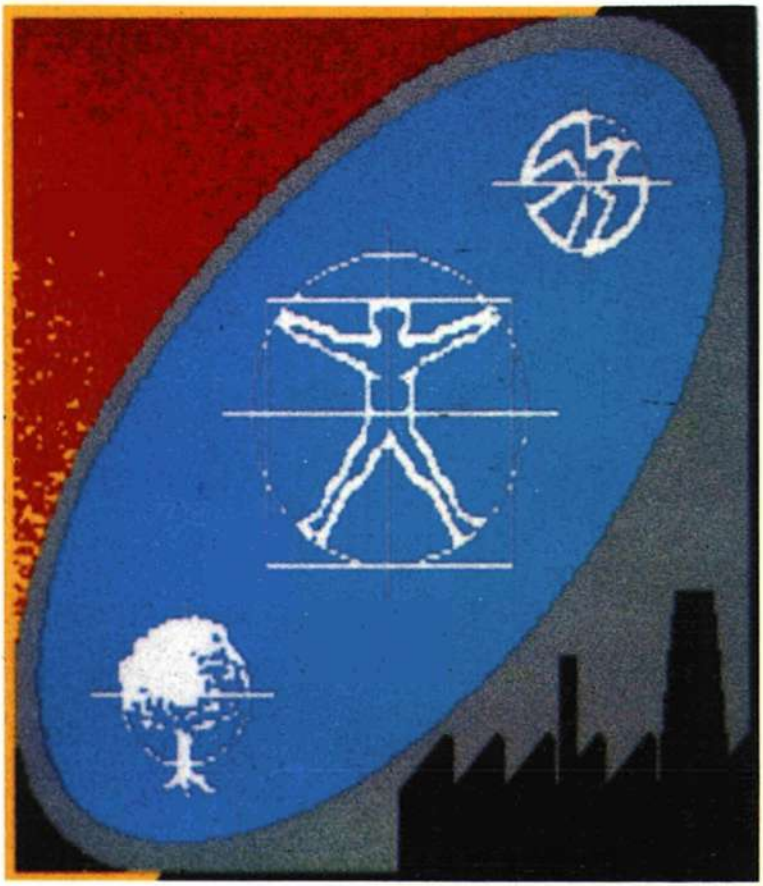
INSTITUTE FOR SYSTEMS ENGINEERING AND INFORMATICS

SAFETY MANAGEMENT SYSTEMS IN THE PROCESS INDUSTRY

Proceedings
CEC Seminar on 7/8 October, 1993
Ravello (SA), Italy



Report EUR 15743 EN

JOINT RESEARCH CENTRE
EUROPEAN COMMISSION

An audit technique for the evaluation and management of risks

A.J. Muyselaar
Ministry of Housing, Physical Planning and Environment (VROM)
The Hague

L.J. Bellamy
Four Elements Ltd, Industrial Safety Consultancy,
London

Summary

The Seveso directive is implemented into Dutch regulations by two different ministries through the obligation to submit Occupational and External Safety Reports for Major Hazard installations. Unlike the Occupational Safety Report, until recently the aspect of Management of Safety has not been addressed to the same extent in the External Safety Report.

It was the increasing attention towards the influence of safety management in the process industry in the late eighties that led the responsible External Safety Division of the Ministry of Housing, Physical Planning and the Environment (VROM) in the Netherlands to join the UK Health and Safety Executive in commissioning a series of research projects to determine how Management and Organisational factors affect the potential for major loss of containment accidents. In these projects particular emphasis was put on empirical research of historic data. Two separate techniques were used to identify management related causes in the different areas of influence and layers of the organisation. Much effort was further spent in the development and application of audit question sets and the relation between (management) performance indicators and generic failure rates used in QRA. This work resulted in a rough set of audit questions with which a factor for the performance of management could be determined.

Experience in testing this Process Safety Management System Audit points out that there is great potential to use the audit system as an inspection tool with particular focus on Major Hazardous installations. At the moment a revised prototype version has been developed based on earlier test experiences and the recommendations of an expert group, with representatives of different (government) authorities and industry. This prototype has very recently been tried out for the first time and will be further tested next year at different Seveso sites in four European countries in a collaborative CEC project.

Introduction

In the Netherlands the Seveso directive is mainly implemented through the occupational Safety Report, concerning risk to employees, and the External Safety Report, concerning risk to the population. The Ministry of Social Affairs is primary responsible for the Occupational Safety Report and the Ministry of Housing, Physical Planning and the Environment (VROM) for the External Safety Report. Up until now the management aspect has not been addressed as much in the External Safety Report as it is in the Occupational Safety Report, in which an extensive description of organisational and management aspects is required. It was the obligation in the Dutch Major Hazards Decree in 1989 to perform Quantitative Risk Analysis as part of the External Safety Report however which added considerably to the discussion on the actual quantitative contribution of individual management of plant safety to the quantification of risks. Also the Human Factor in accident causation was getting more attention as the result of investigations with evidence of human failures in major accidents like Bhopal and Chernobyl.

In a QRA the risks that a potentially hazardous installation presents to the external population must be expressed in the form of probabilities of death for humans per year. The basis of a QRA is the list of assumed representative failure scenarios, with descriptions of potential releases at standard failure frequencies. A release of hazardous material develops eventually into a potential lethal dose, which is expressed as a lethality probability for humans. There is general agreement between government and industry on the important parameters for the choice of representative failure scenarios and type of models necessary to calculate risks.

A recurrent issue has always been the failure statistics which are based on industry averages derived from historical accident data of major accidental releases of pipes, vessels, etc. These generic failure rates implicitly take account of all possible influences, including the human factor and the (absence of) safety management systems, which led to failure. This is not always true when methods like fault tree analysis are used, because of the lack of specific statistical data on relevant contributors, e.g. human factors and the effectiveness of safety management systems. Also it is by definition almost impossible to identify the unknown sequences of events which in the future could lead to failure. The generic approach however does not provide for different numbers to take account of the now recognised major influence of individual process safety management systems. The Process Safety Management System Audit gives an alternative to the identification and quantification of safety management. In the following sections a description is given of the structure of the technique as well as its merits as an audit tool.

Initial developments

To effectively manage chemical process safety, it is important to identify more than just the direct causes of loss of containment (LOC) accidents, such as corrosion of a pipe, or overpressure of a vessel. One must also understand where the unsafe condition resulting in a failure originated, and why that unsafe condition was not detected and rectified. By considering the underlying causes of past accidents, valuable insights can be gained as to which facets of safety management are likely to benefit most from increased attention, thus producing the greatest improvements in overall plant safety.

In 1988 the Health and Safety Executive funded a project to examine the underlying causes of failure in loss of containment accidents on chemical and petrochemical plants. Originally, the intention had been only to separate the human from the mechanical causes of failure but this work led eventually to the development of the Process Safety Management System Audit, now the subject of CEC research.

As the project developed VROM, Norsk Hydro and BP also became involved. This collaboration of industry and regulator opened up access to extensive loss of containment accident data both within and between companies as well as providing test sites for assessing the audit.

In the early development phases of the research for the audit system, the results of the methods used in analysing the available historical failure data into direct and underlying causes provided for the structure of the system. Relevant areas of influence, like Maintenance and Design, were identified and their contributions to vessel, pipe and hose failure, quantified. It was found that more than 95% of all failures could be linked to lack of action of management.

Experiences with the audit system so far

This year different versions of the audit have been tried out at two different plants in Europe; a fertilizer plant in France and an alkylation plant in the UK. Apart from ways to improve the audit, which were discussed by an international expert group, the impression was reinforced that the audit system appears to be useful in more than one way. It enables the examination of the integrity of control and monitoring loops of safety management relevant for the prevention of major accidents. Also the quantification of contributing elements within an organisation enables the generation of an overview of the performance of plant safety management with its strong and weak points and the possibility to generate and prioritise possible risk reducing measures. In this respect it provides plant management and the authorities with possible areas of improvement to follow with reference to the management of major hazards. The structure of the audit also enables the investigation of issues with a less direct link to (the quantification of) major hazards, e.g. environmental hazards and emergency response.

With the scarce data on failure statistics available, other than indications of possible relationships, it appears to be very difficult to find evidence to express performance of management in a single relevant factor. Further research in this area is still necessary for incorporation into Quantitative Risk Analysis.

Three Dimensional Classification Scheme

Initially, about 500 incidents involving pipework failure and subsequent chemical releases were analysed, specifically with regard to the human contributions to the accidents (Bellamy, Geyer and Astley, 1989). This study was later followed by a similar analysis of approximately 200 vessel failures (Bellamy and Geyer, 1991), and 160 hose and loading arm failures (Wright and Tinline 1993). As this research progressed, it soon became apparent that there was a difference between human error as a direct cause of failure and as an underlying deeper cause of equipment failure and human error triggers.

In order to capture this human component at both levels, a three-dimensional (3-D) classification scheme was developed (Table 1). Each accident was placed in one or more categories on all three dimensions. At best, previous classification schemes have only looked at two ways of classifying failure (e.g. Blything and Parry, 1988). One is the direct cause such as corrosion or human error (e.g. opening a wrong valve). The other looks at the operation taking place within which the failure occurs e.g. maintenance.

The 3-D model, however, added the extra dimension of management failure. These were failures to either prevent the unsafe conditions arising, or failures to recover unsafe conditions. The accidents were classified on this dimension by considering what management preventive or recovery mechanisms would have worked in that particular case. This avoided the impossible task of having to obtain data on the management characteristics which were present in the organisation at the time of the accident.

The analysis enabled the statistics of direct and underlying cause contributions to loss of containment (LOC) accidents to be reviewed for the dominant contributors.

The results were very interesting. For example, in the study of pipework failures (Bellamy, Geyer and Astley 1989; Hurst, Bellamy, Geyer and Astley, 1991), 24.5% of all pipework failures had an underlying management failure contribution of inadequacies in hazard review of design (the biggest single cause), 14.5% in human factors review of maintenance, 13% in supervision of successful completion of maintenance tasks, 11% in human factors review of operations. Maintenance was the biggest single origin of the cause of a pipework failure (38.7% of all origins of causes).

Table 1. Three levels of causes for chemical releases from pipework failures.

Level	Examples
Direct Causes	Corrosion Erosion External Loading Impact Overpressure Vibration Temperature Wrong In-Line Equipment or Location Operator error Defective Pipe or Equipment (Cause Unknown) Other Unknown
Origins of Failure (Underlying Cause)	Design Manufacture or Assembly Construction or Installation Operations during Normal Activities Maintenance Activities Natural Causes Domino Effects Sabotage Unknown
Recovery Failures in... (Underlying Cause)	Appropriate Hazard Study of Design or As-Built Facility Human-Factor Review Task-Driven Recovery Activities (Checking, Testing, and Correction of Completed Tasks) Routine Recovery Activities (Routine Inspections and Tests, Process Sampling, Safety Audits) Not Recoverable Other

A Sociotechnical Model

In parallel to the data analysis, a theoretical model was developed (Figure 1) - the Sociotechnical Pyramid -to link the influence of management to direct causes of failure. This model presents management influences as the link between more remote (base of pyramid) to direct (top of pyramid) causes of failure. This concept of a hierarchical scheme of accident causation is not a new one. However, the scheme takes into account:

- the climate within which a company operates (regulatory, economic, know-how),
- the company organisation and standards,
- the control, communication and coordination processes,
- monitoring of and feedback on the effectiveness of management control, and
- front line personnel competence and task support (interface, tools, procedures etc.).

Question Generation

Unlike previous audit schemes, the Process Safety Management System Audit has been developed through a "bottom-up" approach to LOC accident analysis, as opposed to the "top-down" method of identifying what are considered to be the important management characteristics of companies with the best safety records.

The current audit still addresses these topics but in an entirely different way; it is the integrity of the safety management system which is of interest, rather than the treatment of each topic in isolation. Nonetheless, the audit still addresses the major "top-down" areas, as Table 2 shows.

The pyramid of causes, from climate level up to direct engineering and human reliability causes, was combined with the 3-D statistical data model to provide a question generation mechanism appropriate to an audit of process safety management. The idea was that the 3-D data indicated areas in which an assessment of management was important (i.e. prevalent underlying causes of failure), such as hazard review of design, and the sociotechnical pyramid indicated an appropriate audit trail. This provided the basis for generating a set of questions which would globally cover the management influences underlying loss of containment, and provide a means of quantifying the importance of the questions, using the data model.

Table 3 shows the results of the statistical analysis of the underlying causes of pipework and vessel failures. The eight main (most important) audit areas, derived from the largest scorers in the table, are:

1. DES/HAZ Hazard review of design
2. MAINT/EIF Human factors of maintenance

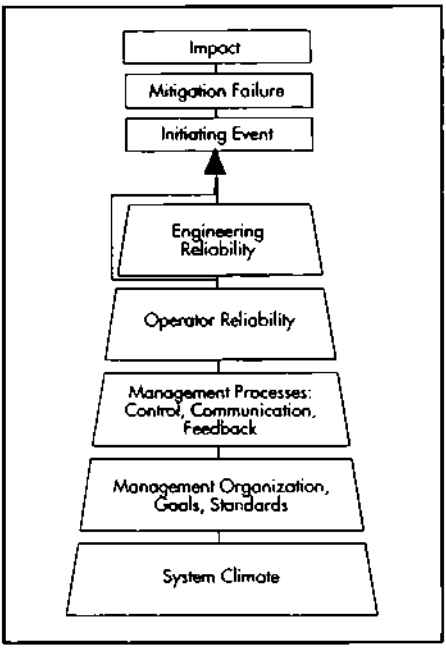


Figure 1 Sociotechnical pyramid

3. MAINT/CHEC Task checking and supervision of maintenance
4. MAINT/ROUT Routine inspection, testing and maintenance
5. OP/HF Human factors of normal operations
6. CON/CHEC Task checking and supervision of construction work
7. OP/HAZ Hazard review of normal operations
8. OP/CHEC Task checking and supervision of normal operations

There were also four themes (for explanation, see next section):

Theme A - Procedures and processes to do the job.
Theme B - Standards for the job.
Theme C - Do other pressures interfere with the job?
Theme D - Are there adequate resources for the job?

Examples from the audit questionnaire are shown in Annex 1. The design of the format for the question set was assisted by an "Expert Group" made up from experts in auditing from industry and the regulator.

Table 2: COMPARISON OF PROCESS SAFETY MANAGEMENT SYSTEM AUDITING TECHNIQUES

ISSUE: LEADERSHIP AND THE MANAGEMENT OF CHANGE							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Leadership & Administration	Management Leadership	Top Management	Accountability & Responsibility + Management of Change	Management of Change	Management of Change	Management of change/ organisational factors	System Climate (Level 5) & Organisation & Management (Level 4) Issues Particularly Theme C Pressures
ISSUE: COMPETENCE OF PERSONNEL AND TRAINING							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Management Training + Employee Training + Hiring & Placement	Personnel	Training	Training and Performance	Training	Training	Training	Operator Reliability (Level 2) Issues Particularly in HF recovery mechanism areas
ISSUE: MAINTENANCE AND INSPECTION							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Planned Inspection	Maintenance & Inspection	Inspection + Maintenance	Process Equipment Integrity	Pre-startup Safety Review + Mechanical Integrity	Critical equipment QA and Mechanical Integrity + Safe Work Practices + Pre-startup Safety Review	Maintenance	All MAINT underlying failure areas + all other CHEC recovery mechanism areas
ISSUE: ACCIDENT / INCIDENT INVESTIGATION AND ANALYSIS							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Accident / Incident Investigation + Accident / Incident Analysis	Incident Investigation	Loss Prevention	Incident Investigation	Incident Investigations	Process Related Incident Investigation	Incident and Accident Reporting	Communication, Control & Feedback (L3) Issues
ISSUE: EMERGENCY PLANNING AND RESPONSE							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Emergency Preparedness	Emergency Management	Contingency Plan: particularly for Loss Prevention	Emergency Response Planning	Emergency Planning & Response	Emergency Response and Control	Emergency Resources and Procedures	Not included in main audit since not relevant to the modification of failure rates Emergency Response questions are now available specifically addressing evacuation from flammable releases
ISSUE: OPERATING PROCEDURES							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Job Analysis & Procedures	Technology + Personnel: Safe Work Practices	Operations: Procedures	Process Safety Knowledge	Operating Procedures	Operating Procedures	Written procedures	OP/HAZ and OP/HF areas Particularly Theme A: Procedures
ISSUE: HAZARD ANALYSIS OF ENGINEERING DESIGN							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Purchasing and engineering controls	Technology	Engineering	Process Safety Knowledge	Process Hazard Analysis	Process Hazard Analysis	Safety Policy + Formal Safety Studies	DES/HAZ issues.
ISSUE: COMMUNICATIONS							
ISRS	CMA	SMAPI	CCPS	OSHA	API	MANAGER	PRESENT TECHNIQUE
Personal Communications + Group Meetings	Management Leadership. Information sharing	Communication topic within each area	Human Factors	Management of change?	Management of change?	Organisational Factors	Communication, Control and Feedback (L3) issues

Table 3: % Contribution of Underlying Causes to Pipework (n=492) and Vessel Failures (n=193) (All unknown origins and unknown recovery failures removed). Origins of failure are shown across rows and recovery failures in the columns.

	NOT RECOVERABLE		HAZARD STUDY		HUMAN FACTORS		TASK CHECKING		ROUTINE CHECKING		TOTAL	
	Pipes	Vessels	Pipes	Vessels	Pipes	Vessels	Pipes	Vessels	Pipes	Vessels	Pipes	Vessels
Natural Causes	1.8	0.5	0	0	0	0	0.2	0	0	0	2	0.5
Design	0	0	25	29	2	0	0	0	0.2	0.5	27.2	29.5
Manufacture	0	0	0	0	0	0	2.5	0	0	0	2.5	0
Construction	0.1	0	0.2	0.3	2	0	7.6	1.8	0.2	0	10.1	2.1
Operations	0	0	0.1	5.4	11.3	24.5	1.6	2.1	0.2	0	13.2	32
Maintenance	0	0	0.4	2.1	14.8	5.7	1.3	3.6	10.5	10.8	38.7	22.2
Sabotage	1.2	1	0	0	0	0	0	0	0	0	1.2	1
Domino	4.6	11.9	0.2	0.3	0	0	0	0	0.3	0.5	5.1	12.7
TOTAL	7.7	13.4	25.9	37.1	30.1	30.2	24.9	7.5	11.4	11.8	100	100

The Control and Monitoring Loop

Previous audit schemes have concentrated on evaluating the separate components of a management system, such as training, permit-to-work systems, documentation, accident investigation, management of change etc. The current scheme, however, focusses on evaluating the integrity of the management control and monitoring loops that run vertically through the organisational structure. The generic Control and Monitoring Loop is shown in Figure 2. This important aspect of the audit trail was derived from earlier work by Bellamy (1983) on the prevalence of organisational aspects of accidents, particularly communication problems, which resulted in unsafe conditions developing within a system and remaining undetected. From this early work four themes were derived which recurred in major system failures. The most prevalent was communication failures across organisational boundaries. The other themes were failures caused by pressures (e.g. time, peer group, workload, uncertainty), equipment and people resources problems (e.g. insufficient means of communication, lack of required skills, organisational overlap in use of resources), and organisational rigidity in response to change (e.g. failure to upgrade standards and personnel awareness). Typically then, an organisation prone to accidents might be expected to exhibit many of the following features:

• Poor control of communication and coordination:

- between shifts.
- upward from front line personnel to higher management in the organisational hierarchy and downward in terms of implementing safety policy and standards throughout the line of management (particularly in a many-tiered organisation).
- between different functional groups (e.g. between operations and maintenance, between mechanical and electrical).
- between geographically separated groups.

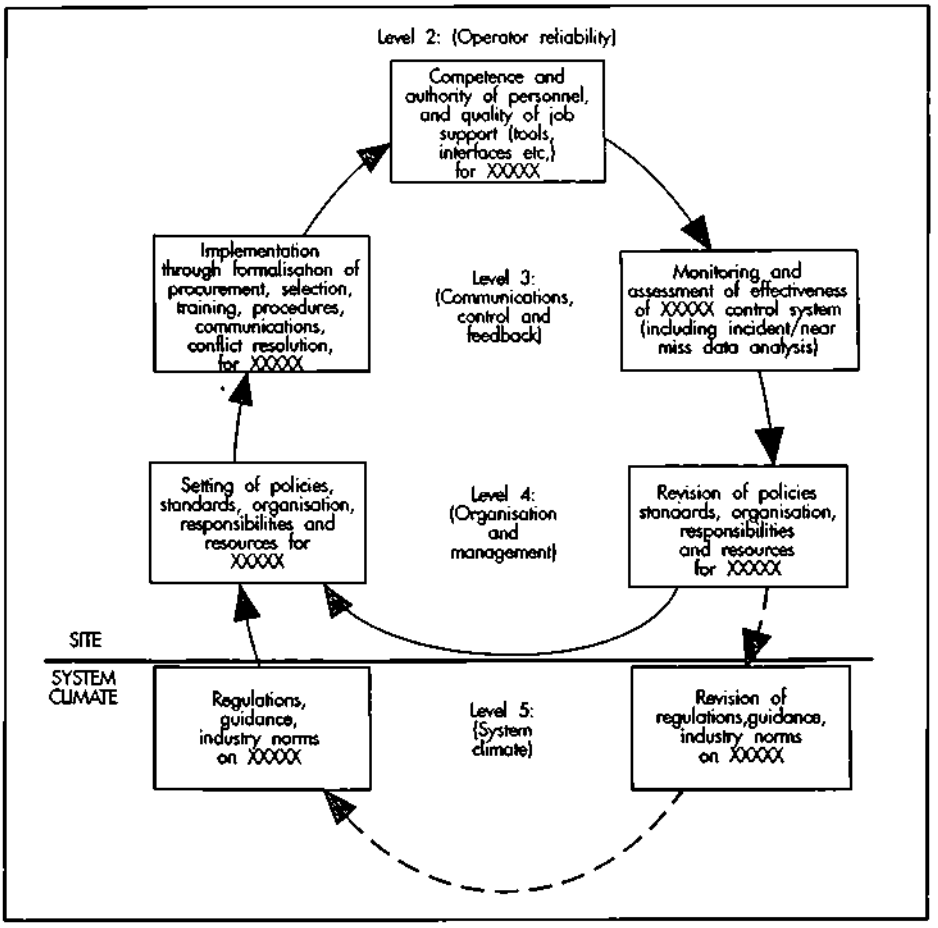


Figure 2 The Control and Monitoring Loop

- in inter-organisational grouping (particularly where roles and responsibilities overlap) such as in the use of sub-contractors, or in an operation which requires the coordination of multiple groups within the same operational "space".
- in heeding warnings (which is one of the important manifestations of the above where the indicators of latent failures within an organisation become lost or buried).

• Inadequate control of pressures:

- in minimising group or social pressures.
- in controlling the influence of workload and time pressures.

- of production.
- of conflicting objectives (e.g. causing diversion of effort away from safety considerations).

• Inadequacies in control of human and equipment resources:

- where there is sharing of resources (where different groups operate on the same equipment), coupled with communication problems - e.g. lack of a permit-to-work system.
- where personnel competencies are inadequate for the job or there is a shortage of staff.
- particularly where means of communication are inadequate
- where equipment and information (e.g. at the man-machine or in support documentation) is inadequate to do the job.

• Rigidity in system norms such that systems do not exist to:

- adequately assess the effects and requirements of change (e.g. a novel situation arises, new equipment is introduced).
- upgrade and implement procedures in the event of change.
- ensure that the correct procedures are being implemented and followed
- intervene when assumptions made by front line personnel are at odds with the status of the system.
- control the informal learning processes which maintain organisational rigidity.

It was clear that the safety aspects of a hazardous system were very dependent on the integrity of management of the control and monitoring system. In fact, it was not only very important that the different layers of management down to front line operations implemented and preserved the necessary safety functions of the system, it was also vital that the status at the front line was fed back to higher level management. This "discovery" led to the fundamental concept of the control and monitoring loop which is the key to the audit system.

The Good, the Bad and the Average Process Safety Management System

The model of the Process Safety Management System is that it is composed of a number of essential control and monitoring loops (i.e. in the 8 important areas described above). This means that the definition of a "good" plant is contained within the logic of the control loop concept, rather than being associated with changing industry standards and regulatory guidance for each of the components (training, inspection, procedures etc.).

The following text gives an example of the control and monitoring loop for the area "Hazard Review of Design":

HAZARD REVIEW OF DESIGN AND MODIFICATION AND FOLLOW UP (DES/HAZ) CONTROL AND MONITORING LOOP

Level 5 -> Level 4

There is evidence that senior management are aware of the regulations, guidance, industry and parent company norms concerning hazard reviews of the engineered design of a plant/process and modifications to plant/process. They take account of these norms, regulations and guidance in their own site policies and standards relating to hazard reviews of design.

There is allocation of authority, roles and responsibilities for hazard review of design in the organisational structure, and allocation of resources to meet the role requirements. The site management's policies and standards on hazard review of design are not compromised by system climate factors such as economic pressures and limitations in resource availability.

Level 4 -> Level 3

Management are committed to carrying out hazard reviews of design and modifications to plant/process. This commitment is shown through the actual implementation of policies and standards.

The implementation of policies and standards on the hazard review of design is achieved through formalised selection and training procedures for competence, and the provision of standard procedures and communications, and procurement of the tools, for the job. There is a way of resolving conflicting pressures acting against hazard reviews of design and modifications.

Level 3 -> Level 2

The tasks of hazard review of design and modifications are carried out by competent personnel who have adequate support for the job in terms of training, procedures, and tools for the job. Conflicting pressures acting against hazard review of design are resolved without detriment to the hazard review and follow-up process.

Level 2 -> Level 3

The effectiveness of hazard reviews of plant design and modifications are systematically assessed. There is a management system in operation that monitors whether the site standards of procedures and communications, human and equipment resource allocation, and methods of conflict resolution are adequate, are being adhered to, and that those responsible for carrying out hazard review of design tasks are fully competent.

Level 3 -> Level 4

Systems are in place and used for collecting and assessing information on the effectiveness of hazard review of design. These systems include collecting and analysing incident and/or near miss data. Assessments of the effectiveness hazard reviews and their follow-up are used to revise site policies, standards, priorities, definition of authorities and responsibilities, and allocation of resources.

For the purposes of assessing the quality of the Process Safety Management System, the audit evaluation is performed on a 3 point scale of Good, Average and Bad for each of the 8 most important control and monitoring loops. The judgement for each control and monitoring loop area is assisted by having text descriptions or "anchor points" which have been found to help maintain inter-auditor consistency. The anchor points are as follows:

Good

The Safety Management System (SMS) of a good plant is represented by the diagram of the Control and Monitoring Loop (Figure 2). It is difficult to find evidence of weaknesses within any of the key elements. The system components are specified by the boxes and links between them. The system components and links are in place. They are actively used. There is complete integrity within the Control and Monitoring Loop. There is a continuous process of improvement.

Average

On the whole, the SMS of an average plant is represented by the diagram of the Control and Monitoring Loop (Figure 2). However, there is some evidence of weaknesses within the system components specified by the boxes *or* links between them.

The system components and links are in place. The systems are *normally* used. Sometimes there is not complete integrity of the Control and Monitoring Loop (sometimes systems are not used or are used incorrectly). The process of continuous improvement contains weaknesses.

Bad

Rarely does the SMS of a bad plant match the diagram of the Control and Monitoring Loop. There is considerable evidence of major weaknesses and absences of system components specified by the boxes or links between them. Not all system components and links are in place. Ad hoc systems may be used There is no integrity of the loop. The process of continuous improvement may be absent or have considerable weaknesses.

In making the evaluation, the auditor is required to state the main reasons for his or her judgments by stating: "Maint/chec is judged to be bad because..." or "Op/HF is judged to be good because..." etc. These statements then form the basis for reporting the strengths and weaknesses of an installation's Process Safety Management System.

Quantification of the Audit Results

Another unique characteristic of this audit system is that recommendations for improvements can be prioritised, and the effect of the SMS on the likelihood of loss of containment rates quantified.

Each of the eight areas of the audit has a weighting associated with it, based on

the results of the statistical analyses of the LOC accidents. The proportions of causal contributions in each of the underlying cause areas for vessels and pipework is shown in Table 3. Thus, for example, task checking of maintenance has a weighting of 13% for pipework and 3.6% for vessels. When these weightings are combined with the area judgements (good, average, or bad) it becomes possible to prioritise recommendations.

The combined weightings and qualitative evaluations are used to produce a single number or "Management Factor" (MF) for the overall Process SMS for that site derived from the weighted proportions of Good, Average, and Bad. The purpose of this MF number is to make relative comparisons between sites and as a multiplier for generic failure rates. Recent work in this area is producing scales of Management Factors based on the frequency distribution of LOC accidents (indexed for site size). A Management Factor of 1 is defined as the quantification of the quality of management on the Average plant. The deviation from this Management Factor towards Bad or Good is related to the distribution of the indexed LOC data. However, as this work is not yet concluded, we are currently using a technique from the MANAGER audit which generates MF values based on expert judgement. These MF values range from 0.1 to 100.

Concluding remarks

Regarding the Process Safety Management System Audit it can be said that it is unique in a number of ways:

1. It specifically addresses the underlying management causes of loss of containment accidents.

2. The audit has been developed in a "bottom-up" manner by analysing the causes of loss of containment accidents, rather than by the "top-down" method of looking at what the "better" performing companies do. The former is considered to be a preferable approach because it covers all known management causes of loss of containment accidents whereas the top-down approach cannot guarantee this. For example, the top-down approach tends to identify "better" with those companies having the lowest lost time injury rates. While implementation of the recommendations from a top-down audit might be expected to reduce LTIs, we have found that LTI rates and LOC rates do not correlate.

3. The audit evaluates the completeness, strengths and weaknesses of management control and monitoring loops rather than being topic based. There are 8 key loops which have been identified as those areas which are the predominant management failure causes of loss of containment accidents. Any audit approach which is solely topic based and which fails to simultaneously evaluate control and monitoring loop "integrity" will not fully address the underlying causes of loss of containment accidents.

4. The auditor does not require industry standards or regulator guidance against which to evaluate a site. Rather, three levels of control and monitoring loop "integrity" are defined, which are logically derived and therefore will not require revision as industry and regulator change their standards.

5. The weightings given to the different areas of the audit enable prioritised recommendations to be made in relation to reducing the likelihood of loss of containment accidents. No other audit is currently able to do this.

6. As well as its use as a audit tool, the PSM system audit is designed to enable the results of its application to be fed into Quantitative Risk Assessment to modify failure rates. Although the audit is not the only one available which can do this, it is unique in that the question set has been designed with this purpose specifically in mind, and therefore all the questions are directly relevant to modification of generic failure rates.

The overall conclusion is that at the moment the audit described in this paper is the only one which adequately addresses the safety management system associated with preventing loss of containment accidents in process plants.

In addition to the findings of the collaborative CEC project mentioned, in which the audit is tested in four EC countries, VROM will put effort into tailoring the audit for use in the Netherlands. This means integrating the audit with existing audit/inspection systems in operation and the examination of possibilities to fit a method like this into the regulatory system. It also means examining the consequences regarding possible overlap in Occupational and External Safety reporting. Although the prototype Process SMS Audit as it is can be readily used for the generation of management factors further research in this area is still necessary for incorporation into Quantitative Risk Analysis.

References

Bellamy, L.J. (1983) *Neglected individual, social and organisational factors in human reliability assessment.* Reliability '83, Proceedings of the 4th National Reliability Conference, Birmingham, UK, Vol.1 pp. 2B/5/1-2B/5/11.

Bellamy, L.J. (1986) *The Safety Management Factor: An Analysis of the Human Error Aspects of the Bhopal Disaster.* Safety and Reliability Society Symposium, 25 September 1986, Southport, UK.

Bellamy, L.J., Geyer, T.A.W., and Astley, J.A.A. (1989) *Evaluation of the human contribution to pipework and in-line equipment failure frequencies.* HSE Contract Research Report No. 89/15.

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

Bellamy, L.J., Wright, M.S. and Hurst, N.W. (1993) *History and development of a safety management system audit for incorporation into quantitative risk assessment.* International process Safety Management Workshop, San Francisco, 22-24 September, AIChemE/CCPS.

Besluit risico's zware ongevallen (Decree containing regulations on the notification of hazards of certain industrial activities), Staatsblad 1988, 432, The Hague

Council directive of 24 June 1982 on the major-accident hazards of certain industrial activities, 82/501/EEC

Hurst, N.W., Bellamy, L.J. and Geyer, T.A.W.(1991) *A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies.* J. Hazardous Materials, 26 (1991) 159-186.

Hurst, N.W., Bellamy, L.J., and Wright, M.S. (1992) *Research models of safety management of onshore major hazards and their possible application to offshore safety.* pp. 129-148 in Proceedings of I.Chem E. Symposium Series No.130, "Onshore and Offshore", Manchester, UK.

Wright, M.S. and Tinline, G. (1973) *Further development of an audit technique: Tasks 1-4, Completion of databases.* Four Elements Report C2278, 30th July 1993.

Annex I: Examples of question set format

MAINT/CHEC: TASK CHECKING IN MAINTENANCE

Introduction

This area concerns the checks carried out before and during maintenance work and in the hand-over phase following the completion of maintenance to ensure the following:

- safety tests and precautionary actions which are required before carrying out maintenance work, such as gas tests, have been carried out as required:
- maintenance work, such as replacing piping, has been carried out as required; - equipment has been made safe before re-commencement of operations.

These checks may be formal checks required as part of PIWs, informal checks carried out by pairs of fitters upon each other's work, or standard procedural checks, such as Operators reviewing the state of a component before accepting it back into operation.

Weightings

Pipework - 13%
Vessels - 3.6%

Key Issues

1. *Company experience* of *and expertise* in the task checking and supervision of inspection, testing and maintenance.
2. *Management awareness of industry norms* on the task checking and supervision of maintenance.
3. *Policy* on task checking and supervision of maintenance *and strategies of policy implementation.*
4. *Allocation of responsibilities* for the task checking and supervision of maintenance
5. *Means of changing system* of task checking and supervision of maintenance.
6. *Content of job descriptions.*
7. *Documentation* covering the task checking and supervision of maintenance.
8. *Systems for indicating and communicating status of plant.*
9. *Systems for verification* of *and compliance* with policy and procedures for task checking and supervision of maintenance.
10. *Evidence at operator and supervision levels of successful methods and adequate understanding of responsibilities.*

...

24. *Communication between management levels, shifts and across functional interfaces.*

25. *Process of safety performance goal setting and impact of QA process.*
27. *Control of work systems* for task checking of maintenance *including PTWs.*
28. *Scope of procedures* for task checking of maintenance.
29. *Usability and content of procedures* for task checking of maintenance.

MAINT/CHEC THEME A PROCEDURES AND PROCESSES TO DO THE JOB

Question No.	Question Explanatory Note / Optional Question	Suggested Interviewee	Key Issue
A.4.2	**Describe the policy and approach to checking maintenance work.** This may include: - are personnel meant to be responsible for checking and ensuring the quality of their own work? - is there a system of systematic double checking by independent personnel, such as safety officers and operations personnel? - are checks formalised into procedures or regarded to be part of standard practices?	Maintenance management	3
A.4.3	**What is the method for revising the approach to checking maintenance work in the light of experience?**	Maintenance management	7
LEVEL 3	COMMUNICATIONS, CONTROL AND FEEDBACK		
A.3.1	**What documentation is available regarding the roles and responsibilities of persons involved in checking maintenance work?** Issues covered by documentation may include: - are the supervisory and work inspection responsibilities, such as gas tests and weld inspections, of safety officers and maintenance supervisors noted in job descriptions? - do operations procedures specify that certain personnel shall carry out checks of systems before authorising them back into operation?	Maintenance management and supervisors.	7, 4 & 6
A.3.2	**Describe the procedures available for carrying out checks before, during and after maintenance work?** Procedures may include: - gas test, isolation checks, purging checks, pressure tests etc specified as part of Permit To Work procedure; - checks on quality of maintenance work done, perhaps specified as part of a quality control system; - checks on integrity of plant before authorization back into operation, perhaps specified as part of Standard Operating Procedures.	Maintenance management and supervisors. Safety management.	28 & 29