Thoughts on Safety Responsibilities of Management

Felix Redmill
Redmill Consultancy, London UK

Felix.Redmill@ncl.ac.uk

Abstract

System safety depends not only on 'operators' but also on management at all hierarchical levels. Rules are made at each level, and these define objectives for, and place constraints on, all lower levels. Moreover, at each level, the rules made at higher levels must be interpreted and translated into other forms. This paper examines four concerns in the responsibilities of management for safety: the problems that occur in the transmission of objectives and constraints, the need for wisdom in the interpretation and management of rules, safety considerations in the governance of organisations, and the need for safety self-awareness in management.

Introduction

The theme of this conference is stated to be 'the role of operators as system components or users of safety-related systems'. But who are the operators? Are they only those who push the buttons and pull the levers? Even if the word 'operator' were limited to this meaning, it would still embrace a broad range of roles, tasks, types of people, and physical and mental requirements, for today's operators are not merely rule- and skill-based technicians but also knowledge-based professionals such as aircraft pilots and senior medical staff.

Whatever their knowledge or skills, button-pushing and lever-pulling operators are merely cogs in wheels and systems of wheels. When operating as directed, they follow procedures and rules defined by others, hierarchically above them and removed from them in role and responsibility. And these, in turn, work within, and conform to, specifications, strategies and policies defined by senior management and company directors – as well as laws and regulations from outside the company. At each level of a hierarchy, objectives are set, and these not only define the goals of those at lower levels – including operatives at lower levels – but also place constraints on them. The constraints often create risks, and the objectives may preclude adequate mitigation.

Thus, operation is not only performed but also defined and directed. And the term 'operator' may be taken to embrace not only those who carry out the direct operation of equipment but also the management at various levels who represent the operating company, including the company directors who define the policies that require the equipment's existence, the objectives that it should fulfil, and the productivity that it should achieve.

Are these managers competent operators? Is their way of thinking conducive to the management – or even the understanding – of safety risk? Observation suggests that the answer is far from being a universal 'yes'. Safety management should not be limited to the design and delivery processes but should be integral to management at all levels. Indeed, it should be integral to the overall business culture and not perceived as a stand-alone discipline. Thus, this paper is based on the broader encompassment of the term 'operator', and it explores the need for the 'indirect' operators to be suited to their considerable responsibilities in managing safety risks. The paper explores four areas of management where greater attention might usefully be paid to safety.

This was an invited paper at the 12th Australian Conference on Safety Critical Systems and Software, Adelaide, 30-31 August 2007.

Objectives and Constraints

Each level in a decision-making hierarchy defines objectives for the level below. At every level, the objectives must fall within those set at all levels above. In this manner, high-level objectives are passed down and, ultimately, met by staff 'at the coalface' or by a system at its boundary with 'the rest of the world'. In a company, directors define policies, they and senior management define strategies for meeting them, and subsequent levels of management implement the strategies by defining projects, work schedules, procedures, and tasks.

Each objective defines constraints, for example on the time taken to achieve a goal, on the cost within which it must be achieved, and on the resources to be employed in achieving it. These may be explicitly stated within the objective, or they may be implied. For example, if recruitment of new staff is prohibited, a goal would have to be met with existing resources while also meeting other existing commitments.

Another crucial constraint is that the scope defined by an objective should not be exceeded. Many projects have failed (exceeded intended cost and time, or failed entirely to deliver a useful product) because the scope defined in the company's objectives has been increased by the addition of requirements at one or more succeeding levels of hierarchy (requirement creep may also be caused by an external customer, but in such a case the customer may be expected to pay for the additions).

If a manager at level N perceives the need to set an objective (for level N+1) that extends outside the scope of the objectives set at level N-1, either the higher-level objective should be amended in recognition of its now-discovered deficiency, or the level N manager should desist from the proposed extension in recognition of its inappropriateness. A frequent problem, though, is that manager N neither communicates to manager N-1 the perceived need for an extension nor desists from pursuing the additional requirements, with the result that the difficulty of achieving success is increased: the breach of a constraint introduces risk. Leveson (2004) recognises this, and a key feature of her accident model (STAMP – systems-theoretic accident model and processes) is the identification of constraints and the investigation of the risks surrounding them.

This problem of non-communication is an element – or, perhaps, a symptom – of an even greater problem, or, rather, a set of linked problems. First, policing the transfer of objectives down a hierarchy is a difficult task, for the transfer is not the simple passing on of an instruction but, at each level, its interpretation and re-representation in a different form (for example, objectives are translated into system requirements which are, in turn, translated into a design). Second, senior managers often have no inclination to police the transfer and do not see it as their responsibility to do so; having defined policy, or objectives, they typically expect that appropriate results will follow – through other people's un-policed diligence. Third, senior management are usually incapable of recognising deviations from objectives or violations of constraints in the transfer of objectives down the hierarchy, because they possess no knowledge of the technologies employed in support of the various forms of work that are carried out in their companies. As a result of these problems, the translation of objectives and constraints down a hierarchy is often poorly defined, un-policed, and subject to both error and intentional violation. A visible manifestation of the result of this is the very frequent and public failure of government departments to fulfil the policies defined by their ministers.

The work to fulfil a level N objective is often distributed among a number of managers or teams at level N+1, as shown in Figure 1. There, risks arise not only because of overlaps (JQ) but also because of gaps (KR) and because the original scope (AB) has been extended (to PS). In a development project, the extensions PA and BS add requirements that must in any case increase cost and time and, if their achievement is technologically challenging, could be fatal to a project. They introduce a risk to the project and, if additional time and resources are not provided for their accomplishment, that risk is increased, perhaps substantially.

The overlaps of responsibility (e.g. JQ) are as likely to lead to neither of the two relevant level N+1 managers discharging the responsibilities as to both doing so, and the deficits created by the gaps (e.g. KR) may not be detected, at least until it is too late. When safety is a factor, the risks include conflicting requirements, the omission of risk-reduction features, and trades-off that are detrimental to safety.

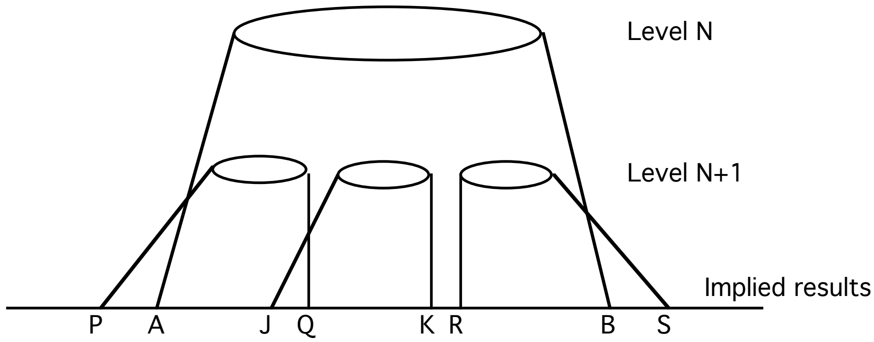

Figure 1: One objective to be fulfilled by three work packages

But the reverse of what is depicted in Figure 1 can also occur. Figure 2 shows a number of senior managers at level N contributing objectives to a project, which is to be executed by a single level N+1 project manager. It is unlikely that the senior managers' objectives and constraints on the project will have been the result of collaboration – at least in the first place – and it is almost certain that there will be conflicts between them. If a project has conflicting objectives, it is bound to run into trouble. And if it has too many objectives, some are bound to conflict with others. The senior managers must be persuaded to agree to common goals. But project managers typically think (and are trained) in terms of requirements rather than objectives and many do not realise the importance of setting common goals. Or they are too timid to challenge the senior managers, or they don't know what to propose as a solution if they did challenge them. The solution employed by the author was to hold soft systems methodology (Checkland and Scholes 1990) workshops for the senior stakeholders at the start of a project and to persist until clear, non-conflicting objectives were defined (so far as could be judged at the time). Getting senior project stakeholders to attend such workshops, together, is not easy, but project success is unlikely without achieving it.

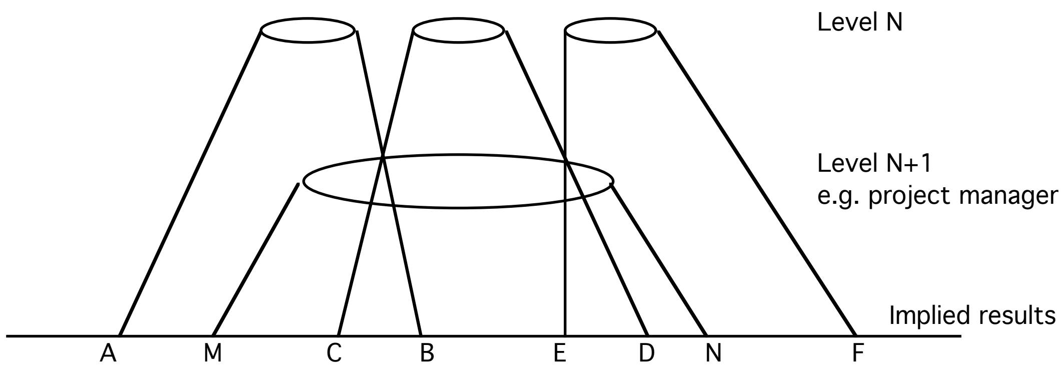

Figure 2: Three sets of objectives to be fulfilled by one project (or system)

In Figure 1 it is the level N+1 managers who are likely to exceed the scope of the proper objectives, but in Figure 2 it is the level N senior managers who are likely to do so. They may genuinely have requirements that lead to the definition of objectives AB, CD and EF, but without careful strategic definition of the project it may not be apparent to them that the business would be best served by a system of scope MN. This may be so for a number of reasons, for example because of the time to develop the system and bring it into productive operation, or the technological difficulty and, therefore, the cost and resources to provide AM and NF. But it is unlikely that the level N senior managers would recognise this, all being blinkered by the perceived importance of their own requirements. It needs a business strategist to analyse the proposed objectives in the light of the business' requirements and arrive at the 'optimum' scope of the system. And then it requires further analysis in order to rationalise the overlaps in objectives – as well as any gaps between the stated objectives and the ideal business system, or the appropriately safe system.

So far in this section the discussion has been general, with references to projects rather than specifically to safety. The fact is that the matters under discussion are general. Clarity of objectives is key to success in any endeavour, and lack of it creates risks. Similarly, the constraints that emerge from objectives throw up risks in all fields and, if they are not recognised and managed, they lead to failure.

Trades-off between safety and productivity (addressed below) may be considered in the light of the current discussion, as can the balancing of safety and functional requirements. An extension of a project's scope in order to introduce risk-reduction functions may be essential, but an extension to increase functional utility may not.

The levels of decision-making and objective setting are not restricted to those within a company. The causes of accidents may be created by the constraints imposed at any of the levels shown in Figure 3 (Rasmussen 1997), so the risks thrown up at all those levels need to be managed (Leveson 2004). The actors at each level in the figure create, by their actions, objectives and constraints that apply to all levels below them. Governments pass down laws, regulators pass down regulations, company directors pass down policies, and so on. And the activities of each lower-level actor should be planned and resourced to meet the objectives, and to remain within the constraints, set at the level above. This simplified adaptation of Rasmussen's socio-technical model omits feedback loops, but they should exist. If staff – at all levels – are to recover from system failures and other threatening occurrences, they need information that is appropriately accurate, designed to be understood by the intended recipient, and provided in time to inform necessary decisions. Safety engineering requires equipment designers to ensure such feedback at the staff and work levels, but feedback planning also needs to be carried out at, and for, the higher levels. Indirect operators involved in company governance should plan for their own involvement in safety-threatening eventualities.

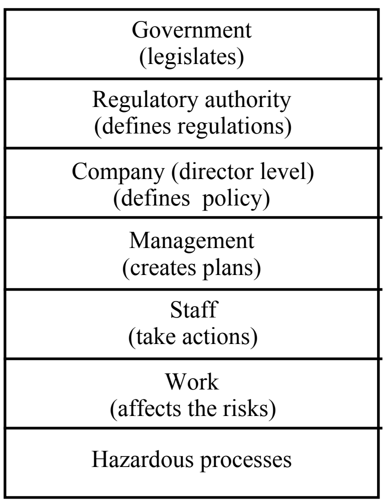

Figure 3: Risk levels (adapted from Rasmussen 1997)

One of the points that emerges from this discussion is that safety risks are not static conditions or single events, but often dynamic processes that depend for their development on current circumstances – which themselves are likely to be in flux. With such a hierarchy of players as shown in Figure 3, each placing constraints that others below them must observe, and receiving feedback on their efficacy (or otherwise), it is inevitable that effective risk management should take account of more than has hitherto been recognised; it must be carried out in the context of change. Senior management must take note of these realities, which affect the safety of the enterprises for which they hold responsibility.

Wisdom in Management of People and Operations

The majority of staff want – and need – rules to work by. They do not want to have to determine each course of action from first principles. Indeed, in most cases they would not be capable of reverting to first principles and, in some cases, when rapid action is required, there would not be time for doing so. Rules are also required to ensure that the members of an organisation achieve consistency in doing the right thing and doing it at the correct time or at the correct point in a process.

Thus, at each of the top four levels shown in Figure 3, rules must be produced, from laws by the government to plans and work instructions by company management of various grades. Rules also take the form of standards (and their associated guidance), and these may be international and wide-ranging, sector-specific, or written or tailored for a particular company or even for a project.

Producing rules is a tricky business. It poses problems that are often not apparent to those involved. It is often not difficult to define what must be done, but rule-makers often neglect to carry out preliminary analysis to determine whether what they want done is effective, or even sensible, and safe. They ignore the training that would inform staff of the importance of particular procedures, and they neglect to assess the conditions under which staff or others are likely to break the safety rules. There are always such conditions, examples being ignorance, inconvenience, and conflict with other rules such as those of productivity. Then, staff are likely to commit violations (which are the unofficial rules devised at the operational level to circumvent the strictures imposed by the rules from above). An aspect of wise management, particularly in the context of safety, is to create rules that do not encourage violations. And, in this context, wisdom also extends to planning for rule breeches, for people cannot be relied on to adhere to rules in all situations.

In the Introduction to this paper, allusion was made to the classification of operators, proposed by Rasmussen, into rule-based, skill-based and knowledge-based. When the term 'operator' is extended to include management associated indirectly with the operation of systems, the classification also needs to be extended. Those who define the objectives that other staff must meet, and the constraints within which they must operate, require not merely knowledge but, importantly, understanding of the systems involved, the tasks to be carried out, the environment within which they must carry them out, and the fundamentals of safety management. More than that, they must apply their understanding in their tasks of definition and direction. They must understand the spirit of the law that they set out to interpret or define and not be governed entirely by its letter. They require wisdom.

The wisdom-based element of operation is necessary (though often lacking) at all risk levels (see Figure 3). Moreover, it is required not only in defining rules (and other instructions) and in decision-making in general, but also in interpreting the rules that have been passed down from a higher risk level. For example, a debate currently in progress in the safety community is that on self-regulation. With the increase in the scope of safety-critical systems, some self-regulation seems essential. But not everyone wants it. In particular, the management of small and medium-sized enterprises (SMEs) do not. They do not want the responsibility of making significant risk decisions, and many such companies do not have the expertise to make them so as to satisfy regulators. They want prescription, in the form of rules of what to do. But regulations are written to fit a range of circumstances, and so, in any given circumstance, even prescriptive rules permit latitude and require interpretation. And there lies the rub. Wise, and not blind, interpretation is necessary. Senior managers, even those seeking simply to follow prescription, need to interpret rules from above and, thus, to be safety-wise. The reason why 'health and safety' rules elicit ridicule, and sometimes rage, in the UK is that they are interpreted and communicated not wisely but foolishly and unsympathetically. Risk assessment is too often misinterpreted in officious and unbending ways rather than wisely.

When it comes to self-regulation, managers at all levels need to be alert to changes that indicate that the company is, or may be, drifting towards the safety threshold. Retrospective analysis by Vaughan (1996) shows how such drift occurred within NASA (the National Aeronautics and Space Administration) and led to the explosion of the space shuttle *Challenger* in 1986. To detect drift, management needs to monitor safety and, with few serious accidents from which to compile statistics, they need to monitor, and derive trends from, lesser incidents (Koornneef, 2000). It is not uncommon for the more safety-aware organisations to keep hazard logs in which identified hazards are recorded, but it is not so common for the recording of incidents that do not lead to loss, and even less common for their trends to be plotted and used as safety indicators. (The civil aviation industry is an example of where this practice is built into the culture.)

The recording of hazards and incidents can be accomplished according to rules. But the understanding of safety trends demands that senior management develop knowledge of safety principles. It is not enough that they delegate all safety responsibility to others. Good and adequate safety management demands that they employ a risk-based way of thinking and that they apply safety-wisdom in their decisions.

Safety management must start at the top, but there are roles for which middle managers also need to be wise. It is they who in most cases are responsible for the interpretation of company policies into procedures and for the introduction of standards. The latter may be written in-house, but are mostly drawn in from outside. In the latter case, they require tailoring to the company's needs, and in both cases they need tailoring to the needs of any particular project. Redmill (2000) defined 'nine necessities' for the introduction and use of a standard:

- Understanding the standard's purpose and scope;
- Understanding the content of the standard;
- Knowing how to apply the standard;
- Understanding the principles embedded in the standard;
- Recognising the standard's assumptions;
- Appreciating what the standard does not cover, both intentionally and by omission;
- Possessing the expertise to apply the standard;
- Providing support to the users of the standard;
- Providing the necessary infrastructure for the effective introduction and application of the standard.

At the time of that paper, which was written in the context of the international standard, IEC 61508, the evidence suggested that almost all senior managers and most middle managers responsible for the standard had not attended to those nine necessities. More recent evidence, derived from experience (and not from formal scientific study), indicates that there has only been modest change – with the exception that now more staff know more about the standard and, therefore, possess a better understanding of its assumptions and its deficiencies, even though these are (typically) not spelt out to them by management. But the effective (and efficient) use of a standard requires support from above, including the provision of an appropriate infrastructure (for receiving queries, providing help, carrying out changes to the standard, and other matters), and these in turn can only be based on the other seven necessities. It seems that they are not yet in place across the safety-critical systems spectrum.

In addition to the requirement for middle management to provide wise leadership of lower-level staff, Flin (2006) points to the pressure on these managers from above to compromise safety in favour of productivity. To counteract this pressure, she identifies three component skills, which, she says, characterise managerial 'resilience'. They are:

- *Diagnosis* – the ability to detect operational drift towards a safety boundary. This, in turn, requires 'the cognitive skill of situation awareness, which encompasses gathering information, making sense of it, and anticipating how the present situation may develop'.
- *Decision-making* – the ability to select appropriate action to reverse the diagnosed drift and so return the system or company to safety.
- *Assertiveness* – the ability to persuade other personnel, including senior management, of the need for the necessary action, particularly given that such action often includes the halting of production and an increase in costs.

In the context of safety, these three skills point to the need for safety awareness, a good safety culture, and safety-wise management. In some companies, these attributes have improved in the last decade, but in general there is yet need for considerable improvement. However, the three skills are not confined to safety but are generally desirable attributes in staff at all levels.

Safety in Governance

In 1987 a roll-on-roll-off ferry, *Herald of Free Enterprise*, sank off Zeebrugge, Belgium, with the loss of 188 lives. The bow doors, which should have been closed prior to departure from port, had been left open. When the accident was investigated (Steel 1987), it was revealed that masters of roll-on roll-off ships in the fleet had requested the installation of a monitor, to indicate the status of the bow doors to the captain and officers on the bridge, but that the requests had been turned down by the company's management. Yet the cost of a monitor and its installation was estimated at £400 - £500. In absolute terms this was, for a shipping company, tiny; in relative terms – relative to the costs thrown up by the accident, including the collapse of the company – it was infinitesimally small.

Since analysis must have shown the repeatedly requested risk-reduction mechanism to be of value, it is likely that senior management dismissed the request cursorily. Yet their business of transporting passengers on the sea was inherently risky. Suppose the proposal was for a change in procedure that would allow the ship's crew to be reduced by one? Or suppose that it was for a way of reducing the company's expenses per journey? We might speculate that such proposals would have been seized on, for company executives are typically motivated by two variables, productivity and cost, and means of increasing the former and reducing the latter are always of interest. (Of course, other variables are also of interest in the boardroom, among them customer satisfaction, public perception, and share price.)

In organisations where safety-related systems are created or operated, safety is of at least equal importance to these two variables, but it does not yet appear to possess their influence. Or, perhaps, there is intellectual recognition and what is missing at the highest levels of management is an understanding of how to deal with safety. Yet, a risk-based approach would readily have revealed the considerable disproportion between the benefit and the cost of having a monitor on the bow doors.

What is required is a better understanding of safety in the boardroom, where safety should be perceived to be as significant in decision making, and as important a motivating factor, as productivity and cost. Safety motivation occurs in a few organisations, but it is not the general rule.

A company that is highly productive, but which pays no attention to safety, risks going out of business. But a company that makes a financial loss because it spends too much on safety also risks collapse. Like other system attributes, safety must be engineered within constraints, and these are on the one hand imposed in absolute terms by measures of cost (e.g. such-and-such must be achieved for less than N units of currency) and on the other hand in relative terms as against other engineered attributes (e.g. a particular reduction of risk is balanced against a resultant loss of productivity).

Thus, in the same way that directors ask if improvements in productivity 'cost in', and what it's worth to achieve greater productivity – or even, what it would cost if we didn't achieve greater productivity – so they need to ask the same questions about safety. But those are the questions about absolute costs. Questions also need to be asked about relativities. Just as the potential effects of risk-reduction measures on productivity are assessed, so it is also necessary to enquire into the potential effects on safety of changes in other attributes (e.g. what would be the effect on safety of the proposed staff cuts?). An example of such relativity in the railway industry is the balancing of safety considerations against the need to meet tight timetable schedules.

There is always tension between safety and productivity, and both should be boardroom-motivating variables, with cost being, in the end, what both are reduced to. Handled properly, the three would be considered not in isolation but in relation to each other, as in Figure 4.

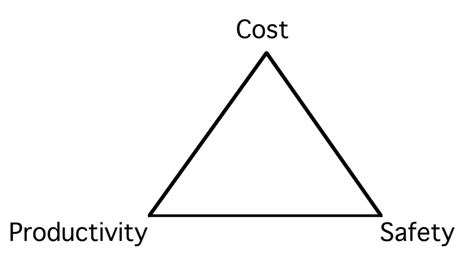

Figure 4: Three decision-critical variables

A natural inclination in looking at Figure 4 is to suppose that the three elements should be in equilibrium. Sure enough, in an effective system (i.e. one that is operated both profitably and safely) they should be. Beware, however, of assuming that such equilibrium must be static, that it can be defined and then achieved and retained indefinitely. The equilibrium of these variables can only be dynamic. The conditions under which a system (and a company) operates are always in flux, as are the criteria against which both productivity and safety are assessed.

Thus, if safety is to be a boardroom motivator, in acknowledged tension with productivity, the dynamic nature of their balance must be recognised by management. If senior management is to pose appropriate questions, make sense of the answers, and, further, carry out assessments so as to create policies and make strategic decisions based on the answers, they need not only to think in a risk-based way but also to do so in the context of change. They need to ponder safety risks as well as financial risks, and they need to understand engineering solutions as well as financial solutions. They may be able to insure against pure financial loss, but risk transfer is not a solution when the company's operations pose risks to the lives of the public or to the environment.

Following the Turnbull Report (ICAEW 1999), it is expected that senior managers should identify, analyse and manage 'the significant risks faced by the company', and the inculcation of a culture of risk-based thinking is occurring in some companies. But before safety can be a boardroom motivator, there needs to be motivation for it to be in the boardroom in the first place, and this must stem from the inclusion of safety principles, and decision-making in the face of risk, in the education and training of executives.

Safety Self-awareness

The developments addressed above will not happen by chance. They are only likely to occur when senior management develop greater awareness of their own influence on the safety of their organisations – through the culture that their leadership promotes, by design or default, and in their decisions.

Where can greater awareness come from? A first and important source is leadership by self-aware managers. A second source, and an essential one if change is to be rapid, must be the education of management – in not only the objective knowledge of safety principles, but also the subjective analysis of one's own influence over organisational and system safety, the absolute importance of this influence, and one's control over it. A third source could be the encouragement of senior managers (and others) to subject their rules, proposals and key decisions to risk analysis (Redmill 2006). And a fourth would be recognition of the potential consequences (accidents and near accidents) of management safety unawareness – which would ensue from greater safety self-awareness.

And so, the development of self-awareness is a circular – or, more correctly, a spiral – process. Greater safety self-awareness leads to change towards improved safety, which awakens greater awareness, which leads to further improvement, and so on. Of course, it also happens that change towards improved safety can lead to complacency – but the point about self-awareness, rather than mere safety awareness, is that it should reveal this tendency and show the need to counteract it.

In recent years there has been much work done on safety culture and safety climate, but a great part of this has been theoretical. Even when safety culture is assessed in an organisation, the matters put forward in this paper are seldom addressed. There is yet work to be done in the boardroom, not merely on the attention to safety of those at lower levels but, importantly, on the safety awareness of those around the table.

Conclusions

This paper has posed the proposition that management – senior management in particular, but also middle management – need to be more informed of, and involved in, the safety management of their companies, systems and projects. Specifically, the paper explores four contributory topics. First, it shows how objectives, passed down a managerial hierarchy, are translated at each stage into new representations of what is required, how distortions are created in translation, how the objectives throw up constraints on the achievement of tolerable safety, and how resulting dynamic interactions give rise to accidents. It is proposed that senior and middle management should have better understanding of the effects on safety of the rules that they produce and that they should make more effort to police the translation and achievement of their objectives. Second, the paper proposes that there is need for greater wisdom in safety management, in management's interpretation of rules passed down to them from above, in their communication and policing of rules to those below them, and in detecting an organisation's drift towards the safety threshold. For this, all levels of management, and particularly senior management, require a foundation of better knowledge of safety principles and improved understanding of the safety technologies that they employ. Third, the paper examines the tension between productivity and safety and suggests that the latter should be as much a boardroom motivator as the former. Fourth, it shows that senior management require greater safety self-awareness, not only as the basis for the previously mentioned three improvements, but also in order to monitor their own decisions and actions from a safety perspective. Indeed, all safety practitioners need to focus on improving their safety self-awareness.

Safety management should be integrated into the culture at all levels of management. Implicit in this is the need for all levels of management to be informed in safety principles. Whereas this is beginning to be the case at lower levels, it is not so at higher levels, and particularly not so at levels where managers are recruited wholly for their financial acumen. It is recommended that all managers responsible for the governance of organisations involved in safety-critical products or operations should possess safety knowledge and understanding. For this there should be compulsory safety education and the inculcation of a risk-based way of thinking.

References

Checkland P B and Scholes J (1990). *Soft Systems Methodology in Action*. John Wiley & Sons, Chichester

Flin R (2006). Erosion of Managerial Resilience: From Vasa to NASA. In Hollnagel E, Woods D D and Leveson N (Eds): *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing, Aldershot

ICAEW (1999). *Internal Control - Guidance for Directors on the Combined Code*. The Institute of Chartered Accountants in England and Wales, London

Koornneef F (2000). *Organised Learning from Small-scale Incidents*. Delft University Press, The Netherlands

Leveson N G (2004). A New Accident Model for Engineering Safer Systems. *Safety Science*, Vol. 42, No. 4, pp. 237-70

Rasmussen J (1997). Risk Management in a Dynamic Society: a modelling problem. *Safety Science*, Vol. 27, No. 2, pp. 183-213

Redmill F (2000). Installing IEC 61508 and Supporting Its Users – Nine Necessities. *Fifth Australian Workshop on Safety Critical Systems and Software*, Melbourne, Australia

Redmill F (2006). Understanding the Risks Posed by Management. In Redmill F and Anderson T (Eds.): *Developments in Risk-based Approaches to Safety – Proceedings of the Fourteenth Safety-critical Systems Symposium*. Springer-Verlag, London

Steel D (1987). *Formal Investigation Into the MV Herald of Free Enterprise Ferry Disaster*. HMSO, London

Vaughan D (1996). *The Challenger Launch Disaster*. University of Chicago Press, Chicago