Auditing – a European perspective

Nicholas W. Hurst*, Robin Hankin*, Linda J. Bellamy† and Michael J. Wright†

*Health and Safety Executive, Sheffield S3 7HQ, UK
†Four Elements Ltd, Greencoat House, Francis Street, London SW1P 1DH, UK

This paper describes the background research, development and application within the UK Health and Safety Executive (HSE) of an audit technique for assessing the effectiveness of safety management systems at onshore major hazard sites. The work is driven by HSE's use of quantified risk assessment for formulating advice to local planning authorities on the siting of major hazards and the development of land in their vicinity. The work aims to assess whether it is possible to use the auditors' assessment of the standards of safety management such that the effects of different perceived standards can be incorporated into risk assessment procedures. Further development and research are now the subject of a research project, funded by the Commission of the European Communities (CEC).

Keywords: auditing; risk assessment; safety management

Historically, the question of quantifying the management influence on reliability arose a decade ago, and, in the mid-1980s, industry started to query the application of generic failure rate data to all companies and plants, given management differences.

The MANAGER technique (which was developed at DNV Technica Ltd) was an initial solution to this problem and was based on considering the major causes of accidents where a system failure had occurred[1]. A question set was developed based on grouping published and company audit questions together with newly developed audit questions under major causal categories.

The decision as to which questions to include was relatively subjective but the intention was to cover all relevant aspects of the safety management system (SMS). The quantification process was developed from a combination of the auditors' evaluations and a risk modification formula derived from both expert judgement and an examination of the ranges of failure rates of components in the classic Rijnmond risk assessment study[2].

Any possible weaknesses of the MANAGER technique, such as the equal weighting given to each question, the nature of the quantification process and the uncertainty as to whether all the relevant areas were being covered, were offset by the strength of having an investigative method which could, with reasonable time and resources, provide a snapshot of the performance of the SMS and provide an organized set of recommendations. Priorities could be put against these recommendations based on the qualitative evaluation of their significance. However, because the system provides an overall quantitative score, it is possible to compare the SMS performance of different plants. This was an important feature of the audit, given that similar, if not the same, generic failure rates were applied to all plants investigated.

Application of MANAGER has produced findings indicating that SMS influences could reduce risk estimates based on generic failure rate data by about half an order of magnitude or increase them by about an order of magnitude[3]. These quantitative results have not been validated, but the technique offers an alternative to other methods, such as the International Safety Rating System (ISRS), which does not allow the auditors' assessment to be used within any risk assessment carried out at the plant.

Developing a scored audit for regulators

The statistical basis

Against the above background, work was undertaken at the HSE to produce an audit system with a demonstrable statistical and theoretical basis which would have the potential to quantify the quality of an SMS at a plant and link this into any risk assessment carried out.

The process began in 1988 when the HSE funded a project to examine the underlying causes of failure in loss-of-containment accidents onshore, particularly the role of human factors. In order to capture this human component at the direct and underlying cause level, a three-dimensional classification scheme was developed. This three-dimensional scheme (direct cause, underlying cause, failure of preventive mechanism) provided an objective quantitative model on which to base an SMS audit which emphasized loss-

0950-4230/94/020197-04

of-containment accidents as opposed to occupational accidents. The results of this work have been described extensively elsewhere[4–10].

It was argued in previous work[4–10] that the accident data analysed for pipework and vessels also represented the pattern of causes underlying generic failure rate data for pipework and vessels. A further indication of the validity of this derives from an analysis of MARS data (reportable accidents under the Seveso directive[11]) which shows a pattern of causes similar to that for vessel failures. *Figure 1* shows the results for the MARS data. Analogous results[4–10] for pipework and vessel failures show 25% and 29%, respectively, for the design/hazard study category, for example.

The percentage contributions from the two dimensions of underlying cause/preventive mechanism failure have therefore been used to provide the weights for the different sections within the audit scheme. For example, failures in hazard study of design were found to be the most predominant single cause of loss-of-containment accidents and therefore questions in this group have an associated weighting greater than that for questions in other groups (25% for pipework failures and 29% for vessel failures, see References 4–10). The weightings are therefore equivalent to the proportion of accidents having that particular set of underlying causes.

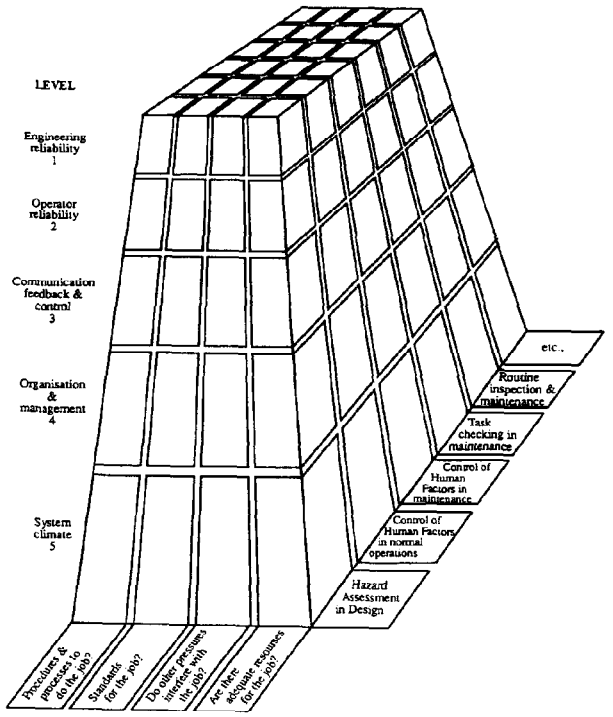

Figure 2 Structure of safety management audit

The theoretical basis

In parallel with the data analysis, a theoretical model was developed (the sociotechnical pyramid) to model the effects of an SMS, and the general climate within which it operated, on failure rates[4]. The pyramid was divided horizontally into levels of causes, and vertically into four themes derived from an analysis of system failures[12]. By combining the data model (three-dimensional classification) and the theoretical model (sociotechnical pyramid), a question generator was produced which provided a set of questions covering all the relevant loss-of-containment causes. This is illustrated in *Figure 2*. In theory, the audit has a set of questions which correspond to each block of the diagram. In practice, the weights of many of the sections are very small and can be ignored. This process is developed in Reference 13 in which it is shown that over 80% of the failures can be attributed to eight of the two-dimensional categories shown in *Figure 1*. These are being used in an experimental audit based on this work[13].

In summary, this section has briefly reviewed the theoretical and statistical basis of the audit scheme, which is based on:

(i) an analysis of industry data describing failures of pipework[4–9],

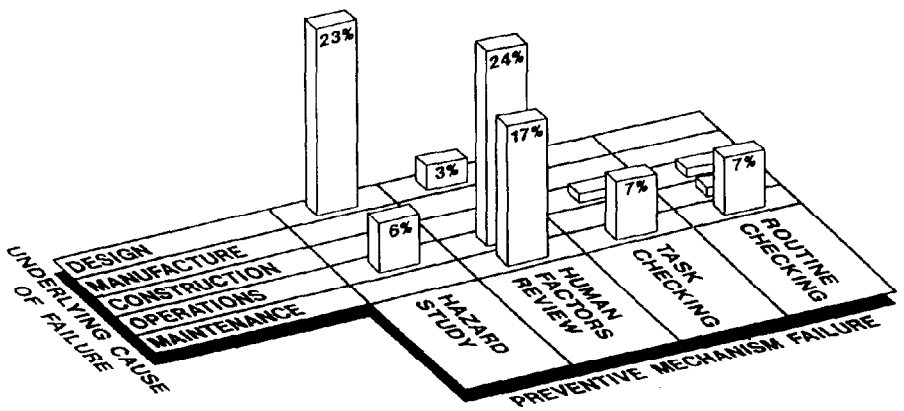

Figure 1 Analysis of accident data: Major Accident Reporting System (MARS)[11]

(ii) an analysis of similar data for failures of vessels[8–10],
(iii) a consideration of authoritative texts on chemical plant risk management, conventional organizational and management theory and management of quality[4,10,14], and
(iv) a consideration of major accident studies and systems failures[5,12]

The key features of the audit are:

(i) a comprehensive question set which covers the main underlying causes of failure and failures of management control systems,
(ii) a statistical analysis of the contribution of these underlying causes to failure rates which enables weights to be applied to the different areas of the audit question set,
(iii) an accident causation model which emphasizes the need to ensure that management control systems are complete and that feedback takes place to allow for constant monitoring and control improvements[15],
(iv) a method which concentrates on completeness of these control systems,
(v) a method which allows different questions to be asked in specific areas without changing the weights attached to that area, and
(vi) a method which does not involve checklist completion but which structures the application of professional expertise by providing a suitable framework and guidance.

Application of the technique

Use within HSE's Field Operation Division

This experimental audit system has been tested within HSE's Field Operations Division (FOD) and is being developed to provide an audit method for the structured inspection of major hazard sites. Within FOD, the system is known as STATAS (structured audit technique for the assessment of safety management systems)[13]. Trials of STATAS have been carried out at two major hazard sites and two further trials are currently in progress. Other trials are also planned.

It needs to be emphasized at this point that the STATAS system is consistent with the management model and control mechanisms illustrated in the HSE Accident Prevention Advisory Unit's (APAU) guidance 'Successful Health and Safety Management' (HS(G)65)[15]. Since STATAS is derived from an analysis of loss-of-containment scenarios and a loss causation model[5], it explores increasingly remote systems failure through levels 1 and 2 (hardware and operator reliability) to level 5 (system climate) (see *Figure 2*). Thus it is inverted in relation to the APAU model which starts with management level commitment to a policy for health and safety. The APAU model[15] 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 continued improvement and development of the system.

The key elements of the APAU booklet are:

- policy development
- organizational development
- planning and implementing
- measuring and reviewing.

The existence of such elements and feedback loops is also discernable through the STATAS audit. Indeed, the complementary nature of the models has been illustrated by considering a systems analysis for training needs[13].

In applying STATAS, the APAU approach to auditing is used. This emphasizes:

(i) a horizontal audit of the senior management structure on a site, to identify the key activities such as maintenance and operations and to assess standards within these areas,
(ii) a vertical audit to investigate management control and feedback by considering the operation of systems from conception (possibly by senior management) through to the workforce who must use the systems,
(iii) the inspection of systems in operation on the plant, and
(iv) a review of documentation, e.g. permit-to-work systems, change order procedures, normal operator instructions, etc.

Possible use to adjust risk assessment calculations

When risk assessment is carried out using generic values for failure rates of items of plant, an assumption is made that the plant is managed to at least 'average' standards. It is considered that generic failure rates include a component of all causes of failure and that generic values therefore reflect 'average' conditions. One aim of the audit system is to enable generic failure rates to be 'adjusted' to reflect non-average conditions and standards of SMS in a risk assessment.

The underlying statistical basis of the question set is described above. We have argued before[4–10] that the percentage contributions from the two-dimensional underlying causes of failure/preventive mechanism failure can be used to weight the components of the failure rates used in a risk assessment. For example, 29% of the failure rate for vessels is attributable to the two-dimensional category of 'hazard studies of design'. These 'statistical' weights for each area of the audit may be combined with the auditors' judgement of 'good', 'poor' and 'average' within each area of the audit to provide a method to carry out a risk assessment which takes into account the standards of management at a plant (as judged by the auditors). One important aim of the research is to develop this area further and to verify the results with plant performance data.

Further development

The audit technique is still being developed as part of a major European research programme being funded by the 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, not only as research tools but also as having potential practical value for both industry and regulatory agencies. Current and future research work is aimed at strengthening and further developing the technique to give it a European perspective. Among other aims, this involves:

- improving the useability of the audit system
- exploring methods to allow 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
- consideration of the uses of the outputs from the system in decision-making in major hazard plants
- collection of data to 'verify' the audit system.

Acknowledgements

The authors are pleased to acknowledge the support of the HSE, VROM and the CEC in funding this work, and the valuable contributions made by others in the development and application of the technique. Special mention should go to Mr K. Ratcliffe of the HSE's FOD for his work on developing the STATAS system.

References

1 Williams, J. C. and Hurst, N. W. 'A Comparative Study of the Management Effectiveness of Two Technically Similar Major Hazard Sites', IChem E Symposium Series No. 130, IChem E, Rugby, Warwickshire, UK, 1992, p. 73
2 Rijnmond Public Authority. 'A Risk Analysis of 6 Potentially Hazardous Industrial Objects in the Rijnmond Area – a Pilot Study', D. Reidel, Dordrecht, The Netherlands, 1982
3 Pitblado, R. M., Williams, J. C. and Slater, P. H. *Plant/Opns Prog.* 1990, **9**, 169
4 Bellamy, L. J., Geyer, T. A. W., Astley, J. A. 'Evaluation of the Human Contribution to Pipework and In-line Equipment Failure Frequencies', Contract Research Report No 89/15, Health and Safety Executive, Sheffield, UK
5 Hurst, N. W., Bellamy, L. J., Geyer, T. A. W. and Astley, J. A. *J. Hazard Mater* 1991, **26**, 159–186
6 Geyer, T. A. W., Bellamy, L. J., Astley, J. A. and Hurst, N. W. *Chem. Eng. Prog.* 1990, **36** (11), 66
7 Bellamy, L. J., Geyer, T. A. W., Wright, M. S. and Hurst, N. W. Presented at the AIChE Spring National Meeting, Orlando, Florida, USA, 18–22 March 1990
8 Geyer, T. A. W. and Bellamy, L. J. 'Pipework Failure, Failure Cases and the Management Factor', Institute of Mechanical Engineers, London, UK, 1991
9 Hurst, N. W., Bellamy, L. J. and Geyer, T. A. W. '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)', eds M. H. Walter and R. F. Cox. Elsevier Applied Science, London/New York, 1990
10 Bellamy, L. J. and Geyer, T. A. W. 'Organisational, Management and Human Factors in Quantified Risk Assessment', ed. J. C. Williams, HSE Contract Research Report 33/1991, Health and Safety Executive, Sheffield, UK, 1991
11 Drogaris, G. 'MARS. Major Accident Reporting System. Lessons learned from Accidents Notified', CEC Joint Research Centre, Ispra, Italy, 1991
12 Bignell, V. and Fortune, J. 'Understanding Systems Failures', Manchester University Press, Manchester, UK, 1984
13 Ratcliffe, K. Presented at the CCPS Int. Process Safety Management Conference, San Francisco, California, USA, 22–24 September 1993
14 Harrison, P. I. and Williams, J. C. 'Organisational Management and Human Factors in Qualified Risk Assessment', HSE Contract Research Report 34/1991, Health and Safety Executive, Sheffield, UK, 1991
15 'Successful Health and Safety Management', Health and Safety Series Booklet HS (G) 65, Health and Safety Executive, Sheffield, UK, 1991