

IS HAZARD MANAGEMENT WORKING?

Graham Dalzell[1] and Andrew Hopkins[2]
[1]TBS Cubed Ltd
[2]Australian National University

This paper questions whether conventional safety management systems and safety cases deliver effective management of major accident hazards and their risks. It proposes 9 criteria by which to judge an organisation and its risk management. Thereafter, it uses them to give an opinion on the question based upon the authors experience.

INTRODUCTION

Both authors have been deeply involved in safety and risk management for many years. They have very different backgrounds; one is a sociologist and academic who has examined the underlying causes of a number of major accidents (Refs 1,2). The other is a practicing engineer who has worked within a major hazard industry, trying to put in place processes and management systems to understand hazards and prevent accidents. This paper raises the question: "Is hazard management working?" It is specifically directed at major accidents which are inherently complex, highly variable, and specific to each site and company. The management of the risks from major accident hazards is a particularly difficult subject and this paper addresses some of the barriers to putting effective processes into practice.

The paper questions the effectiveness of hazard management. It does so by examining the management of three things;

- **critical elements**; i.e. the pieces which are needed to manage the causes and consequences of hazards
- **hazards**; i.e. the provision of an adequate combination of critical elements to match the causes and, where judged necessary, the consequences
- **risk**; i.e. judgement of the tolerability of risks from the hazards and the investment in risk reduction

It is important to bear the use of these words in mind when reading the paper.

THE APPLICATION OF HAZARD AND RISK MANAGEMENT AT DIFFERENT LEVELS OF AN ORGANISATION

In order to answer the question, we must first provide a definition of risk and hazard management, or at least, provide a list of its essential elements and attributes. It is worth referring to other work (Refs 2,3,4) which examined management structures and the causes of accidents in a hierarchical form. These references considered four levels within business

and a fifth which is the society within which the businesses operate. This paper sets out to examine how each of the four levels within a commercial organisation meets the attributes listed below. It does not examine how society as a whole performs. At this level, the desires of society should be reflected by the laws of the country and their implementation by the regulator. Each of the other four levels has a different role in managing hazards and risks.

1. **Level 1 – Individual level:** These are the physical activities required to operate the plant, the undertaking of specific tasks, the maintenance and the testing of critical items of plant; e.g. a particular valve, the inspection of a vessel or a deliberate breach of containment. This is neither hazard nor risk management but the ownership of individual items. Very little real judgement is needed by the individuals as the requirements from the activities should be clearly defined. Where such judgement is required, it is usually referred up to the next level. **This is the management of critical elements.**
2. **Level 2 – Facility level:** This is the daily management of the facility. It may be a specific process unit, a pipeline, offshore platform or a depot. It is the management of the inherent processing hazards combined with the variations caused by the overall plant condition, the status of safety systems, the activities, occupancy and the weather. This is the point where all of the pieces of the jigsaw are examined in the light of the specific hazards to ensure that there are sufficient critical measures in place to manage the causes and consequences. **This may be considered as the management of hazards on a facility.**
3. **Level 3 – Managerial level:** This is the management of all of the facilities on a site, in an offshore operation or in a distributed business. It is the strategic judgement of the tolerability of risks for each of the facilities, including the adequacy of the design, the provision of safety systems, the skills of the people, the manning of the plant and the provision of an adequate supporting infrastructure. It considers the level, pattern and proportion of risk by hazard and by facility. **This is the management of the risks within a business unit.**
4. **Level 4 – Corporate level:** This is the management of the whole company. It is the balance of risk and return, the judgement of tolerable risk and the shaping of that risk within existing operations and its future direction by growth or divestment. **This is the management of corporate risk.**

ESSENTIAL ATTRIBUTES OF HAZARD AND RISK MANAGEMENT

The words risk, hazard and critical element are used throughout this paper in the context of these four levels. Within the context of this structure, the following attributes are regarded by the authors as essential for hazard and risk management.

– **Line responsibility:** As with occupational safety, the management of major hazards and their associated risks is a line responsibility. It is not the consultant or the corporate safety engineer that decides if the risks on a plant are tolerable. They may provide

advice but individuals at each level make decisions that determine the risks on the plant. At the bottom level, it may be the adequacy of an item of plant under test or the specific safeguards put in place to cover an activity. At the facility level, it is the decision to operate the plant or carry out a work programme in the knowledge of the specific conditions at the time. At the managerial level, it is the determination of the overall adequacy of the plant design, engineered safeguards and manning. They should be working within the context of tolerable risk levels which would be set and managed at the corporate level.

– **Risk and hazard understanding:** How can we manage if we don't understand? Each of the individuals with responsibility needs sufficient knowledge to make informed decisions. The technician should know the role of a particular valve in controlling a hazard. The plant supervisors need to understand each of the hazards on their site, the causes, the effects and the consequences together with all of the elements needed to prevent or limit the severity. At the managerial level, it is the pattern of risk by facility and by hazard together with the specific dependence upon parts of the business infrastructure to provide effective support. At the corporate level, it is the overall level of risk within the organisation, the underlying risk drivers and the future trends in those risks.

  A second aspect of hazard and risk understanding is continuity and transparency. The particular risk and hazard knowledge which is needed at each level of an organisation is different but there should be a common thread running through it. It starts at level 2 with the identification and understanding of hazards. This information is progressively distilled into the facility and corporate risk patterns for use at levels 3 and 4. The specific requirements for critical elements are defined for level 1 based on the needs of the hazard. This is described in greater detail in (Ref 7). If particular hazards or facilities are identified as primary risks, this should be reflected in the specific limits placed in these areas and on the criticality of the critical elements needed to manage them. The individuals must be focusing upon those areas that the managers consider to be the most important and vice versa.

– **Corporate unease:** This is a concept introduced within high reliability organisations (Ref 5 and 6). It is characterised by an approach to management that asks the question "Why is it dangerous?" rather than "Is it safe?" It is the attitude of an organisation that recognises that the potential for harm will always exist by the nature of its businesss whatever measures are taken to control it. Such an organisation does not think that hazards have gone away simply because there is a process for clearing all of the recommendations from an audit programme. It is perpetually aware of the potential for major accidents and the ever present possibility for failure of the barriers to their occurrence.

– **The identification of critical elements and the existence of minimum standards:** There is some overlap with the next topic of limits but in this context, critical elements include everything that is needed to manage the hazards on the site effectively. Thereafter, setting standards includes the clear definition of the role of those critical elements in respect of the hazard and the specification or retrospective verification

that it is suitable and sufficient for that role. This will involve measurable criteria which relate to its fulfilment of the role. At the facility level, the critical elements are the people, tasks and plant needed for each hazard. At higher levels, the setting of minimum standards includes the clear definition of the role and service needed from the management systems and infrastructure supporting operations and design.

- **The definition and application of clear operating limits:** An organisation which sets and applies limits consciously knows the boundaries of safe operation and works within a safety factor. It recognises that not only plant but people have limits too. These boundaries should be defined within the performance standards discussed above. At the bottom level, it would be the minimum standard of competence or the performance and availability of a critical item of equipment. However, as we rise up though the organisation, they become more nebulous and less easy to define precisely. At the facility level, the performance limits of the plant are easy to define in terms of throughput but less precise when considering the minimum manning, the maximum level of activity or occupancy and the point at which the combined deficiency of apparently unrelated critical systems, including people, becomes intolerable. At higher levels, it is not the just the plant which may be pushed beyond its limits but the organisation as a whole. An organisation which recognises its limits should be characterised by a management system which sets production targets for different facilities in the knowledge of the variation in the inherent risks. It should consider the relationship and the maximum pressure it applies to its suppliers, particularly where their service is critical. At the top level, the limit is the maximum amount of risk that the company is prepared to tolerate. In theory this may be an overall FN curve but in practice, it involves much more qualitative judgements and the interpretation of social norms and pressures.

  Having set limits, an individual, facility manager and business manager must apply them. They must recognise that a limit as been reached and say stop. The organisation must not only give them that right but expect them to do so. This may range from the limitation of hazardous operations when a critical item is deficient through the temporary shutdown of a facility, its permanent closure or the withdrawal from a particularly hazardous business, product range or territory.
- **The definition of the minimum infrastructure needed to manage the hazards:** A key input to defining the infrastructure is the examination of the load placed upon the organisation both at a business and corporate level by all of the processes such as integrity management or competence assurance. It takes into account the overall demands of all of the hazards and the criticality of these processes in the recognition of the underlying risk drivers. Typically this infrastructure covers the support for people and plant, such as the size, composition and quality of the engineering and training departments.
- **Balance and focus:** A key aspect of management in whatever form is the balancing of conflicting demands. Within risk management, this requires the balancing of prevention vs. cure; occupational vs. major hazards; plant vs. people and the demands from different hazards. A focused organisation does not overly respond to the zeal of

individuals with their specific issue or solution, nor does it give a knee jerk reaction to a particular accident or failure. It takes a measured and balanced approach to the investment in risk management in the light of the risk patterns and demands arising from the facility risk assessments. It also recognises the real contribution of apparently unquantifiable factors such as competence, experience and organisational stability.

- **Management the totality, not just the elements:** Effective management requires integration of departments and business processes to implement a common strategy to manage hazards and risks. Our politicians use the term "joined up government". Neither plant nor people can prevent or control hazards on their own. Every hazard has a series of causes and routes by which it can escalate. They have a multitude of interdependent barriers which will only be effective if all of the parts work together. Effective management identifies these dependencies and shows everything that is needed for each hazard. It allows the facility manager to see the whole jigsaw of critical elements. It requires the business manager to see how each business process such as design, procurement or contract management contributes to, and interacts in the management of the risks.
- **Continuous proactive processes:** Managing hazards and risks effectively in akin to driving a car safely. Both require continuous monitoring of the hazards, the state of the plant, the operators, the external conditions and any other factors which might affect the specific risk at the time. It requires both formalised assessments and a continuous monitoring of the hazards leading to a whole series of risk based decisions. These determine how close the operation is run to the limit. Safe drivers are not necessarily the slow ones or those with the latest safety systems. They are those who are continuously alert and aware of the hazards such that they drive within their limits and those of their vehicles. They moderate their speed or apply the brakes as soon as the conditions change rather than waiting for a periodic formalised assessment. They gather and act upon knowledge before a situation becomes critical rather than waiting for an accident to happen and relying upon the emergency systems. They are proactive not reactive.

EXAMINING THE QUESTION "IS HAZARD MANAGEMENT WORKING"

In order to examine the question fully, each of the nine aspects listed above may be examined at each of the four levels of the organisation.

Line responsibility

There is no doubt senior managers would agree that they have direct responsibility for the hazards and risks on the facilities under their control. Many show leadership by site visits and highlighting the importance of "safety" but do they really manage the totality? If there is an accident, do they assume that responsibility or search the lower echelons for the individual responsible for the failure of the particular element which caused it? If we examine critical items at the lowest level, those who are responsible are usually clearly identified

and have prescribed basic competences and formal specific training. They are therefore fully able to take on their responsibilities. At the levels above with responsibility for hazard and risk, the identification of those with line responsibility is much more difficult and is rarely formally documented. The only cases where such documentation has been found are those where the law requires a safety case to be signed off by the facility or business manager. In cases where there is no legislative requirement it has been virtually impossible to persuade these managers to sign a formal acceptance of a hazard register or facility risk assessment. They will take responsibility for closing out recommendations but will not formally accept the residual risk that remains and by default their responsibilities that go with it. Hazard and risk management involves gathering and assessing diverse information, developing a picture of risk and hazards in their mind and making judgements which require interpretation of corporate risk criteria for their particular activities. However, there does not appear to be any recognised training or qualifications in this area for line mangers. Indeed, there does not appear to be any recognition that this is a skill that is essential for anyone with this line responsibility. Instead, the analysis and decision making has been subcontracted to specialists, either within a large corporate organisation or more commonly to a specialised consultancy. These specialists are rarely an integral part of the operations or design team. They visit, do their work and depart. This means that the vast majority of day to day critical decisions are taken without their input. There seems to be a presumption that competence in risk management appears as if by magic with promotion to a senior position. This is not to say that there is no evidence of this competence. It does exist but it has been hard won and is demonstrated by individuals with years of operations experience combined with the right mind set. Unfortunately, the criterion by which they judge the tolerability of risk is usually their own, driven by their personal perception of risk and the margin of safety in their operations on the day. It is questionable whether this has any relation to corporate risk criteria and it would be interesting to witness the discussions whenever their judgement to shut down a plant is questioned at higher level. As we rise through the company to levels 3 and 4 where the risks are managed strategically, it becomes an even more judgemental and skilled process. People at this level should be skilled in managing business risks and conscious of all of the factors above when it comes to financial or production losses. However they don't seem to use the same thinking process and logic when addressing the risks of an accident, even though the financial and reputation losses can be potentially catastrophic.

Risk and hazard understanding

This is appearing to fall down at all four levels. At level 1, there seems to be a presumption that every individual looking after a critical item will know why it is important or will be able to picture what might happen if the task goes wrong. With occupational hazards, this is a reasonable presumption; a poorly erected scaffold will result in crush injuries and possible death. However, with major hazards in which so many pieces of the jigsaw interact, the importance may be recognised but the exact role may not. For example, if we ask a technician working on an instrument what the fire will look like if the 3/4 inch tapping

fails, they will only be able to guess as to the size, intensity, duration and potential for escalation. The facility supervisor may be similarly uncertain. A well informed facility manager should be able to tour the site talking knowledgeably about each of the major hazards; the causes, characteristics and consequences. Although such knowledge can be found, it is not common and it is only seen where there has been a deliberate attempt to extract and communicate this information from safety cases. It is more common to be given their perception of the hazards and characteristics. This is valid and valuable information but it is unlikely to be complete and balanced, at least in those cases where specialised analysis is required to predict the effects and potential escalation. However, they are often the most knowledgeable about the causes and likelihood. At the business and corporate levels, again those responsible appear to have piecemeal knowledge about elements which contribute to the risks, often arising from audits. It is more common to encounter a full understanding of the pattern of occupational risks arising from injuries and LTIs but this almost totally hides the real risk picture by excluding those highly infrequent incidents that do not appear in periodic statistics. The reasons behind this lack of understanding are two fold; those in the senior positions are not seeking this information and those undertaking the risk assessments are not providing it in a form that is immediately usable. Risk and hazard understanding is rarely a corporate requirement. It is more usually; compliance with the law, meeting specific standards for individual elements, driving down occupational risk and satisfying audit requirements.

Corporate unease

It would be wrong to say that most major organisations are complacent. They do worry about injuries and indulge in prolonged corporate soul searching, particularly after multiple fatalities (Ref 8 and 9). One of the symptoms of this concern is the almost constant change in corporate standards and processes. Another is the plethora of initiatives that appear with the emphasis being driven cyclically by the specific causes of major accidents or by occupational risk trends. The unease would appear to be greatest at the lowest level where there is direct exposure to the plant. People and at the next level such as the facility managers or discipline engineers are also acutely aware of tightening resources and the implications such as the loss of supporting infrastructure. There is also growing unease at a corporate level with the recognition that complete financial collapse can arise from a major accident. The intermediate levels would appear to be more comfortable and their level of unease is dependent upon the signals they receive both from above and below. It may also be a function of their perception of their personal exposure and culpability. Perhaps of more concern is not the state of unease but the way in which it is expressed and placated. There appears to be an ongoing search for faults through audit programmes and the number of concerns and outstanding recommendations is overwhelming many business units. There may need to be a change from a search for solutions to an open acknowledgment of risks and underlying risk drivers. Unfocussed corporate unease may be of less value than open acknowledgement of risk and its management. Real unease would then result in the active implementation of limits.

Minimum standards

This is the requirement to identify what is needed to manage the hazards and risks at each level of the organisation. It appears to be deficient at every level of the organisation. The development of supporting legislation for the offshore safety cases (Refs 10 and 11) required that the prevention, detection, control and mitigation systems should be identified and that performance standards should be set for them. It proved to be a difficult, if not impossible task to interrogate the original risk assessments for the safety case in order to deliver this information (Ref 12). In many cases, only generic roles were given and the measurable standards such as reliability, flow rate or sensitivity were default rather than being based on the risk or characteristics of the hazards which they were intended to control. The requirement for minimum standards for people; i.e. competence were not specifically enshrined in legislation and received even more generic and imprecise treatment. At higher levels in the organisation, it is not the critical elements which require identification and minimum standards but the business processes which support their management. There is no real evidence that risk assessment has been used at all to define what is needed and the role which it should perform. This is dealt with in more detail under infrastructure.

Setting limits and saying no

There is clear evidence that individuals are saying no. Multinational companies are divesting assets which are judged, by formal risk analysis or by audit to offer too great a corporate risk for the returns that they offer. There is increasing awareness of the catastrophic effects on business which can be realised from an operation which has inherently high risk or is in poor condition, particularly where the effects upon the public would be devastating. They are increasingly aware of the Bhopal scenario (Ref 13) and of the power of the media. At the lowest, individual level, there is also evidence of facilities being shut down because of a specific weakness in the plant or the failure of a critical protective system such as a firepump. However these cases do appear to have arisen on an individual case by case basis rather than as a general requirement in the organisation. Again it is at the top and bottom levels where there is more evidence of saying no. At the middle levels, there appears to be a much more general tendency to ask – "What do we need to do to keep going. . . . , or can we get by without. . ..?" At the managerial levels there seems to be a reluctance or inability to set precise limits and to say no. Instead the opposite is appearing – the setting of stretch targets for production and return, and the encouragement always to say "yes".

Minimum infrastructure

Ideally, a fully comprehensive analysis of the causes and consequences of hazards should not only identify critical plant, processes and people, but their criticality, the departments and individuals responsible for them. A systematic analysis of these demands upon the infrastructure should show the overall loading on the individuals and management systems. Although this would appear to be a relatively simple task, in practice it needs

considerable resource for a thorough analysis and it is simply not done. There has been no evidence of studies which attempt to map demands against the various management systems. The result is that there is no systematic definition of the minimum infrastructure needed to support effective hazard and risk management. In cases where it has been attempted, it has been based upon the managers perception of what is important rather than what the risk processes could define. The primary concern resulting from this lack of definition is that reorganisation or streamlining of the business can undermine this infrastructure by eroding critical skills and the resources needed to support those with line responsibility; i.e. there is no basis for assessing the effects of organisational change.

Balance and focus

There is a finite resource available to reduce risks. Effective allocation of this resource will result in the smallest and most infrequent bang for your buck. While a rigorous risk assessment process should encourage focus and balance, in practice it appears to do the opposite. This may be attributed to the culture which has expected these assessments only to make recommendations; either to repair what has been judged to be deficient against default criteria or to seek quantifiable improvements in the search for the demonstration of ALARP. As the softer, human side of risk cannot easily be quantified, risk reduction tends to focus on hardware and protection. It also tends to add more safety systems rather than incrementally improving the integrity of the existing plant, as again that cannot easily be quantified. Another source of imbalance is the compartmentalisation of organisations; the silo culture (Ref 1). The relative investment in each area will be a function of its ability to seek funding, to "defend its patch" or conversely its ability to demonstrate that all is well in the face of auditing. This imbalance has been particularly apparent in cases where major deficiencies have been identified. Multimillion pound projects have been commissioned to re-establish a basic level of plant integrity and to add state of the art protection systems but the investment in people has by comparison been minimal. Another source of imbalance is the zeal of the individual specialist. A case in point has been the myopic concentration on explosion overpressures on offshore installations. The development of models and the prediction of overpressures and structural response has become almost an obsession. Examining the results of offshore risk analyses and the changes as modelling capability has "improved" shows progressively increasing overpressures, effects and risks. It may be argued that this has distorted the real risk picture (Ref 14). If the historical risks were as high are they are predicted using current models, there would have been much more evidence of smaller explosions offshore, based on the argument that for every large incident there are 10 medium and 100 smaller one. The reaction to this highlighted risk has primarily been the optimisation of the structures to withstand the effects. Again this demonstrates a lack of focus as escalation though process failure is more likely and arguably more serious. More importantly, the predictions of catastrophic overpressure can only result from a very large gas cloud which requires a combination of larger holes and still air conditions. Rather than examine the structural strength to withstand these blasts, surely it would have been better to identify the sources of large failures

with a view to ensuring that they do not occur, particularly during the benign weather conditions.

Managing the totality

There is some evidence of integrated hazard management with examples of hazard registers which list the primary systems required to control and mitigate hazards. However, this does not appear to be uniform practice either across all operations and regions within multinational companies or within one country covered by particular legislation. These registers identify the parts of the jigsaw but don't ensure that all of the pieces are in place and that they all fit together. Take several examples: HAZOPs should be a complete causation analysis but how often do they only focus on hardware and fail to rigorously analyse operating procedures and practices. These tend to be assessed using other methods which often do not take into account of the frequency with which the task will be performed or a real understanding of the consequences. As a second example, when managing the effects of fire hazards, it is more common to see an unrelated "kit of parts" such as detection, depressurisation, protection and emergency response rather than an integrated strategy. Such a strategy would use the hazard analysis firstly to determine the design events and then use the control systems, ESD and depressurisation to actively limit the severity so that it matches the extent and capability of the protection systems. In practice, this fully integrated strategy is most uncommon. The documented performance standards for these systems reinforce the view that there is no strategy. The high level standard should clearly state what the system is intended to do with respect to a particular hazard; e.g. the deluge may be required to suppress external flaming from a large oil fire in a roofed module. Instead, there is more likely to be a generic statement such as to prevent escalation. Perhaps the greatest indication of the lack of integrated management is the plethora of unrelated ways of categorising the criticality of critical systems. Within those managing one particular hazard, there may be as many as 10 different rating types. For example corrosion management may use a 9 by 9 risk matrix (Ref 15), activities may be controlled by task risk assessments using another unrelated 3 by 4 matrix and the control systems will have an integrity level set according to ISO 61508 (Ref 16). Another indication of an absence of integrated management is the lack of clear rules for managing risks or limiting operations when a critical system fails to meet its performance. There may be a specific limit when, for example a fire pump is down for maintenance but a different set of rules may be applied if a corrosion allowance is used up or an ESD is slow to close. It will generally be the engineer with responsibility for the particular system that set these limits, not the person with overall responsibility for the hazard. It may be argued that the use of bow tie diagrams does aim for integration but it is doubtful if they really meet the aims listed in this paper.

Continuous proactivity

A well run organisation will have ongoing monitoring of all critical plant and will control all hazardous activities. It will react to individual deficiencies by applying specific limits or refraining from a particular activity. It may be said that such organisations proactively

manage critical elements. It is difficult to say that the same approach applies at higher management levels, i.e. those looking after hazards and risks. If there was to be real evidence of proactivity, the hazard and risks would be a key input to the planning process; for activities, maintenance programmes, and resourcing the organisation. Instead it appears to be reactive; plans and strategies are developed and then "safety" is examined in the light of the decisions. The reactive application of management of change to a corporate reorganisation is a case in point. Instead of asking what resources are needed to manage the risks in this plant or organisation, the impact of the loss of an individual is assessed. If the process is to be continuous, there must be constant awareness of how risks are changing; for example through the numbers of people on the facility, its age and condition, the weather or the pressures to meet corporate production and cost targets. There is no real evidence to show that the risk or hazard picture is constantly updated. The information does not appear to be either requested or offered. Instead, there is more likely to be monitoring of audit recommendations and the tracking of key issues on a Boston square. These issues may be months if not years old but a bigger question must be asked – does their ranking really reflect their contribution to the risk picture or is it based upon the perception of the people who championed the issue? In almost all organisations, the process is reactive and discontinuous. To return to the driving analogy, there is not constant assessment of the conditions, limitation of the speed and application of the brakes.

SUMMARY

This appears to be a fairly damning picture both of industry and of the response to the goal setting regulatory environment. It is not and is not intended to be so. Diligent companies are trying hard to maintain and improve the building blocks upon which effective hazard and risk management are based. These building blocks are well inspected and maintained plant, competent people and a comprehensive well resourced set of business processes. Without these, it is pointless to attempt hazard and risk management. The goal setting regulatory regime has also delivered real reductions in risk. Without it we would probably not be holding this 19th sell out major hazard conference. However, these risks reductions have been focussed on adding safety systems and investing upon in those areas where the benefits are numerically quantifiable. This paper is about moving to the next level; distilling the knowledge from the safety cases and risk assessments to optimise what we do; to deliver the lowest possible risks for the investment and resources that we choose to assign. It is moving from managing the basics into those areas which are less quantifiable but can deliver further significant risk reductions.

Responsible operators appear to be successfully managing the critical elements; the tasks and plant which, by their failure, might cause or exacerbate a major accident. They are also managing safety studies, risk assessments and the recommendations arising therefrom. However, the attributes for effective hazard and risk management listed above have not been widely observed. Why is this, and what might be done to move industry to this next level of excellence?

RECOMMENDATIONS

SIMPLIFYING THE COMPLEXITY AND REGAINING OWNERSHIP OF THE RISKS

We have all made the analysis of major accident risks such a complex subject that most operators feel it necessary to employ specialists to carry out the work. They not only carry out the analysis but the assessments as well and in effect, they make the decisions. They decide if risks are tolerable, the levels of investment to achieve ALARP and the areas that should receive this investment. In some cases, these specialists are employees but in most, they are external risk consultants. Their complexity is such that the limited number of staff personnel could not possibly deal with the day to day questions that would arise in a proactive system. It is a refection of the external dependence that a reasonable practical query from the regulators immediately results in a call for support and often a complete rerunning of a QRA. It is highly debatable whether the current levels of complexity are necessary, particularly the need for, and dependence upon the statistical analysis within QRA. Its failure to present its knowledge and the reasons behind its results have hindered rather than facilitated day to day risk management. It is also often seen as the only decision making tool. It is appropriate for levels 3 and 4 of an organisation but not for managing the detail of specific hazards or critical elements where it is increasingly being used. Before embarking on either a safety case or a QRA, a better start point would be the identification of the people with line management responsibility for hazards and risks as described above. Next, consider the decisions that they have to make on daily activities, planning or strategy and the information that they need to make those decisions (Refs 3 and 4). Now consider the best method of hazard and risk analysis (note not assessment) that can deliver that information and agree the form that it should take. This should put those responsible in a position to take on those responsibilities. They make the assessment, make the decisions and carry the can. The UKOOA decision making framework (Ref 17) gives appropriate tools which engineers and managers can use to make those decisions. If they cannot access distilled information, how can they understand and if not, then they cannot manage.

COMPETENCY AND RESPONSIBILITY

Even with some reduction in unnecessary complexity, managing risks and hazards as described above requires considerable skills both in understanding all of the competing factors and in making judgements. This should be recognised by the establishment of minimum standards of competence for anyone with line responsibility for hazard and risks. These competency requirements will broaden as individuals are promoted and their responsibilities increase. In parallel with these mandatory skills, there should be clear assignment of responsibility. Currently it is well documented for critical elements but not for hazards or risks. If a permit to work is the authorisation for a task, could there be an equivalent for hazard; a daily or weekly permit to operate? Rather than addressing the risks and safeguards for an individual action, this would examine the overall condition of the facility, any deficiencies and exacerbating conditions such as bad weather, the

activities and overall personnel exposure. This permit would be a clear statement that, in the view of the facility manager, it is safe to operate, man the facility and carry out the activities planned for that period. Developing an equivalent at the managerial level is a little more difficult and vague. The current equivalent is signing off the safety case, where there is one. In theory this is a strategic permit to operate and acceptance of responsibility for the risks by the business manager but it only occurs every three to five years, yet the managers may change out every two. It would be much more effective if the safety case included more transparent documentation of the risks, their distribution, underlying drivers and of the processes and infrastructure to manage them effectively. It must also state clear overall limits which, if exceeded will result in unacceptable risk. While QRA might form the basis for deriving the risk, it is an unacceptable means of expressing those limits. They need to be translated into tangible criteria such as throughput, overall plant integrity, availability of critical measures, minimum infrastructure and above all, the availability and workload of competent people. The safety case resubmission interval of three - five years is clearly too long and an internal strategic three - six monthly acceptance of the risks which takes into account planned activities and a status review of the plant and people would be more realistic. It would be even more difficult to elevate this formal acceptance of risk to the corporate level but this does not mean that it should not be attempted.

MANAGING RISKS NOT RECOMMENDATIONS AND STATISTICS

This requires a cultural shift from retrospective compliance of prescriptive corporate or industry standards into the proactive understanding and management of risk. It is the move from asking; “is it safe?” to asking “why is it dangerous?” It is the transition from corporate ease to corporate unease. One of the characteristics of a recommendations culture is the way that senior management tracks this process. If it is simply studying the numbers of outstanding issues or deficiencies rather than the content or the underlying reason, then it is not managing either risks or hazards. Similarly if it is fixated with LTIs and days away from work, it focuses upon the lowest level – the task and also gives disproportionate emphasis to occupational risk. If risks are to be managed on a continuous basis, senior managers must not focus upon the minutiae of individual tasks and items but should concentrate upon the wider risk picture. They must realise that it is continuously variable and have means in place to continuously monitor it. Their response must be continuous and appropriate i.e. running the plants within limits that reflect the inherent risks, their condition and the capabilities of the people and supporting organisation. This means; knowing the limits, setting an appropriate safety margin, applying the brakes, and providing resources.

CHANGING A SAFETY MANAGEMENT SYSTEM INTO RISK MANAGEMENT SYSTEM

There is a widespread misconception that conventional safety or integrity management systems are effective risk management systems. There is also another common presumption

that the safety case is, in itself, a risk management system. In the case of the safety or integrity management systems, most companies have between eight and sixteen key elements. Risk or hazard assessment is either the first element, or the second if superseded by leadership and accountability. Some make reference to risk or hazard management but most only use the terms analysis or assessment. In cases where the word management is used, the supporting documents do not explain what it means, at least not in the terms outlined in this paper. Most systems are not explicit about the type and standard of risk or hazard assessment that it required. The interpretations range from the requirement to carry out specific assessments such as a task risk assessment or HAZOP or a broader quantitative assessment of a whole facility. Above all, they do not provide the holistic information needed to manage hazard or risks, despite this being the supposed intent of QRA. It could but it doesn't and is not used in this way.

The remaining elements of a classical SMS list topics such as safety critical systems, procedures, management of change, competence, emergency response, lessons learned etc., much along the lines of the American Process Safety Management systems (Ref 18). There is rarely any requirement to link these latter elements back to the initial risk assessment outputs or for them to determine their performance. In most cases, they simply meet default standards set by the owner of that particular element, usually based upon industry codes. The individual elements may have their own particular form of hazard analysis and may to some extent be risk based but they almost never refer back to a wider risk analysis for the whole facility. The stand alone nature of the way safety integrity levels for instrumented safety systems are set is a case in point (Ref 16).

These Safety or Integrity Management Systems and Safety Cases are also notably deficient in defining the requirements of the overall infrastructure and the resourcing of an organisation to match the risks. The management of change process might refer to it but there is no link to a risk analysis process to determine what is needed.

A good Safety or Integrity Management System provides the building blocks upon which effective risk management is based. However, a radical overhaul of the risk assessment element is required. It must be holistic, in that it either defines or confirms the adequacy of each of the subsequent elements as part of a comprehensive, integrated and effective set of elements to manage the hazards and risks. Above all, it must change from simply requiring an assessment to delivering real usable risk and hazard knowledge with a specific requirement that risks are effectively and continuously managed. It must also explain exactly what that means at every level of an organisation.

CONCLUSIONS

Much has been achieved over the last 20 years in improving the elements which are required to manage hazard and risks. This includes improvements in technology, hardware, human factors and hazard analysis techniques. Further risk reduction can be achieved by continuing these improvements but it is making the whole process of risk management more complex and taking it out of the hands of line managers. The

authors argue that a better way to reduce risk is to restrain this complexity and to hand risk management back to the line managers. In parallel, we must make sure that they are competent to take on this responsibility.

REFERENCES

1. Hopkins, A. (2005) Safety, Culture and Risk. *CCH Australia Ltd*.
2. Hopkins, A. (2000) Lessons from Longford. *CCH Australia Ltd.*
3. Ditchburn, S. and Mohess, R.; (2004) Impelementing Major Accident Hazard Management; *Hazards XVIII I Chem. E*.
4. Dalzell, G. (2003) Risk Assessment or Hazard Management *OECD Workshop on the Education of Engineers in Risk – Montreal*.
5. Weick, K, Sutcliffe K, and Obstfeld; (1999); Organising for High Reliability: Process of Collectful Mindfulness._Research in Organisational Behaviour_21_81-123.
6. Weick, K, Sutcliffe K, Managing the Unexpected: Assuring High Performance in an Age of Complexity. San Fransisco: Jossey Bass.
7. Dalzell G.; SPE 86705 The Body or the Smoking Gun? (2004) Society of Petroleum Engineers HSE Conference.
8. Investigation into the fatalities at in the leg of the Brent Alpha (2004) *unpublished*.
9. Macnaughton N.J., Watson C.C., Lessons from Grangemouth; (2004)*Hazards XVIII I Chem. E*.
10. Prevention of Fire and Explosion, and Emergency Response on Offshore Installations Regulations (1995), Approved code of practice; *HSE books*.
11. A Guide to the Integrity, workplace Environment and Miscellaneous Aspects of the Offshore Installations and Wells (Design and Construction) Regulations Offshore Design and Construction Regulations (1996) *HSE books*.
12. Dalzell G., Hazard Management or Safety Case (2003) *4th International Conference on Fire and Explosion Hazards, Londonderry*.
13. Kruzman, Dan (1987) A Killing Wind – Inside Union Carbide and the Bhopal Catastrophe; *New York McGraw Hill*.
14. Vinnem, J.E. Perspective on Gas Explosions Risk Offshore; Low Historic Gas Explosion Frequency; SPE 61501(2000); SPE Health, Safety and Environmental Conference, Stavanger.
15. Poblete B, Singh B, Smith G (2005) The 3Rs Risk Rust and Reliability; *NACE Corrosion 2005 Conference*.
16. Safety Critical Systems; International Standards Organisation ISO 61508.
17. UKOOA, (2001) Risk Based Decision Making Framework; *Published by the United Kingdom Offshore Operators Association.*
18. United States Process Safety Management System; OSHA 1910.119.