DEVELOPMENT AND APPLICATION OF A STRUCTUREDAUDIT TECHNIQUE FOR THE ASSESSMENT OF SAFETY MANAGEMENT SYSTEMS. (STATAS) ©

N.W. HURST & K. RATCLIFFE
Health and Safety Executive

This paper describes a structured audit method (STATAS) which has been developed from research work sponsored by HSE and others. The audit aims to assess the quality of safety management at Major Hazard on-shore plants. The paper describes the empirical basis of the system, a management related loss causation model and the development and application of audit question sets derived from these inputs.

Key Words: Safety Management. Audit Risk Assessment

1. INTRODUCTION

HSE has, for a number of years, been concerned about the role of Human Factors, that is human error, ergonomic factors and the influence of management systems in major incidents and have published a number of booklets on these subjects (Ref. 1-5).

Original research work has been commissioned by the HSE from consultants Technica and Four Elements (Ref 6-12) to determine how Management and Organisational factors affect the potential for loss of containment of hazardous substances . HSE's Research and Laboratories Services Division (RLSD) have managed the projects and together with the Hazardous Installations National Interest Group of the Field Operations Division (FOD) have developed a structured audit technique from the research and have recently finished the first of a series of trial audits.

The system as developed for FOD is known as STATAS; (Structured Audit Technique for the Assessment of Safety Management Systems) and this paper will describe its empirical basis, a Management related Loss Causation Model and the development and application of audit question sets derived from them.

In the UK, premises storing or using quantities of hazardous substances sufficient to raise concerns about the potential for major accidents and the extent of any residual offsite risk are identified by the Notification of Installations Handling Hazardous Substances Regulations 1982 (NIHHS) and the Control of Industrial Major Accident Hazards Regulations 1984 (CIMAH). Major incidents or events that could escalate into major incidents occur when the hazardous substances involved escape their containment systems, whether these are storage tanks, process vessels or transfer systems including pipework and in-line equipment such as pumps and valves. The first task of the researchers was therefore to analyse and classify data

relating to vessel and pipework failures from a number of national and international data bases. A total of 921 pipework and in line equipment failures and 230 vessel failures were examined and an incident causation model developed.

2. A LOSS OF CONTAINMENT MODEL

2.1. Direct causes of loss of containment

At the initial analysis stage it could be seen that most incidents had an obvious or direct cause of failure. Examples include over pressurisation, corrosion or failure due to external impact. These direct causes arose either from a failure of hardware or were the result of human error. A pipe may corrode and leak or a fitter may simply break into a line without adequate isolations. The two, human and hardware failings, may well be linked. A mistake on the part of an operator could lead to over pressurisation in a system and conversely equipment or instrument failure, by demanding human intervention, can lead to an error which causes or compounds the release. Twelve categories of Direct Causes were identified and used to classify the incidents under study. These are as follows:-

Corrosion	Overpressure	Human Error
Erosion	Vibration	Defective Equipment
External loading	Temperature	Other
Impact	Wrong Equipment	Unknown

2.2 Origins of failure

Failure from these causes may occur as an immediate and direct consequence of an action or condition or may be latent within the system for some time before manifesting itself. There can exist a mismatch between the company's belief as to the state of the system and its actual condition. A valve for example, may have been installed to the wrong specification but may operate satisfactorily for some time before failing. The origins of the failure lies somewhere else in the lifecycle of the plant than the point at which it occurs. The original design may have been wrong, there may have been failures during manufacture or during the construction of the plant. The plant may have been incorrectly modified or an error may have been made during maintenance. Most of the incidents analysed could be classified in this way as having their origins in one of the major lifecycle phases of the plant, the exceptions being a few cases where the causes were due to external factors such as natural events, sabotage or the domino effects of failure of an adjacent piece of equipment or plant. Nine classifications for the origins of failure were identified and are listed below.

Design	Normal Operations	Manufacture/Assembly
Maintenance	Construction/Installation	Domino
Natural Causes	Sabotage	Unknown

2.3 Prevention and recovery mechanisms

It is better to prevent an unsafe condition in the first place than to try and recover it once it exists. However, both possibilities, prevention and recovery, exist and have important parts to play in a strategy to minimise failures. Preventative measures are most appropriate in the design of plant and plant modifications while recovery mechanisms are important in the field of routine inspection, testing and maintenance to cope with the normal ageing processes that occur on any plant. These mechanisms can be either in the field of hardware control or

equally in the modification of human behaviour. Taken together they represent an overview of available procedures that can minimise the overall risk of catastrophic failure. Not all failures may be recoverable however, and in some of the incidents studied the recovery mechanism remained unknown. Excluding the unrecoverable and the unknown four broad classes of Prevention/Recovery mechanisms were identified:

Hazard Identification and Assessment	Human Factors Review
Routine Checking and Testing	Task Checking

2.4. Incident classification scheme

Each of the pipework, equipment or vessel failures examined, after being classified as to the direct cause of failure and its origin in the lifecycle was further classified as to which of these four potential prevention or recovery mechanisms either failed or had the potential for identifying and preventing the failure occurring. Each incident could therefore be classified in three ways and the method is illustrated in Fig 1. Where more than one mechanism appeared to be involved expert judgement was used to determine contributions to the overall failure. Each incident can be located within the 3-dimensional matrix illustrated. For example, an overpressure failure due to wrong design and not prevented during the initial hazard and operability studies would be located in the cell defined by the 3 co-ordinates. As incidents are classified data accumulates within the cells and are open to analysis. Figs 2 and 3, for example, show the contribution of known direct causes to overall failure rates for pipework and vessels. The substantial contribution from operator error, overpressure, corrosion and temperature is illustrated. This in itself is useful information but is much more powerful when illustrated in relation to the origins of the failure and the potential preventative or recovery mechanisms. This reveals in a hierarchical way the areas of activity within each part of the plant's lifecycle which contributes most to failure and where the potential for recovery or prevention lies. This is illustrated in Figs 4 and 5 and represents collapsing the data as it accumulated in the 3-dimensional matrix into "tower blocks". Each tower block consists of the sum of direct causes. Looking at the data for vessels the diagram illustrates that 29% of the overall failure rate was due to faults of design that were not recovered or prevented during hazard identification studies. Similarly 24% of the failure rate had its origins in normal operations where human factors review could have detected and prevented the faults. Figures for pipework and vessels are different, illustrating the relative probability of different failure modes. Presentation of data in this form clearly illustrates where maximum benefit can be obtained from investing in sound management systems that are designed to implement the prevention and recovery mechanisms which are relevant to a particular part of the plant's lifecycle.

These mechanisms include engineering based prevention through hazard identification and hazard assessment and recovery through routine inspection checking and testing. Human factors prevention mechanisms include task analysis, competencies, communications etc. while recovery mechanisms include task checking and testing. In the next part of the paper I shall look at how the overall engineering and human reliability of these systems can be linked to a management model, and how this lends itself to the development of a structured audit scheme.

3. MANAGEMENT AND ORGANISATIONAL FACTORS: A SOCIO-TECHNICAL MODEL OF ACCIDENT CAUSATION.

This part of the paper will describe the factors which have an effect on the frequency of loss of containment incidents using a Management and Organisation Model, the Socio-Technical Pyramid, and link this to HSE's guidance, "Successful Health and Safety Management", HS(G)65. (Ref. 1).

3.1 The Socio-Technical Pyramid

This model (Fig 6) has been developed from case studies of major accidents including Three Mile Island and the Challenger Space Shuttle Disaster (Ref. 6) and a review of existing management models. Models have the advantage of rendering a complex organisation more easily understandable so that it can be looked at as a whole or examined in part in a simplified way yet retain the essential characteristics of the whole.

The Socio-Technical Pyramid represents, progressing from Level 1 to Level 5, increasingly remote factors that, nonetheless, have a casual link to the frequency of undesired events on site, specifically the loss of containment of hazardous substances. Fig 2 gives an indication of factors operating at the various levels.

Level 5 - The system climate

Factors exist which are generally outside the control of the company under review. These factors include the state of knowledge within the industry, the effects of historical incidents both on and off site and industry norms particularly in the field of hardware standards and maintenance procedures. The existence or absence of specific legislation and the activity of the regulatory body also have an influence as do official guidance and Approved Codes of Practice, on the standards adopted on site. There may be political and financial pressures operating as well as local public opinion. The scale of the hazard, the availability of relevant resources, the activities of the emergency services, the location of the plant are all factors which will influence the way in which site management commits itself to the desired outcome of the lowest practicable incident rates.

Level 4 - Organisation and management

This is the level within the management model where organisational and management structures are determined, policy decided and arrangements made. Of particular importance are:

a) Policy. Corporate goals should be set via policy documents. There should be clear leadership at the highest level on targets and priorities.

b) The Organisational Structure. This is the mechanics of how the company organises itself to achieve its desired goals. There may be discreet operational, maintenance, safety and training structures or these may be integrated in an infinite variety of ways.

c) Defined Responsibilities. Whatever the actual organisation it is important that roles and responsibilities are clearly defined and methods exist for those with health and

safety responsibilities to be held accountable. Mechanisms for control, eg review and revision of objectives should be specified, and individual scope for decision making defined.

d) Site Standards. The arrangements made for the selection and setting of appropriate site standards and the mechanism for maintaining and improving these. Standards should take due note of Regulatory requirements, industry norms and relevant nationaland international standards. They should also be routinely reviewed and revised.

e) Resources. The allocation of resources, setting of budgets and deadlines and ground rules for control of contractors and use of specialist equipment.

f) Information. Good data management assist all these activities. It is important to have a policy on the use of data from monitoring, auditing and inspections to close the management control loop and develop a climate of continuous improvement.

g) Reward and Punishments Systems. These systems should form a constructive part of the whole system, aiming for a no-blame culture.

This level (Level 4) defines the "Mission". This is achieved by the implementation of good management practice through planning, control, leadership and organisation. Activity at this level will change and evolve through influence from lower levels as well as in response to changes in system climate.

Level 3 - Communication and Feedback

At this level management processes are in operation. It is here that systems must demonstrate the elements of control, communication, co-ordination and co-operation and the essential monitoring, programme review and development necessary to the management control loop. Issues include:

a) Formal and informal communications. Written communication includes the development and dissemination of instructions, use of log books and handover documentation, and the development and review of standard operating procedures. Verbal communications include formal meetings, eg safety committee meetings and informal meetings at all levels whereby the company's policy is spread and reinforced.

b) Documentation. There should be a policy covering the generation, dissemination and updating of documents. These include records of inspection, incident investigation reports, standard operating procedures, P and I diagrams, hazard and operability studies, permit to work systems, design of documents, eg accident report forms and the availability of standards and data sheets.

c) Man machine interface systems (MMI). Control room operability can be effected by the design of data presentation on visual displays and instruments.

d) Communications hardware. The reliability of hardware systems ensuring communication particularly during emergencies.

e) The activities of supervisors in the role of task checking and inspection.

f) Monitoring, feedback and programme evaluation and review. The role of auditing. Auditing is a necessary part of the system whereby a 'third party' can give an independent and structured report on the health of the controlling Safety Management Systems.

g) Data presentation and acquisition and the use of performance measures. Traditional measures can be too coarse - loss time accident data alone rarely gives sufficient insight into the underlying causes of incidents or illuminates early trends. Appropriate performance measures need to be identified concentrating on acquisition and use of near-miss information and other measures that can be built-in to system such as progress with Safety Committee items, response time to deviation reports etc.

Level 2 - Operator reliability

At this level the overall safety of the system depends upon the reliability and competence of the operator. This is in turn effected by activity at Level 3 through Performance Shaping Factors. These include:

a) The demands and design of tasks.

b) Operator selection and, through training and acquired experience, levels of skills, knowledge and overall competency.

c) Man machine interfaces. Stresses and pressures, peer group influence, influences of the environment.

Level 1 - Engineering reliability

At this level the integrity of system relies upon the overall control of plant design and site modification. Issues include:

a) Use of failure rates and failure analysis.

b) Instrumentation and controls. Hardware design and maintenance.

c) Programmable electronic systems, potential failure modes and ergonomic weaknesses.

A hardware failure can not only be a manifestation of a failure within the controlling management system but could be as a direct result of human failure. Operator error could result in part of the system being subject to conditions outside its operating criteria, eg overpressure. Conversely a hardware failure requiring human intervention gives rise to the possibility of the operator making a wrong decision. This may be particularly so if

emergency action is needed with the operator required to follow infrequently used procedures under pressure.

Level 0 - Loss of containment and mitigation

The actual impact of an event can be effectively mitigated by action taken once the alarm is raised. Mitigation covers all the activities that should be contained in a good on-site emergency plan. Issues include:

a) Bunding arrangements and post release action, eg foaming.

b) Control of ignition sources.

c) Arrangements for fire fighting from onsite resources and attendance by Fire Authority.

d) Use of water sprays, scrubbing systems and venting systems. These systems are normally included in initial design considerations and appropriate standards.

e) On and offsite emergency planning including arrangements for escape, site evacuation, temporary refuges, use of PPE during evacuation.

f) Effectiveness of emergency shut down systems, automatic shut off valves, remotely operated shut off valves or manual isolation valves. Time taken to control a release is typically quoted as one minute for an ASOV, 5 minutes for a ROSOV and 20 minutes for manual intervention. (Bellamy and Geyer 1990 TECHNICA). Mitigation of impact is also influenced by plant layout, design and accessibility of controls, initial hazard assessment and awareness, eg appreciation of the likely consequences of a release and its development with time, gas detection systems and containment systems including secondary containment.

4 MANAGEMENT CONTROL

The Socio-Technical Pyramid as a model of a management structure is consistent with the management model and control mechanisms illustrated in the HSE's Accident Prevention Advisory Unit's guidance "Successful Health and Safety Management" HS(G)65. (Ref 1) since the Socio-Technical Pyramid is derived from analysis of loss of containment scenarios and explores increasingly remote systems failure through Level 1 and 2 (hardware and operator reliability) to Level 5 (system climate) it is inverted in relation to the APAU model (Fig 8) which starts with management level commitment to a policy for health and safety. The Socio-Technical Pyramid is a loss causation model with casual links between each level. The APAU model is a diagrammatic representation of the key elements of a successful health and safety management system incorporating the essential feedback loops through monitoring and auditing to ensure the continued improvement and development of the system.

The complimentary nature of the models can be illustrated by considering a systems analysis for training needs as shown in (Fig 9). Information about operator reliability from routine assessment or evaluation of errors is fed back to assess the content and delivery of the

training scheme. If the scheme is found wanting the standards and resource allocation are revised and through external communication routes the company's experience may be fed back into a revision of an industry standard.

The Key Elements illustrated in Fig 8 are the essential components of a successful health and safety policy and the extent to which they are present in the system is a measure of a firms progress towards a self- improving health and safety culture. The Key Elements are summarised below.

a) Policy.
The lead for setting a policy which recognises the hazards associated with a firm's activity and lays down an overall strategy for evaluation, elimination and control must come from the top of the management structure. To be successful the policy should:

i. Be comprehensive.

ii. Recognise the letter and the spirit of legal requirements.

iii. Recognise the contribution that a commitment to high standards of health and safety makes to the overall performance of the company.

iv. Demonstrate real commitment and involvement from the highest levels of management.

v. Demonstrates the will and ability to develop the necessary structures, systems and safety culture.

vi. Commit the necessary resources to achieving identifiable goals.

vii. Be systematic in the identification of hazards, the assessment of risk and the application of control measures.

viii. Recognise the essential value of measuring output from systems as a necessary step in reviewing and developing standards.

ix. Recognise the value of regular independent auditing of systems.

b) Organising.
Organising for successful health and safety management requires building upon the essential areas of developing controls, co-operation between functions, communication between individuals and groups and promoting high levels of competence for all individuals within these functions. Elements of control include:

i. Defining responsibilities allocated to managers in different functions.

ii. Comprehensive job descriptions for line managers and defining the role of safety adviser.

iii. Enabling individuals with authority, competence, time and resources to carry out duties effectively.

iv. Developing systems with accountability and motivation through target setting.

v. Providing adequate supervision, instruction and guidance.

Co-operation is developed by:

i. Good communications between functions.

ii. Involving employees and safety representatives in developing and monitoring performance indicators.

iii. Participative systems for recognising achievements.

Good communications are developed by:

i. The visible involvement of management in control activities.

ii. Provision of clear, comprehensive supporting documentation.

iii. An efficient system of formal and informal meetings.

Competence is assured by:

i. A sound policy on recruitment and selection and promotion to key jobs.

ii. Standards of training with monitoring of the effectiveness of the results.

iii. The availability of specialist advice to decision makers.

c) Planning and Implementing
A successful safety management system must be seen to be drawing up short and long term plans, setting relevant performance standards aimed at eliminating and controlling risks and to be putting those plans in to practice. These objectives are achieved by:

i. Identifying objectives and setting targets to be achieved within specified time limits.

ii. Setting appropriate standards to achieve, maintain and improve a positive health and safety culture.

iii. Using hazard identification and risk assessment as a basis for the control of risk.

iv. Having as a prime aim the elimination of risk where possible and otherwise the minimisation and control of risk through engineering reliability and operator competence.

v. Establishing priorities.

vi. Establishing a system for the development, dissemination and review of documentation.

d) Measuring Performance.
Measurement is an essential part of the managerial control loop. Some systems have simple performance indicators, eg lost time injury rates, other require judgements as to their success or a combination of both. For example, the effectiveness of a training programme can be judged both through scores in tests and by an evaluation of operator competency via line management. Measuring systems should include:

i. Active monitoring systems as routine comparing planned attainment of objectives and standards within time limits against actual performance.

ii. Reactive systems for collection and analysis of data relating to failures in the system and its use to remedy underlying causes. These include causes of injuries and ill health, dangerous occurrences and near misses.

iii. The evaluation of information at the appropriate management levels.

e) Reviewing and Auditing.
Information relating to the success or failure of safety management systems must be collected routinely and used to develop and improve the system. These systems should:

i. Test the health of the whole system.

ii. Identify remedial action where the system is deficient or no standards have been set.

iii. Measure the degree of compliance of the systems against stated policy.

iv. Allow for third party audit for unbiased judgement and to enable comparisons to be made.

5. CONSTRUCTING AN AUDIT SCHEME

The earlier parts of this paper have described the development of an incident model which classifies releases of dangerous substances in terms of a direct cause, an origin of failure (within the plant's life cycle) and a potential prevention or recovery mechanism. The system failures underlying a release were related to a management loss causation model, the Socio- Technical Pyramid as well as good management practice as outlined in the HSE Guidance Booklet HS(G)65 "Successful Health and Safety Management". In this part I will show how these models can be combined to form the structure of an audit scheme and how STATAS, a scheme developed for possible use by HSE's Field Operations Division evolved.

5.1 Major contributions to failures

The purpose of an audit is to provide an independent assessment of management's planning, organisation and control systems. It should support all other activities on site by providing information about the relevance of standards and the extent to which plans and systems are properly implemented and effective. Any audit scheme needs to be comprehensive in its examination of the relevant safety management systems and the extent to which the key elements of the management control loop are in place.

The empirical basis for STATAS starts with the research work described earlier which analysed and classified pipework and vessel failures. In particular with the quantitative data, the "tower blocks" (Figs 4 and 5) which represents the sum of all direct causes located at their origin in one of five identified phases of the plant's life cycle and according to what potential prevention or recovery mechanism either failed or was available to identify and correct the error. The 5 phases of the plant's life cycle were identified as:

a) Design; (Des), including the choice of design, and the design process. This also covers modifications.

b) Manufacture; (Manf), including off-site manufacture of components and pre-construction assembly.

c) Construction; (Con), including installation and commissioning.

d) Operation; (Op), covers all normal process operations including start-up, shut downs and emergencies.

e) Maintenance; (Maint), includes all planned inspection and testing as well as routine replacement and emergency maintenance..

The 4 prevention/recovery mechanisms are divided between assessment of hardware or human behaviour and whether the activity is designed to prevent faults and errors or detect any that occur. The categories therefore are, for hardware:

1. Hazard identification and assessment techniques (HAZ)

2. Routine inspection, testing and sampling (ROUT)

Similarly for human activities:

3. Human factors review (HF),

4. Task checking (TCHECK).

Different forms of these activities are relevant at different parts of the plant's life cycle. The information represented graphically in Fig 4 and 5 is shown numerically in Table 1.

TABLE 1

ORIGINS OF FAILURE/PREVENTATIVE MECHANISMS COMBINATIONS CONTRIBUTIONS TOWARDS OVERALL FAILURE RATES

Combination	Contribution		Cumulative Totals		
	Pipework	Vessels	Pipework	Vessels	
DES/HAZ	25	29	25	29	
Maint/HF	15	6	40	35	
Maint/TCHECK	13	4	53	39	
Maint/ROUT	10	11	63	50	
Op/HF	11	24	74	74	
Con/TCHECK	8	2	82	76	
OP/HAZ	-	5	82	82	
OP/TCHECK	2	2	84	83	
==========	========	======	=======	======	**CUT OFF**
DES/HF	2	-	86	83	
Manf/TCHECK	2	-	88	83	
Maint/HAZ	-	2	88	85	
Con/HF	2	-	90	85	
etc (all other known)	2	2	92	87	
Unknown/Not revcoverable	8	13	100	100	

All contributions> 1%, figures rounded to nearest whole number.

NB.
Some of the smaller contributors may be included in the audit's other categories. eg. Maint/HAZ may be included in other maintenance areas by the addition of a few extra questions.

Although much of this paper has been about theoretical models it must be remembered that the exercise starts with real incidents and the prevention/recovery mechanisms refer to real activities on sites. For example when designing plant or plant modifications all firms, to a greater or lesser extent, will use a variety of hazard identification and assessment techniques. Precisely what may be done depends upon many factors but would include Preliminary Hazardous Assessment, Hazard and Operability Studies, Event and Fault Tree Analysis, Check Lists etc. Similarly for other activities at other parts of the life cycle. It is these activities that are examined by the audit and the percentage contribution towards overall failure rates suggests a hierarchical approach.

5.2 Structure of the STATAS audit

There are 20 possible combinations of origins of failure (5) and prevention/recovery mechanisms (4). It can be seen from Table 1 that some of the combinations contribute little to the overall failure rates. For STATAS it was decided to concentrate on the 8 areas of activity above the cut-off point. These 8 areas cover 84% of the total contribution towards pipework failures and 83% towards vessel failures. This is compared with the maximum recovery potential of 92% for pipework and 87% for vessels, the balance of the contribution comes from combinations that were not recoverable or unknown. The audit therefore consists of 8 question sets, one covering the use of hazard identification techniques in the design and modification of plant, one covering task checking during and after construction work, 3 linked to maintenance activities and covering human factors, routine inspection and testing and task checking, and 3 linked to normal operations covering human factors, hazard identification and task checking.

Each identifiable activity which has a direct causal link to a human or hardware failure constitutes in whole, or in part, a safety management system. The audit probes the systems at each relevant level of the Socio-Technical Pyramid, tailoring questions to establish operator competency at Level 2, the effectiveness of a company's communication control and feedback mechanisms at Level 3 and establishing details of the management organisation at Level 4. Level 5, the systems climate, has been left out of the formal audit structure as these are matters which are outside the direct control of site management. It is, however, important to understand the environment within which the company operates and STATAS uses guidelines to assist the auditor in assessing the system climate. This may be particularly useful where it becomes apparent at a multi-site manufacturer that site practices and powers of decision making are controlled or restricted by corporate policies. In this case it is necessary to influence the highest decision maker, by direct approach at corporate level.

Job Relates Themes

At each level of management, questions are grouped into 4 job related themes. These are:

Theme A - Structures, systems and procedures.

Theme B - Standards and criteria.

Theme C - Mitigation of pressures.

Theme D - Availability and use of resources.

A fuller description of these themes is given below but it can be seen that the principles now described totally define the structure of the question set and the role and purpose of individual questions. The structure is illustrated at Fig 10 with the questions themselves designed to show the extent to which the management system under review can demonstrate the existence of the key elements of successful health and safety management, particularly the management control loops. Indeed there should be many embedded control loops at each level of the system as well as a major one covering the systems main output, eg training. The smallest sub set of questions is a "cell" which may consist of between 2 and 10 questions, exploring one of the themes at a particular level within the management structure relating to one area of activity. At the moment the questions are a mixture of the general and the specific. General questions are designed to let the company demonstrate its range of activities in a particular area and specific questions are on those systems which would seem to be essential at any site, for example permit to work procedures. The questions are not designed to be followed slavishly. Once the auditor has established the extent of the activity and the quality of its controlling management system by "key elements" questions then he/she can move on. Neither is it necessary to use all of the audit at once. The question sets can be used in any combination, for example concentrating on maintenance activities or using 2 of the sets to look at human factors across maintenance and normal operations. This flexibility enables the auditor to judge and tailor the input of resource to individual companies.

The themes in more detail, are as follows.

Theme A - Structures, systems and procedures. These are the arrangements that are in place to ensure that the system operates correctly. This includes the way rules and responsibilities are specified and how people are held accountable, the development of procedures and means of communication between individuals and groups.

Theme B - Standards and criteria. These are the means that ensure that proper use is made and notice taken of statutory requirements, approved codes of practice, guidance from the regulatory authority, industry standards and American, British or other International standards. It also includes the way in which these are incorporated into site standards and how any deviations from accepted norms are justified. Arrangements should also be made for monitoring and reviewing the performance of these standards with the objective of routine revision and improvement.

Theme C - Mitigation of pressures. These questions explore the extent to which economic, operational and other pressures may interfere with the achievement of policy objectives. Pressures may arise from schedules of work, customer demand etc. and arrangements should exist for recognising the potential for pressure and ensuring that safety considerations are given proper regard.

Theme D - Resources. Questions seek to show that proper resources have been allocated to various functions, including properly competent personnel, information and equipment.

Each question set consists of between 40 and 80 questions and is fronted by a summary sheet (Fig 11) showing the percentage contribution to overall failure rate to this particular activity and
summarising the key issues. This provides a "map" for the auditor to establish his/her position in the audit structure.

5.3 The assessment process

The way in which the audit is conducted is based upon current best practice. The extent of the audit is determined from operational needs and an assessment of information already held about the firm. In the UK sites subject to the top tier requirements of the Control of Industrial Major Accident Hazards Regulations must submit Written Reports which include descriptions of their management arrangements. This report may point to activities which would be appropriate for an audit approach. The firm is contacted at highest site level with a preliminary visit to explain the methodology and agree on personnel to be interviewed. Such a visit is also useful to establish the system climate (Level 5).

The audit does not attempt to interview everyone on site but aims to sample "horizontal" and "vertical" slices. A degree of redundancy is built into these slices so that perceptions are obtained from more than one person and, to support information obtained from interview relevant documentation is examined and formal inspection carried out of procedures. The horizontal slice includes managers with influence and duties at Levels 4 and 3 and therefore with involvement in the process of policy and standard setting. The vertical slice looks at those involved with the delivery of engineering reliability and operator competence as appropriate including of course, operators, fitters and technicians. The 3 "legs" of the audit are mutually supporting. Information from formal interviews directs the auditor to particular documentation and claims made about systems are tested at operator and maintenance fitter level. The audit is conducted in a series of visits as close together as possible with 2 auditors assisting and supporting each other. In practice it is found that interviews last for about one hour for less formal 'system climate' discussions; about 1- 1 1/2 half hours for senior managers; about 45 minutes - 1 hour for middle management and about 30 minutes for operators, not including on site discussions. The auditors take turns asking questions and taking notes. Longer interviews start to become unproductive both from the point of view of the auditor and interviewee.

After all the evidence is assembled together with supporting documentation and the experience of inspection the auditors seek to make judgements about site performance in each theme of the activity. Ratings are made on a 5 point scale with "average" as the centre point. In areas of activity where clear standards exist then judgement can be made directly against these standards. In many areas, however, there are no such standards and judgement is made against the evidence of management activity. For example, at an average site it would be expected that there would be some management activity in most areas although procedures would not be formalised and there would be little feedback through monitoring. A site marked well below would have no measurable control activities and indeed, hazardous conditions would be likely to exist. For an assessment of "well above average" it should be seen that programmes exist with properly chosen standards, that management control principles are understood and applied and control loops built into the systems are working and generating system improvements.

The choice of "anchor points" is an important one to any audit scheme. In the development of STATAS and parallel work this is an area where further research is continuing and more robust points are being produced. Once these judgements have been made the results are assembled and can be presented to the company for an Improvement Plan to be agreed. In the UK it is seen as important that firms safety representatives and union officials are included in these procedures. It is almost axiomatic that a company well on the path of good management and safety performance would have a high degree of involvement from the workforce.

The report is a comprehensive one giving a background to the structure of the audit and commenting on good aspects of the firm's system, commenting on areas where management control is not apparent and making recommendations, some on relatively straight forward matters of fact but mostly highlighting those systems where comprehensive managerial control had not been demonstrated in relation to policy making, definition of roles and responsibilities, target setting, standards selection, training, monitoring, review and revision of procedures and auditing.

Priorities can be assigned to recommendations by considering the overall contribution of that activity to failure rates. Experience has shown that this is not quite as straight forward as it seems and auditor judgement is usually mixed with company pragmatism to prioritise the recommendations. It must be recognised that in many cases, the changes recommended cannot be achieved in the short term. Fundamental systems may have to be redesigned and the programme may extend to two or three years. The most important thing is the commitment to bring about improvements and establish a culture of continuous improvement by the involvement of all concerned.

6 CONCLUSIONS AND FURTHER WORK

The development team have now concluded a number of audits using STATAS developing and refining the system as a consequence. Although the Field Operations Division of the Health and Safety Executive is not committed to adopting any such system at this time it is very actively looking at the role of audits and how a system such as STATAS could be used to augment more traditional inspection techniques. The main qualities of STATAS are its sound theoretical and empirical basis and the fusion of management and loss causation models to produce a series of judgement based question sets that, taken together with reviews of documents and traditional inspection, produce a robust assessment of site activities designed to control risks of major accidents, and a framework for improvements.

The audit technique is still being developed as part of a major European research programme being funded by HSE, the Dutch Ministry of housing and environment (VROM), the CEC, and industry. The methods developed so far are proving to be of great interest both as research tools and as having practical value for both industry and regulatory agencies. Current and future research work is aimed at strengthening and further developing the technique. This involves among other aims:

- Improving the useability of the audit system.

- Exploring methods of allowing the auditors judgements to be included in risk assessment.

- Providing anchor points or "standards" against which the performance of areas within the audit can be judged.

- Application of the technique in different European countries.

- Collection of data to 'verify' the Audit System.

Acknowledgement
The authors are pleased to acknowledge the support of HSE, VROM and The CEC in funding this work and the valuable contributions made by others to the development and application of the technique.

REFERENCES

1. HS(G)65 "Successful Health and Safety Management"
HSE: Accident Prevention Advisory Unit, HMSO ISBN 0 11 885988 9

2. HS(G)48 "Human Factors in Industrial Safety"
HSE, HMSO ISBN 0 11 885486 0

3. "Guidance on Permit to Work Systems in the Petroleum Industry"
OIAC, HMSO ISBN 0 11 885688 X

4. "Guidance on Multi-Skilling in the Petroleum Industry"
OIAC, HMSO ISBN 0 11 886319 3

5. "Dangerous Maintenance: A Study of Maintenance Accidents in the Chemical Industry and how to prevent them"
HSE, HMSO ISBN 0 11 883957 8

6. L J Bellamy, T A W Geyer and J A Astley
Evaluation of the Human Contribution to Pipework and In-Line Equipment Failure Frequencies. Contract Research Report No 89/15. HSE. ISBN 0717603245

7. N W Hurst, L J Bellamy, T A W Geyer and J A Astley.
A Classification Scheme for Pipework Failures to Include Human and Sociotechnical Errors and their Contribution to Pipework Failure Frequencies. J Haz Mat 26 (1991) 159-186

8. L J Bellamy, T A W Geyer, M S Wright and N W Hurst.
The Development in the UK of Techniques to Take Account of Management, Organisational and Human Factors in the Modification of Risk Estimates. AiChemE. Spring National Meeting, Orlando 1990

9. T A W Geyer and L J Bellamy.
Pipework Failure, Failure Cases and the Management Factor. I Mech Eng 1991

10. N W Hurst, L J Bellamy and T A W Geyer.
Organisational, Management and Human Factors in Quantified Risk Assessment. A Theoretical and Empirical Basis for Modification of Risk Estimates. Safety and Reliability in the 90's (SARRS '90). Ed Water and Cox. Elsevier Applied Science

11. L J Bellamy and T A W Geyer (ed J C Williams).
Organisational, Management and Human Factors in Quantified Risk Assessment. HSE Contract Research Report 33/1991

12. P I Harrison and J C Williams.
Organisational Management and Human Factors in Qualified Risk Assessment. HSE Contract Research Report 34/1991

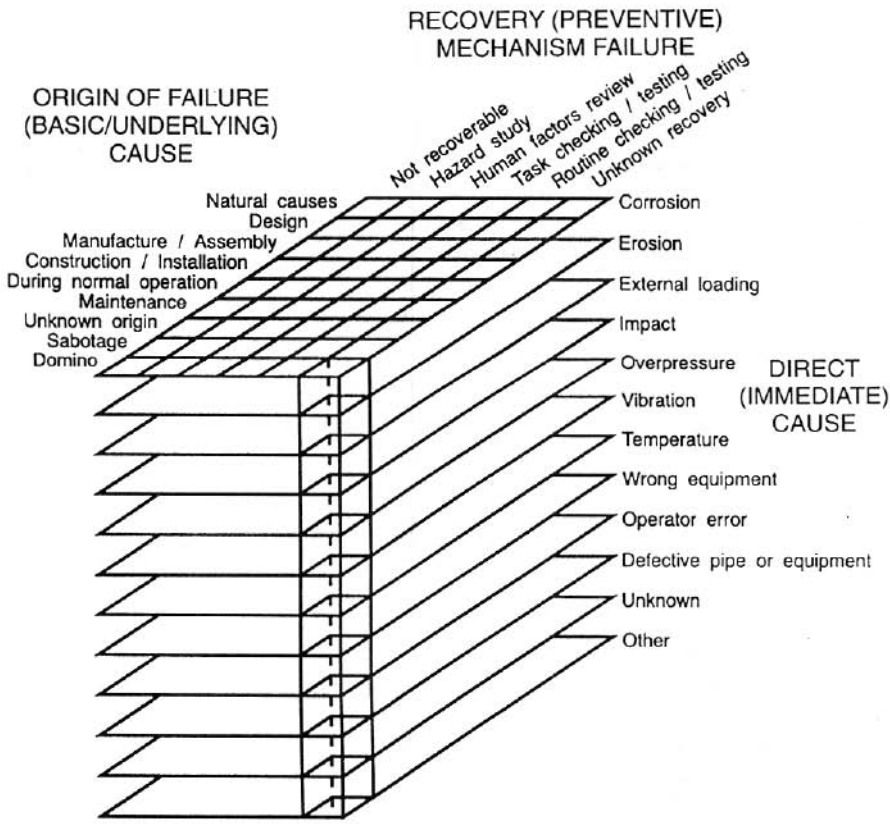

Fig.1 - A 3-Dimensional classification system

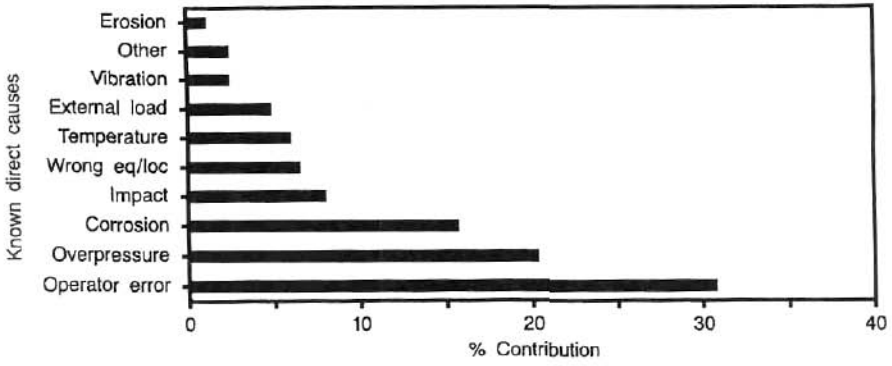

Fig.2 - Pipework and in-line equipment

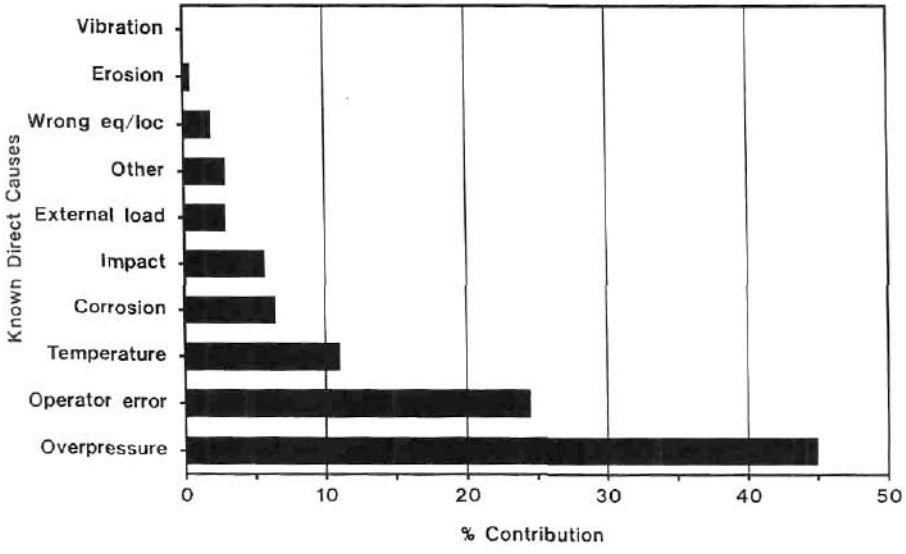

Fig.3 - Vessels percentage contribution of known direct causes

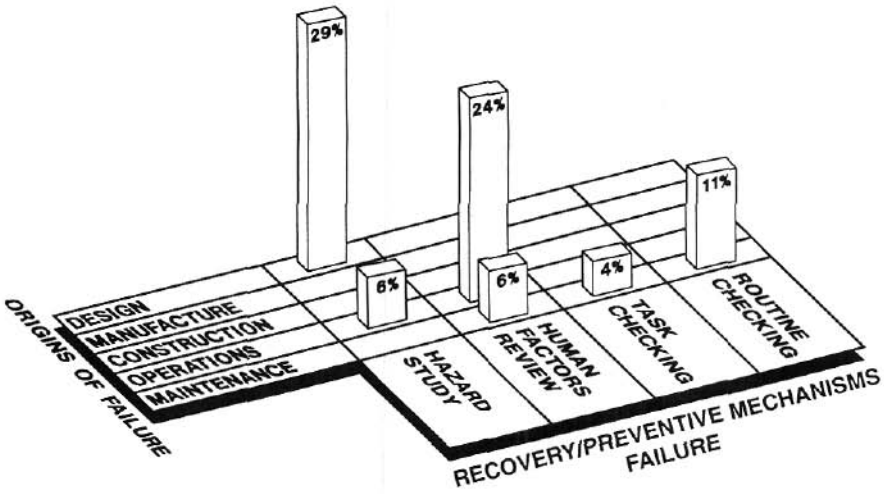

Fig.4 - Classification of vessel failures by origin of failure and prevention / recovery mechanism

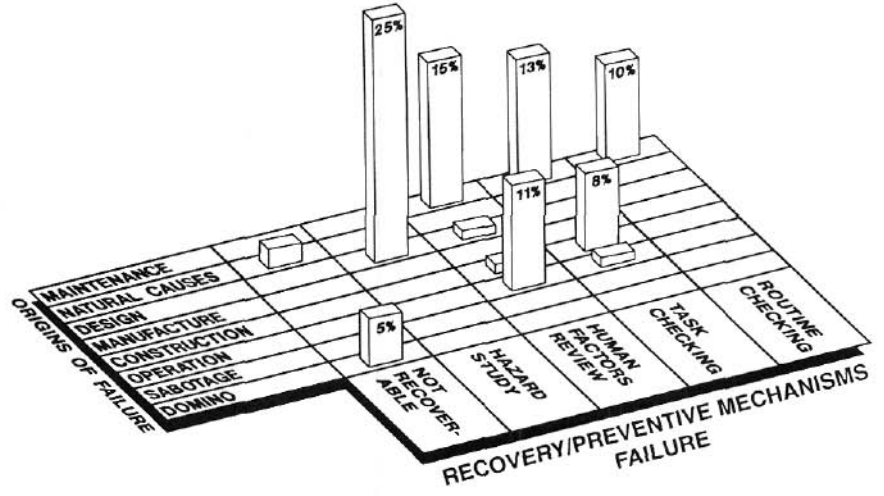

Fig.5 - Classification of pipework failures by origin of failure and prevention / recovery mechanism

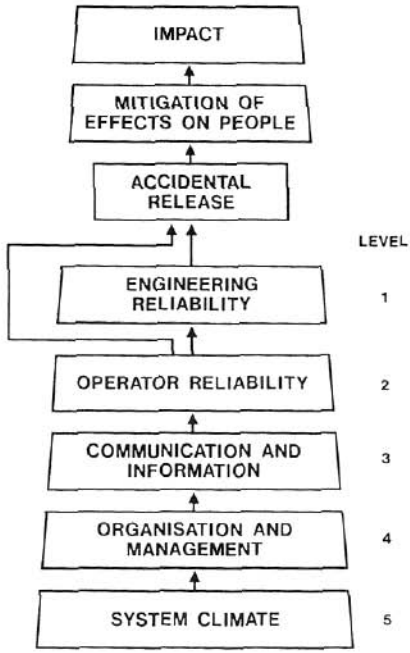

Fig.6 - The socio-technical pyramid

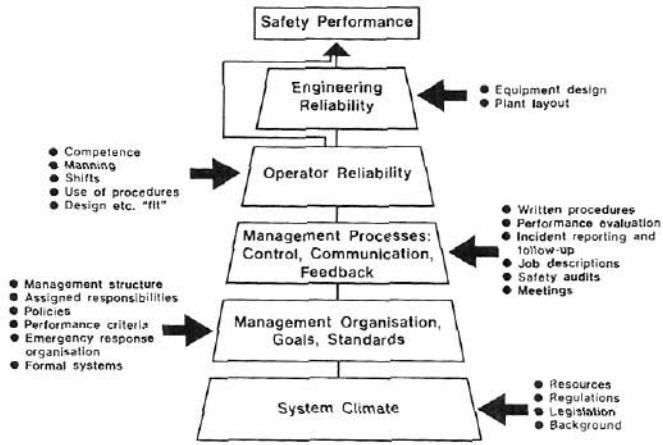

Fig.7 - The socio-technical pyramid factors affecting performance

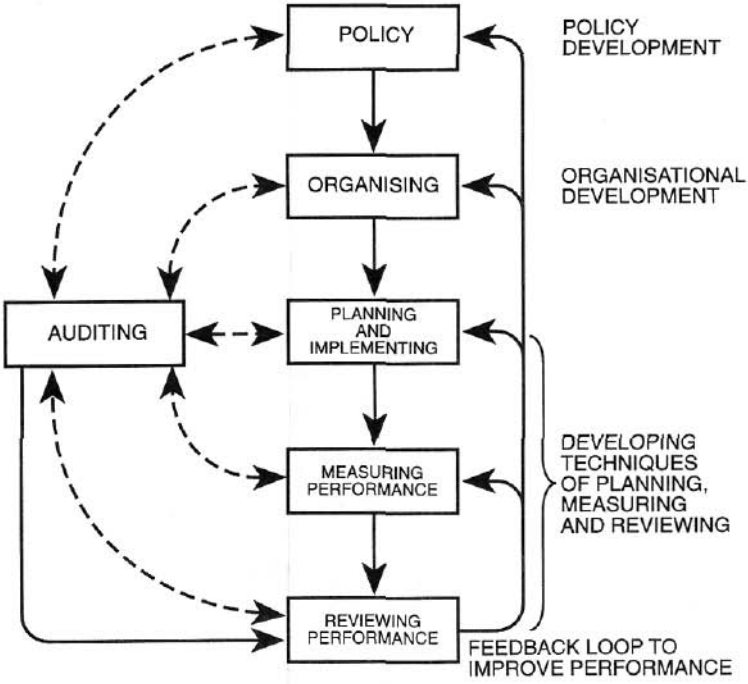

Fig.8 - Key elements of successful health and safety management
Source: Health and Safety Series booklet HS(G)65

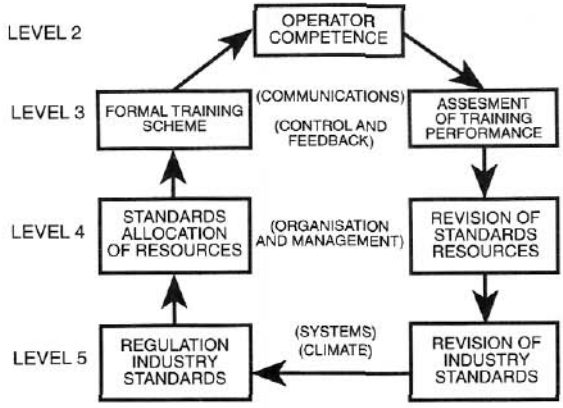

Fig.9 - Control loop - training

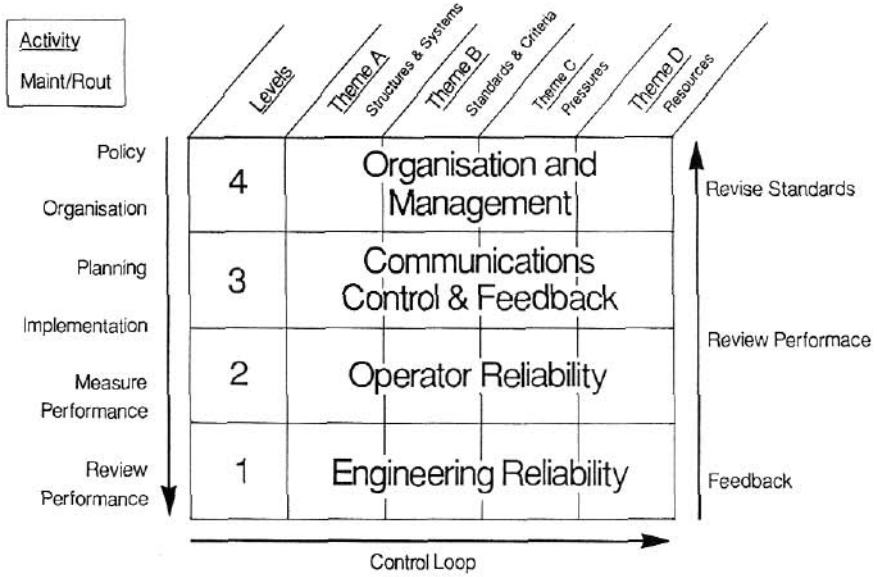

Fig.10 - Arrangement of question set cells

HSE
Health & Safety Executive

S T A T A S

HAZARD IDENTIFICATION IN THE DESIGN OF PLANT
(Des/HAZ)

Origins of Failure	Prevention/ Recovery *Mechanism*	Weightings %	
		Pipework	Vessels
Design	Hazard studies	25	29

KEY ISSUES:
Design criteria, materials, venting, fire precaution, process parameters.
Modification procedures.
Formal hazard studies (HAZAN, HAZOP etc).
Consequential changes (P and I diagrams), Standard *Operating Procedures*.
Multi-disciplinary team composition; leadership and duties.
Programmable electronic systems and ergonomic factors.
Instrumentation and controls.
Location of hazardous plant in relation to control rooms and office locations.
Lessons from previous incidents locally, nationally and worldwide.

TESTED AT:

LEVEL 4
Organisation and management structures.
Roles, responsibilities and resources.
Priorities and standards; setting and review.
Data management.

LEVEL 3:
Procedures for monitoring, feedback and auditing.
Formal, informal and written communications and meetings.
Documentation control.
Team membership and job specifications.
Training, experience and qualifications of team members.

LEVEL 2:
Operator awareness and competency.
Active participation in change procedures.

LEVEL 1:
Evidence of implementation of procedures.
Appropriate shutdown systems, pressure relief settings etc.

ASK	OBSERVE	CHECK

Fig.11 - Example of summary sheet