings. The analysis described was a mixture of immediate causes and underlying causes of failures. For example, Technoware errors included design defects (an underlying cause of failure) and corrosion (a direct (immediate) cause). Humanware included tension and operator stress and inability to perceive the risk, while Climoware included weak factory safety inspection. The APCTT areas may be regarded as being on a similar hierarchical scale of accident causation from the most immediate Technoware causes (level 1) to increasingly remote causes.

Another approach is the systems failure method [18], which also analyses failures by consideration of all aspects of the sociotechnical system. The failures method includes the following important areas for consideration (the level indication from Fig. 5 is also shown):

- system failure (level 4, 5);
- communication (level 3);
- information (level 3);
- control (level 3);
- human factors (level 2);
- engineering (level 1).

This method is very flexible and can examine all types of system failures at a variety of levels of detail. It incorporates the concept of 'mismatch' between

the ideal system (the system paradigm) and the actual system. Another method which is being developed [20] is one which utilises a detailed checklist for post-accident analysis. The areas covered include:

- organisation (4);
- planning (4);
- resource availability (5);
- skills (2);
- information (3);
- communication (3);
- instructions/procedures (3);
- engineering (1);
- control (3);
- design problems (4).

Again the level indication from Fig. 5 is also shown.

Audit methods are not ways of describing accidents at chemical plants, but rather methods of assessing safety in the plant. As such they are not directly comparable with the methods above, but nevertheless contain many similar areas of investigation. The MANAGER system [23] developed by Technica has four main areas of investigation (system norms, pressures, resources and communication) which are subdivided into 26 areas each of which has a subset of questions. These areas are listed below with the level indication shown in parentheses:

System norms:

- Written procedural standards (4);
- Incidents and accidents (3, 4);
- Safety policy (4, 5);
- Training (4);
- Operations (4);
- Management of change of technology (4, 5).

Pressures:

- Training in understanding and skills (2, 3);
- Alarms (1, 2, 3);
- Operator workload/stress (2);
- Interaction between maintenance and other activities (3);
- General procedural support and acceptance (2, 3);
- Reporting incidents and follow-up (3);
- Reward and punishment (4).

Resources:

- Control room and plant (1, 2);
- Evacuation/emergency resources (3, 4);
- Personnel/manning (2);
- Maintaining standards (3);
- Shared resources (3);

- Fire prevention resources (1) – general housekeeping (2).

Communications:

- Team training (2, 3);
- Inspection/maintenance (3) – procedures (3);
- Shifts (3);
- Vertical communications in the organisational hierarchy (3);
- Logs (3).

For comparison, the 20 areas considered by the International Safety Rating System are given below:

1 – Leadership and administration (4);
2 – Management training (4);
3 – Planned inspections (4);
4 – Job/task analysis and procedures (2);
5 – Accident/incident investigation (3, 4);
6 – Job/task observation (2, 3);
7 – Emergency preparedness (3, 4);
8 – Organisational rules (4);
9 – Accident/incident analysis (3, 4);
10 – Employee training (2);
11 – Personal protective equipment (1);
12 – Health control and services (2, 3);
13 – Program evaluation system (4);
14 – Purchasing and engineering controls (3, 4);
15 – Personal communications (3);
16 – Group meetings (3, 4);
17 – General promotion (4);
18 – Hiring and placement (2);
19 – Record and reports (3);
20 – Off-the-job safety (2).

Item 7, emergency preparedness, relates to both mitigating of the release parameters and impact effects of the release and item 11, personal protection equipment, also related to impact effects of a release. See Fig. 5.

The International Safety Rating System has its origins in the work of Bird and Germain and is supported by The International Loss Control Institute (ILCI) Loss Causation Model [19] and the Systematic Cause Analysis Technique (SCAT) for post accident investigation [16].