EUROPEAN STATE-OF-THE-ART RESEARCH: INTEGRATING TECHNICAL AND MANAGEMENT/ORGANISATIONAL FACTORS IN MAJOR HAZARD RISK ASSESSMENT

Martin Anderson[1], Health and Safety Laboratory[2]
Broad Lane, Sheffield, S3 7HQ

This paper describes the development and current status of a research project with the objective of providing a model for integrating a broad overview of the organisational and management system of a major hazard site with the initiating events that lead to accidents. Following a desktop trial, this model and the integrated methodology have recently been applied with considerable success at a major hazard installation. This paper outlines the lessons learnt from this exercise and suggests some modifications and considerations prior to a third trial.

Keywords: management, organisational, technical, risk assessment, QRA, audit

BACKGROUND AND RATIONALE

The Health and Safety Executive (HSE) provides advice to Local Planning Authorities concerning land-use planning proposals for the siting of new major hazard plant and for the development of housing etc. in the vicinity of existing major hazard installations. The Health and Safety Laboratory (HSL) and HSE have collaborated over the past 10 years in the development of a range of computerised Quantified Risk Assessment (QRA) tools, collectively known as RISKAT[3], to inform such land-use planning advice.

This suite of QRA tools draw heavily on generic failure rate data. In this context, generic data is derived mainly from historical and some theoretical data. These generic failure rates are incorporated into the numerical estimation of risk from a hypothetical release of hazardous materials from a particular installation. Generic failure rates, being derived from historical and theoretical data, include all causes of failure and should thus reflect 'average' conditions or standards.

Even identical plants can, however, be operated, maintained and managed to varying standards. Hurst (2) describes how the differences in safety performance between technically similar installations may be in the region of three orders of magnitude. Some plants thus may warrant a failure rate different from the generic value to reflect site specific conditions. There was, therefore, interest in these generic failure rates and the extent to which they included management, organisational and human factors in addition to engineering and hardware failures.

---

[1] Now at Human Reliability Associates, 1 School House, Higher Lane, Dalton, Wigan, WN8 7RP
[2] An agency of the UK Health and Safety Executive
[3] Risk Assessment Tool, for example, see Hurst et al. (1)

This interest led to research to examine the underlying causes of loss of containment incidents for the main items of equipment on chemical plant (pipework, vessels and hoses and couplings), with the aim of assessing the contribution of human errors, design problems and maintenance errors to generic failure rates (for example, see Hurst et al., 3). Assuming that the quality of safety management will determine standards of plant design, operation and maintenance etc., the inclusion of these factors in QRA will thus more explicitly consider the standards of safety management. In his discussion of what are perceived to be the strengths and weaknesses of QRA, Hurst (2) emphasises the importance of any such assessment being as transparent as possible. Making more explicit the inclusion of organisational and management factors in QRA is a consideration in the proposed 'agenda for risk assessment' in this recent book.

The above research illustrated how previous loss of containment incidents had occurred and identified practical actions to prevent future incidents. Following this work, the HSE developed an audit technique known as STATAS (Structured Audit Technique for the Assessment of Safety Management Systems). This technique has subsequently been included within a set of tools collectively known as 'The FOD[1] Guide to the Inspection of Health and Safety Management' after being modified within the management system framework described in a HSE (4) document 'Successful Health and Safety Management': HS(G)65.

A subsequent research project for the CEC Environment programme 1992-1994 (summarised in Hurst et al., 5) explored a modification of risk methodology whereby an evaluation of the quality of management was used to modify the generic failure rates of QRA. This methodology had been under development since the early 1980s, stimulated by questions from the process industry who wished to have the quality of their safety management accounted for in risk evaluation, and subsequently by the Regulator requiring tools to investigate a site specific Safety Management System (SMS).

This project involved the application of a safety attitude questionnaire and a process SMS audit tool called PRIMA (Process Risk Management Audit) at six major hazard sites in four European countries. The tools provide quantitative measures of safety attitudes and SMS performance respectively. The work compared these quantitative measures with accident performance data for the six sites. The approach allowed the uncertainty in risk estimates due to variation in safety performance at different sites to be explicitly considered within risk-based decision making. The approach adopted in this research was successful and received much support from the Regulator and industry.

In 1995, a new European research project commenced, sponsored by the European Commission, the Dutch Ministry of Social Affairs and Employment and the Health and Safety Executive. This research, 'Development of an Integrated Technical and Management Risk Control Monitoring Methodology for Managing and Quantifying on-Site and Off-Site Risks', has come to be known as 'I-Risk'. This project brings together a multi-disciplinary team of specialists in Europe on two aspects of risk control in major hazards – organisation and management on one hand and technically orientated approaches on the other. The project participants are:

[1] Field Operations Division of the HSE

- The Division of Labour Circumstances of SZW (the Netherlands Ministry of Social Affairs and Employment), (project co-ordinator);
- SAVE, Netherlands (consultancy);
- Technische Universiteit, Delft, Netherlands (Delft University of Technology);
- Four Elements Limited (consultancy);
- NCSR Demokritos, Greece (National Centre for Scientific Research);
- RIVM, Netherlands (National Institute for Health and Environment);
- Health and Safety Laboratory (HSL).

This team includes consultants, academics, industry and regulators. This project follows on from the previous EC project, which was co-ordinated by HSL and involved several of the above organisations.

Currently, the relationships between different aspects of the control of risks to people and the environment from major accident hazards are poorly modelled and assessed. Methods of evaluating these risks (e.g. Quantified Risk Assessment), management quality (e.g. audit methods), safety culture (e.g. attitude survey) and organisational structures (by reference to organigrams, responsibilities, manning, emergency plans) are not integrated into a single approach which would enhance an examination and understanding of their inter-relationships.

The requirements for Seveso sites to produce Safety Reports have never clearly indicated how the integration of organisation, management and technical systems in controlling the risks should be considered. This is also true of the proposed COMAH revision of the Seveso Directive. This poses potential problems for assessing the overall sociotechnical system of a major hazard site in its control of risks relating to health, safety and for protection of the environment, and for companies in setting priorities for improvement.

PROJECT OBJECTIVES

Thus, the overall objective of this research is to provide a model for integrating the methods of control of risks. The emphasis is on the chemical and petrochemical industry, focussing on major hazard installations at all stages in the installation life cycle. This will give a basis for controlling the interactions between failures at different levels in the sociotechnical system, as have been repeatedly observed in accidents.

The sub-objectives are:

1. Development of an integrated technical and management risk control and risk monitoring model including both on-site and off-site risks and their variation over time. The model will be developed in the context of considering the requirements of the proposed COMAH Directive.
2. Development of an Integrated Quantitative Risk Assessment (I-QRA) method, based on the integrated model from (1), which takes account of management as well as technical design as an integrated whole and which will produce measures both of the risk level and the rate with which this is expected to change over time. The identification of risk

reduction strategies will then be focussed on the system as a whole, not primarily on hardware, and on a more realistic representation of risk as something which changes over time rather than as a time-based average.

3. Development of management 'corrosion' probes to assist in monitoring the state of the risk management system over time and in setting priorities for improvement.
4. Testing and application of the Integrated Model and I-QRA.

Never before in the chemical/petrochemical industry has the technical risk control model been fully developed in parallel to the management risk control model. Previously, the two have evolved fairly independently, coming together only at certain points. The proposed new model will enable an evaluation of questions about the effects of organisation on risks, which previously may not have been addressed, such as 'what will be the effects of contracting out maintenance compared to keeping it in-house?'

Time varying risk profiles are now viable, giving the opportunity to model how variation in management, plant states etc. over time can affect risk. Questions can be posed such as whether prescriptive versus goal setting regulation have different 'decay rates'. The integrated model would generate key indicators of risk management health equivalent to corrosion monitoring of hardware. It would enable management to target risk control and mitigation measures most effectively to avoid accidents 'waiting to happen' and to respond appropriately in the event of the unforeseen.

THE RISK MODEL

Whereas the previous project linked management weighting factors at a high aggregation level to assessments of loss of containment risk, the current project aims to link management factors to the parameters that govern unavailability of safety related equipment and to the probabilities of human error and hardware failure which appear as initiating events or as failures at lower levels in fault trees. By developing the links between a broad overview of the organisational and management system and the initiating events that lead to accidents, the research will provide a system for directly examining the effect of the management system on risk levels. The I-Risk model consists of two sub-models (technical and management), and an interface between them.

Technical Sub-Model

As the research is concerned with major hazards, within the context of the Seveso Directive, it focuses on loss of containment (of hazardous material) events. These events are represented generically by Master Logic Diagrams, which share the basic features of qualitative fault tree analysis.

The technical model is thus used to identify the plant-specific initiating events that can lead to the release of a hazardous substance; the controls in place to prevent such a release (engineered systems, procedures and actions) and any factors that may mitigate such a release. The Master Logic Diagrams produce a set of hardware failures, hardware and system unavailabilities, initiating events and human errors/recoveries. These features are said to be governed by a set of mathematical parameters which include:

- Frequency of initiating events (both hardware and human errors);
- Time interval between tests;
- The frequency of routine maintenance.

Management Sub-Model

These parameters (or more correctly, the generic data for each of the parameters) are modified by plant-specific management influences which are considered to determine the quality of four main categories of activities:

- Design;
- Construction;
- Operations;
- Maintenance.

These plant-specific management influences are themselves determined by the quality of the systems which specify and deliver the resources and controls to these activities. In the I-Risk model, these are known as the delivery systems. Eight such delivery systems have been developed within this project:

- The availability of personnel with responsibility and authority to carry out the work;
- The competence of these personnel;
- Their commitment and motivation to carry out the work well and safely;
- The resolution of conflicting pressures and demands antagonistic to safety;
- The internal communication and co-ordination of people on the activities;
- The plans, procedures, rules and methods which specify the required level of safety or accepted way to carry out the work;
- The hardware, controls, plant interface etc. on which the activity is carried out;
- The delivery of correct spares for repairs and equipment.

These eight delivery systems are in turn influenced by the system which defines and modifies the safety management system.

The delivery systems have been modelled using a variation of the 'control and feedback learning loop' methodology developed within the previous EC project described above, and taking into account recent research by TU Delft (Hale et al. 6). This control and feedback loop model provides a conceptual basis for characterising a high performance safety management system. In this model, high performance stems from a focus on objectives which are faithfully translated into delivery systems within a closed loop, self-correcting framework. An example of the loop structure for one of the delivery systems is presented in Figure 1. The audit of management quality assesses all of the boxes in this figure and the loops that connect them. The research has identified which aspects of each delivery system are relevant for a particular parameter in the technical model (presented in Bellamy, 7). The delivery systems thus structure the audit and assessment of management influences.

The combination of these influences for each of the aspects to be assessed results in over 8000 potential assessment points for the audit, clearly more than can be addressed in a typical audit. Therefore, the influences are combined with respect to the common modes that exist in the particular company under examination.

The data points are assessed on a scale by the auditor with the help of anchor points at each pole of the scale; these points being textual descriptions of the characteristics of the management control and feedback loops.

The Technical-Management Interface

The interface effectively consists of a table of the parameters, a listing of base events and an audit preparation table. Pre-audit preparation partly consists of determining who (in the company) should be asked what questions and structured documentation enables the recording of information generated in the audit interviews.

Each of the technical parameters has a series of output components, which, when combined, link to the base events in the technical model. For example, the parameter Time to Repair (T_R) comprises of 17 output components grouped under the four headings:

- waiting time prior to repair;
- accessing and replacing time;
- time to do the repair;
- time for return to service.

The management influence is assessed for each of the output components for all of the parameters. The parameter in the technical model is then modified according to this influence. In this way, a plant specific technical model is linked to the plant specific management system by concentrating only on major hazard events and only on those aspects of the technical and management system which are relevant to such events.

MANAGEMENT 'CORROSION'

One of the objectives of the I-Risk project is to consider how the influence of management can lead to a sustained deterioration in safety over time, which if unchecked by regular review and revision processes will eventually lead to an accident. Such accidents generally provoke interventions aimed at restoring an acceptable level of safety, but ideally such intervention would come before, not after, an accident. For this purpose, it is necessary to develop means of identifying when an organisation has become 'an accident waiting to happen', or is heading in that direction.

In the previous project, a measure of the influence of the SMS on risk was achieved by mapping the relevant subsystems onto a conventional control and feedback loop model and developing an audit method for assessing the completeness and performance of the loop by considering each of the elements (comprising both the boxes and the links between them). Depending upon the strengths or the weaknesses of the elements, an overall 'management factor' was determined for the system in question. However, when applied to a plant, the approach does not explicitly distinguish between static and dynamic behaviour, between

what the current risk is (as influenced by management) and whether safety is set to improve or deteriorate in the foreseeable future. Providing a methodology for the determination of this future risk is an important aspect of the current research.

The dynamic aspects of the model thus relate to future states, given the current state. These future states are connected to the feedback, monitoring, analysis and revision side of the loop; and the first, second and third order learning loops (see Figure 1). The frequencies of these feedback, monitoring and analysis activities are known as Management Influence Monitors (MIMs) or corrosion monitors. These frequencies, combined with their relevance and quality, are the things which can have an effect on the technical parameters in the future.

PILOT TRIAL OF THE METHODOLOGY

The first test of the methodology was conducted by means of a desktop audit on a major hazard operation in which some of the project team had prior research and production experience. All relevant documentation for this operation was obtained from the company including aspects of the CIMAH Safety Report, procedures, piping and instrumentation diagrams, etc. The technical model adopted in this desktop audit (reported in Papazoglou and Aneziris, 8) expanded upon previous research conducted by the HSE on this operation (Anderson, 9).

Based on the knowledge and experience of the team, a typical SMS was constructed from the site information. In this simulated audit, members of the project team role-played the various site personnel to be interviewed, drawing upon predetermined pen-profiles for these roles.

This pilot study highlighted the strengths and weaknesses of the approach and following this desktop audit several major modifications were made to the methodology, particularly with reference to the complexity of the audit method, the pre-audit preparation phase, *support material for the auditors and the nature of the delivery systems.*

FIELD TRIAL OF THE METHODOLOGY

Following the pilot study detailed above, preparations were made to audit a section of plant in an oil refinery in the Netherlands. The Regulators were aware that in many respects this site was 'above average' - having a mature and comprehensive safety management system. As such, this site would prove to be an excellent test for the I-Risk methodology.

The technical model was subsequently developed and identified a total of 59 initiating and base events, 10 of which were deemed to relate to human error.

The preparation stage for the audit was comprehensive, requiring three man-days on site, and the assessment of common mode allowed the total number of data points to be assessed to be reduced from over 8000 to less than 500. In some instances, the company was found to have some redundancy in the SMS - where a number of feedback systems mapped onto

the same boxes in the model. This preparation also involved drawing up an interview plan and audit data points were assigned to particular individuals to be interviewed.

During the three-day audit, a total of 19 interviews were conducted with a range of personnel in the company hierarchy. These interviews, each involving two auditors, lasted from 15 minutes to 45 minutes depending upon the seniority of the interviewee. Also present in the interviews were three observers recording the process and content of the audit for later analysis.

LESSONS FROM THE FIELD TRIAL

The data from the field trial is still under analysis and it is not yet possible to describe the evaluations of the management influences or estimate their effect on the parameters in the technical model. However, at this stage it is possible to outline several lessons learnt and means of improving the model and the audit methodology:

- There are some aspects that need to be made more explicit, most importantly the emphasis on the fact that the method is specifically in relation to major hazards, within the context of the Seveso Directive. Such an emphasis on major hazards will need to be incorporated in all aspects of the method, including the delivery systems, assessment loops and audit attention points.

- The links (that is, the interface) between the parameters of the technical model and the delivery systems of the management model are considered to require some further consolidation.

- Preparatory work is essential to any successful audit. This preparation involves a visit to the site and discussions with key personnel. It is considered by the audit team that a more structured approach to this stage of the method would be highly advantageous and optimise the limited time available for the audit proper.

- Questions arose during the audit concerning the level of understanding of technical information required by the auditors (for example, relating to specific major hazard scenarios) in order to perform an audit of a management system. This clearly has implications for the level of detail to which the management system is defined and subsequently assessed.

- During the audit it became clear that more common mode existed in the company SMS than originally envisaged, further reducing the amount of audit points to be assessed from 500 to in the region of 120. The method of identifying common mode in the company SMS requires further development, particularly to ensure that it is transparent.

- The audit would have been greatly assisted by an improved matrix of interviewees for each activity within each delivery system, including details of attention points for each interviewee. In addition, these attention points should be prioritised.

- *The link between the audit attention points and the interface between the technical and* management models needs to be made more explicit.

- Supporting documentation for the auditors should ideally include the facility to record what activity boxes have been assessed and to what extent.

- The importance of time for auditors to consolidate between interviews is stressed, especially if future audits may utilise audit teams working in parallel.

A further field test is planned for later in the year, although it is considered that only fine-tuning will be required at this stage following detailed consideration of the modifications prompted by the above trials. Following the incorporation of lessons learnt in this next field trial, an audit manual will be produced detailing the method and its philosophy.

CONCLUSIONS

The recent field trial of the I-Risk methodology has proved to be an extremely useful exercise. One of the main strengths of the method is that it is based around a collection of concepts (such as the delivery systems, assessment loops and attention points) that are easily grasped by the auditing team and that the links between these components is made explicit. Problems identified with the model and audit in the early desktop exercise have been largely overcome. However, the audit can be greatly improved by attention to the audit strategy and the supporting documentation. This work may include prioritisation of the attention points and their allocation to a specific interviewee in the preparatory phase.

This research project has produced a model and methodology that integrates management and technical factors in QRA in a more highly sensitive manner than has ever been accomplished before. It is intended that the products of I-Risk will enable both *industry and Regulators in the participating countries to systematically assess the quality of* a safety management system in a site-specific manner and examine its effect on the current and future risk levels, as assessed by the technical modelling. Through explicitly linking the influence of management and organisational factors to the assessment of risk, the methodology will enable improvements to be made to existing systems in a more cost- and safety-effective manner. The audit method has also proved to be a powerful tool in enabling a systematic and critical qualitative examination of an organisation's safety management system.

ACKNOWLEDGEMENTS

This paper reports on the developments and progress of an EC research project involving significant contributions from several organisations. The author acknowledges the work of these participants to the material in this paper. These contributors and their respective organisations are as follows:

- Project Co-ordinator: Joy Oh, Ministry of SZW, Netherlands
- Dr Linda Bellamy, Ingenieurs/adviesbureau SAVE, Netherlands;
- Prof. Andrew Hale, Frank Guldenmund, TU Delft Safety Science Group, Netherlands;
- Helen Shannon, Mark Morris, Helen Walker, Four Elements Limited, London;
- Ben Ale, Jos Post, RIVM, Netherlands;
- Iannis Papazoglou, Olga Aneziris, NCSR Demokritos, Greece;
- Williet Brouwer; Ministry of SZW, Netherlands;
- Andre Muyselaar, Ministry of VROM, Netherlands.

The research work described in this paper is being carried out under the CEC Environment programme 1995-1998 and the author is pleased to acknowledge the support of the following organisations in funding this work:

- European Commission, DGXII;
- Ministry of SZW (Social Affairs and Employment), Netherlands;
- UK Health and Safety Executive.

This paper is dedicated to the late Dr Nick Hurst of the Health and Safety Laboratory who, through his ideas, experience and enthusiasm pushed forward the boundaries of research in this field during a distinguished career in the HSE.

REFERENCES

1. Hurst, N. W., Nussey, C. and Pape, R. P. (1989). Development and application of a risk assessment tool (RISKAT) in the Health and Safety Executive. Chem. Eng. Res. Des., 67, 362-372.
2. Hurst, N. W. (1998). Risk assessment: The human dimension. Royal Society of Chemistry, Letchworth, Herts. ISBN 0 85404 554 6.
3. Hurst, N. W., Bellamy, L. J., Geyer, T. A. W. and Astley, J. A. (1991). A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies. J. Haz. Mat. 26: 159-186.
4. HSE (1997). Successful health and safety management. HS(G)65. HSE Books, Sudbury, Suffolk. ISBN 0 7176 0412 8.
5. Hurst, N. W., Young, S., Donald, I., Gibson, H. and Muyselaar, A. (1996). Measures of safety management performance and attitudes to safety at major hazard sites. J. of Loss Prev. Process Ind. 9(2): 161-172.
6. Hale, A. R., Heming, B. H. J., Carthy, J. and Kirwan, B. (1997b). Modelling of safety management. Safety Science. 26: 121-140.
7. Bellamy, L. (1998a). Technical model parameters management systems. Document prepared for CEC I-Risk. SAVE. Apeldoorn, March 1998.
8. Papazoglou, I. A. and Aneziris, O. N. (1997). A technical model for QRA of the chlorine loading to road tankers. Document prepared for CEC I-Risk. NCSR Demokritos, October 1997.
9. Anderson, M. (1997). The development of site-specific failure rates for use in risk assessments of major hazard sites: A case study of road tanker loading operations. MSc Dissertation: University of Sheffield, August 1997.

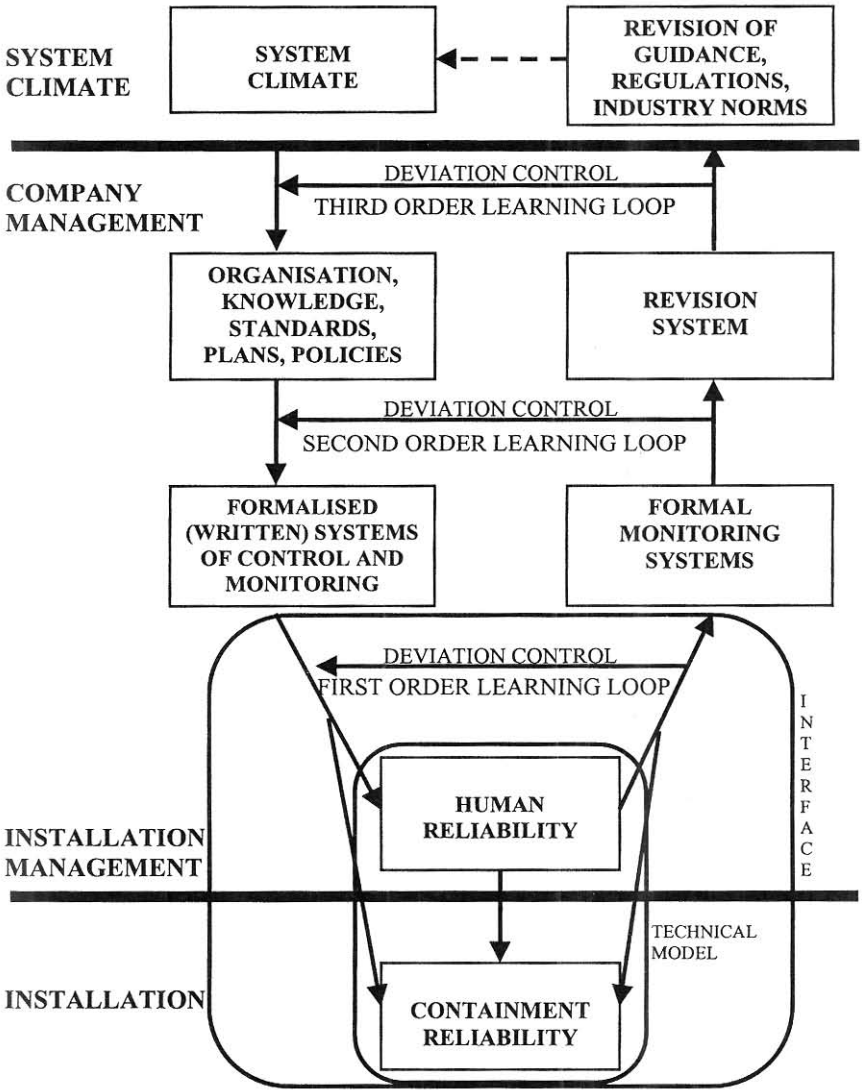

Figure 1: The I-Risk Model. (Simplified) This model describes the development of specific outputs of the safety management system and their modification based on experience with those outputs. The 'loop' runs from the development of a policy, its elaboration into detail, through its implementation and feedback of experiences.