Where is the safety management system heading – a company wide approach to continuous improvement

Accou, B.

European Railway Agency,
120 Rue Marc le Francq,
59300, Valenciennes, France

Abstract

Business risk management (McNamee and Selim, 1998) defines inherent risk as "the risk found in the environment and in human activities that is part of existence" and residual risk as "the remaining risk after risk management techniques have been applied". Building on these basic concepts, projected in the risk space, the paper rethinks the fundamental elements that traditionally are part of a safety management system.

This reflection leads to a generic safety management system model that makes a clear distinction between:

a) Operational processes that create, produce and deliver the products and services that customers want, including the direct response to operational threat. This also means that all operational risk control measures –whether they be technical, human, organisational or any combination of them- form an integral part of these operational processes.

b) Four management processes that together define how to accomplish tasks, how to evaluate and how to adapt them to an ever changing environment. Their main objectives are: anticipating potential threats, monitoring performance and learning from experience.

c) Four support processes that, by underpinning both operational and management processes, are indispensible to run the business: people need to know what their role in the system is and what their level of responsibility is; they need the knowledge and skills to know what to do in all circumstances, and at all times they need to have all relevant information available in an adequate form

Later in the paper, this model is used to reflect on what "continuous improvement" is and what type of indicators or triggers might be necessary to realise this objective. Finally, the loop is closed by going back to the principles of business risk management and the definition of risk as "the effect of uncertainty on objectives", which leads to the conclusion that the principles of the developed model can easily be transposed from a safety to a wider business objectives setting context, giving a new dimension to the integration of different management systems.

Introduction

Within the European railway system, Directive 2004/49/EC introduces the concept of a safety management system as one of the corner stones of the safety regulatory framework that should ensure a high level of railway safety. All those operating the railway system (infrastructure managers and railway undertakings) should hereby bear the full responsibility for the safety of the system, each for their own part; and the establishment of a safety management system is identified as the appropriate way to fulfil this responsibility.

A safety certificate, issued by the national safety authority of a Member State, should then give evidence that the railway undertaking has established its safety management system and is able to comply with the relevant safety standards and rules. Directive 2004/49/EC hereby recognises the clear distinction a Member State should make between, on the one hand the immediate responsibility for safe operation, and on the other hand the safety authorities' task of providing a national regulatory framework and supervising the performance of the

operators. For international transport services it should then be sufficient to approve the safety management system in one Member State and give the approval European wide validity.

Although this framework has been mandatory in all EU Member States since 2006, recent findings show an unwillingness to accept these different roles and responsibilities and a poor understanding of even the basic concepts of a safety management system. Within this context, there is clearly need for a more thorough understanding of the safety regulatory framework and the important role of safety management systems within it. This paper is an attempt to gain a better understanding of what a safety management system is and should achieve by exploring the functioning of its basic elements and the way they can help to improve safety.

Basic risk management concepts

Directive 2004/49/EC defines a safety management system as "the organisation and arrangements established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations". Hereby it is generally recognised that, in an increasingly complex and global business environment, risk is the driver of organisational activity and risk management is a key organisational process for running the railway business in a safe way.

But using the concepts of risk and risk management requires somehow the understanding and measurement of risk. In this context the new international standard for Risk Management (ISO 31000, 2009) states clearly that Risk Management should be dynamic, iterative and responsive to change. The question of how to deal with this effectively remains open however. To find a possible answer to the question in this paper, the widely accepted concepts of inherent and residual risk are used.

Business risk management (McNamee and Selim, 1998) defines *inherent risk* as "the risk found in the environment and in human activities that is part of existence" and *residual risk* as "the remaining risk after risk management techniques have been applied".

A first, well know approach to reduce an inherent risk to an acceptable residual risk focuses on prevention. This requires organisations to anticipate occurrences that must not happen, identify all possible initiating events or conditions that may lead to them, and then create a set of control measures to avoid them. A second approach -protection- interacts only when events occur and tries to avert the effects or limit them before they escalate. Taking into account the traditional two components of risk -likelihood and consequences- pure prevention reduces the likelihood of something happening, where protection reduces the consequences if it happens. This can be represented in the risk space -a two-dimensional representation of risk- as follows:

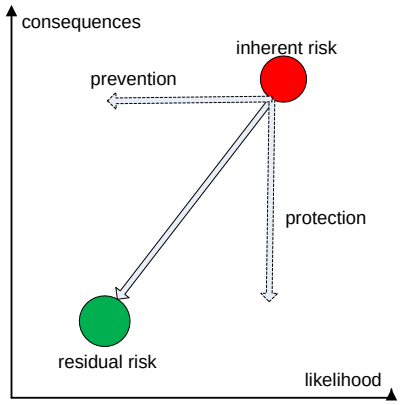

Figure 1: risk and risk control measures projected in the risk space

Both approaches for risk control have their limitations, and probably the best results for reducing risk can be achieved by combining them. Also much more detailed and elaborate classifications for these risk control measures or barriers exist. However, for the purpose of this paper, this simple model is sufficient to emphasise that it is impossible to understand the actual level of any safety risk -the residual risk i.e. the position of the green bullet in the risk space- without also having an idea of the internal and external environment it is situated in -the inherent risk i.e. the position of the red bullet in the risk space- and the effectiveness of the control measures -i.e. the length of the arrows in the figure.

Indeed, only looking at the indicators that witness the residual safety risk (a negative outcome) could be an indication, but is certainly not proof of safely performed operations. An organisation also needs to ascertain if the designed control measures perform effectively and continue to do so in a changing environment. Furthermore, risk control measures are designed based on what is perceived to be the inherent risk and are therefore largely determined by the organisations (necessarily limited?) knowledge of the dangers that threatens its activities.

The way railway undertakings and infrastructure managers truly succeed in continuously understanding this trinity of risk for every uncertainty on their objectives of ensuring the safe management of their operations, will predetermine their sustainable success. In fact, the degree to which an organisation’s understanding of this model reflects reality, together with their capability of translating this acquired knowledge into their operational practices, will indeed determine their ability to respond to various operational disturbances and to regular and irregular threats.

Nevertheless, in my career as an auditor, I’ve witnessed a lot of operators performing safety related procedures without knowing or appreciating their purpose. I’ve also seen many senior managers taking important decisions without understanding or even reflecting on the impact any introduced changes could have on safety performance. Therefore I believe the real goal of a safety management system for railway undertakings and infrastructure managers should be to optimise their risk control measures based on a true understanding, at all organisational levels, of both the inherent and residual risks related to their operations.

Regrouping the elements of a safety management system

Building on the abovementioned model and the subsequent goal, the overall objective of the classic elements that constitute a safety management system, as mentioned in management standards and legislative texts (e.g. Annex III of Directive 2004/49/EC that will be used throughout this paper as a reference) has been analysed. Based on their intended purpose, this analysis leads to three main groups of safety management systems elements or processes.

A first group of processes create, produce and deliver the products and services that customers want, including the direct response to operational threats. This means that also all operational safety risk control measures -be it technical, human, organisational or every possible combination of these- form an integral part of these processes. For the purposes of this paper, these processes are called *operational processes*. A classical example of such an operational processes that is typically considered as part of an adequate safety management system is the presence of an emergency plan – In Annex III, 2 (i) of Directive 2004/49/EC referred to as "provision of plans for action and alerts and information in case of emergency, agreed upon with the appropriate public authorities". In the risk model developed before, such an emergency plan forms part of the protective risk control measures that aim at reducing the consequences of an adverse occurrence, every time it happens. It is clear that these are the processes that should deliver safe operations at the sharp end of business activities.

A second group of processes are indispensible to implementing and establishing the operational processes, including the corresponding risk control measures, and making them work as they are designed. For the purpose of this paper, these processes are called *support processes*. The typical support elements that come back in most safety and other management standards can be classified in one of the following four subgroups:

- *Structure and responsibility*:
  To be able to fulfil their activities in an adequate way, people need to know what their role in the system is and what they are responsible for. This is referred to in Annex III.1 of Directive 2004/49/EC as part of the main requirements: "The safety management system … shall in particular describe the distribution of responsibilities within the organisation of the infrastructure manager or the railway undertaking. It shall show how control by the management on different levels is secured, how staff and their representatives on all levels are involved …". Furthermore, the structure of this organisation needs to be adapted to the activities.
- *Competence management*:
  Also, people need to have the knowledge and skills to perform their tasks effectively, to know what to do in all circumstances, and to be aware how they can impact on safety. This is referred to in Annex III (e) of Directive 2004/49/EC as "provision of programmes for training of staff and systems to ensure that the staff's competence is maintained and tasks carried out accordingly". This support process covers element like recruitment based on identified competences, training, the evaluation of staff performance, knowledge management, etc.

- *Information*:
  Further, to be able to function adequately, the system needs at all times to have all relevant information available in an adequate form. This is referred to in Annex III (f) of Directive 2004/49/EC as “arrangements for the provision of sufficient information within the organisation and, where appropriate, between organisations operating on the same infrastructure”. The purpose of this support process is to identify the sequence and interactions of specific operational processes, to determine the information needs of different subsystems (technical sub-systems but also groups or individuals) involved in the process and to manage these interfaces.
- *Documentation*:
  The purpose of this last support process is to develop and maintain the recorded information produced by operational processes. This is referred to in Annex III (g) of Directive 2004/49/EC as “procedures and formats for how safety information is to be documented and designation of procedure for configuration control of vital safety information”. Also, to avoid inefficient use of resources, unclear responsibilities, uncontrolled decisions, and uncertainty whether objectives will be met, this support process can help to establish a suite of core standardised processes as they apply to the organisation’s business activities.

Unlike the operational processes which, because of their origin in very diverse types of operational activities, are more specific in nature, these support processes are very generic and should be applied to all existing operational processes to ensure that the business is run as intended. Without having developed its support processes, an organisation clearly risks an inefficient use of resources, unclear responsibilities, uncontrolled decisions, and uncertainty as to whether safety objectives will be met.

A last group of processes is necessary to define how to accomplish tasks, how to evaluate and how to adapt them to an ever changing environment. Their main objectives are: anticipating potential threats, monitoring performance and learning from experience in order to improve operational process, the corresponding risk control measures and the support processes that are necessary for their effective implementation. For the purpose of this paper, these processes are called *management processes*. Typically the following four subgroups can be indentified:

- *Leadership*:
  An organisation should outline the principles and core values according to which the organisation and staff operate. Thus, it gives evidence of the organisation’s management commitment to the development and improvement of safety as a long term business objective. It also provides staff with clear guidance for action to consolidate safety culture and safety awareness within the organisation. Corporate safety targets need to be set and broken down at all levels of the organisation. This is referred to in Annex III.2 of Directive 2004/49/EC: (a) “a safety policy approved by the organisation’s chief executive and communicated to all staff” and (b) “qualitative and quantitative targets of the organisation for the maintenance and enhancement of safety, and plans and procedures for reaching these targets”. Furthermore, management decisions need to be taken consciously and based on the results (and

limitations) delivered by the other management processes.

- *Risk assessment*:
  An organisation should define the risk assessment methodologies to be used, develop criteria to evaluate the significance of safety risks as well as strategies to control them. These criteria and risk control strategies should reflect the organisation's values, objectives and resources as well as take into account other business objectives. This is referred to in Annex III (d) of Directive 2004/49/EC as "procedures and methods for carrying out risk evaluation and implementing risk control measures whenever a change of the operating conditions or new material imposes new risks on the infrastructure or on operations".
- *Monitoring*:
  An organisation, throughout all levels, should rely on a structured monitoring system, to ensure that delivery (technical, behavioural and organisational) meets expectations. This should be used to initiate further analysis and to provide decision-makers both at the frontline and in back office functions of the organisation with adequate information to make appropriate decisions about risks. The only place where this important management process is referred to as an element of the safety management system in Directive 2004/49/EC Annex III is 2.(j) as "provisions for recurrent internal auditing of the safety management system". In addition, top management should review the safety management system as such at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
- *Organisational learning*:
  Finally an organisation should analyse appropriate data to evaluate where continual improvement of both safety performance and the effectiveness of the safety management system can be made. This shall include the analysis of data generated as a result of monitoring and from all other relevant sources (including proactive internal information on hazards). Organisations should also ensure the management of all change/transition. This is referred to in Annex III.2 of Directive 2004/49/EC (h) "procedures to ensure that accidents, incidents, near misses and other dangerous occurrences are reported, investigated and analysed and that necessary preventive measures are taken" as well as (j) "provisions for recurrent internal auditing of the safety management system".

Like the support processes, these management processes are also generic in nature. They should be applied in an adapted way to both operational and support processes –and even to management processes. In addition, it is logical also to apply the support processes to all management processes. How else could management take well informed decisions?

Continuous improvement

In common with other management systems in domains like quality and environmental protection, "continuous improvement" is stated in Annex III of Directive 2004/49/EC as one of the basic requirements of the safety management system. When reflecting on how this continuous improvement can be achieved and taking into account the previous discussion,

including the stated goal of a safety management system, different degrees of improvement can be identified.

At a first level railway undertakings and infrastructure managers typically try to measure safety performance by following a number of hazardous events and sometimes precursors to these hazardous events. For the purpose of this paper I refer to them as “outcome indicators”. These outcome indicators try to build an image of the residual risk, but (fortunately) the incidents with major consequences within the railway system, like collisions and derailments, only appear with low frequency in a company, so it’s unlikely that they will be applicable for statistical analysis. There are more incidents than accidents and also near misses could enlarge the amount of useful “outcome” data, but even then we are looking at a negative image, which is from my point of view impossible to manage, when examining the 2-dimensional risk model previously developed. This type of safety management can therefore only deliver a reactive improvement of the existing risk control measures, by investigating accidents and incidents and by looking at what went wrong in a specific case or series of cases. This is even more difficult, since most accidents involve a variety of events and conditions and significant factors leading to the accident do not necessarily emerge from the physical evidence and are therefore hard to discover afterwards.

Most railway undertakings and infrastructure managers within the European railway system, I believe, are operating at this level. Does this mean that they are actually operating in an unsafe manner? No, not necessarily: it should be possible to operate safely, when the necessary risk control measures are adequately identified and implemented, based also on well developed support processes and under the conditions that the internal and external environment is not changing (too much). But when relying only on outcome indicators for improvement of the safety management system, there is also no definitive indication that the organisation is not heading towards a next catastrophic accident, since we lack knowledge of both the environmental threats and the real effectiveness of the risk control measures -i.e. what really occurs in normal operations.

At a second level railway undertakings and infrastructure managers will need to collect data which provides information on how they are performing during “normal” operations –i.e. operations without reportable incidents or near misses. To be able to do so, they will need to identify for all relevant risk control measures those actions or processes that must function correctly to deliver the desired outcome. For the purpose of this paper, I will call these indicators “performance indicators”, since they are measuring the effectiveness of existing risk control measures against a predefined standard or tolerance level. To a certain degree this will not only require the measurement of operational processes, but also of the specific application of support processes since their development will be important for the performance of the risk control measures. This approach should give railway undertakings and infrastructure managers the quantitative ability to detect performance problems early and to take the necessary measures for improvement in a more proactive way.

In the approaches described so far, it has always been taken for granted that risk control measures are of an optimal design and, when applied correctly, reduce the inherent risk of an organisation to an acceptable residual risk. But the full implication of operational activities may not have been understood correctly during the risk assessment or some conditions and combinations of events may just not be foreseeable when designing the risk control measures, etc. Continuous improvement in the context of a safety management system should therefore also include checking whether the foreseen risk control measures actually deliver the intended safe performance. This somehow requires looking at the combinations of outcome and performance indicators and in this context one could question the usefulness of investigating accidents where it is clear that risk control measures did not perform adequately, since the situation clearly delivered the expected outcome (although probably not intentionally and certainly not wanted). To be able to improve the match between the organisation's understanding of the risks it runs and the real threats it faces, more focus should rather go to those events where the outcome turns out to be beyond that expected.

Finally, I believe that adequately optimising the risk control measures requires a collective inquiring mind. It needs continuous examination of possibilities to improve and adapt to possible changes. To be able to do so, other indicators -which for the purpose of this paper I have called "change indicators"- are needed to check assumptions made during the initial assessment of the risk and the design of risk control measures, e.g. on the environment or on the performance of the risk control measures. They are also required to identify changes in the environment of the organisation (both external and internal) which could have an impact on the risks faced.

The environment of railway undertakings and infrastructure managements is dynamic and continuously evolving, like the organisations themselves. This means that there is a permanent need to monitor how effectively an organisation's understanding of its risk and risk control measures -i.e. the mental model of an organisations risks and the way they are controlled- matches the demands and pressures of both the external world and its own internal organisation. Only a combination of the three different types of indicators defined beforehand will provide the necessary information needed to be able to fulfil the defined goal of a safety management system: optimising the risk control measures based on a true understanding, at all organisational levels, of both the inherent and residual risks related to their operations.

Integration of management systems

The new definition of risk, introduced by the 2009 standard on Risk Management (ISO 31000), no longer describes risk only as the combination of the probability of an event and its consequences, but clearly links it to the business objectives of a company by defining risk as the "effect of uncertainty on objectives". So far, we have only looked at the developed models with safety as the sole business objective but it is clear that most organisations have multiple business objectives like customer satisfaction (quality), occupational health, environmental protection, etc. Not to mention the most obvious, driven by the objective of profit: productivity.

I see no reason why the ideas developed earlier in this paper and the described generic elements of a (safety) management system could not be generalised to all identified business objectives. Of course, each objective will require specific techniques, tools and an adapted structure within the organisation and therefore the implementation of the different support and management processes may differ or vary for each objective; the principles however should remain the same. On top of the obvious advantage of reducing the bureaucracy that may exist when supporting separate management systems for different objectives, I'm convinced that this integrated approach –or should I just call it an enterprise-wide risk management approach– will make the (sometimes difficult) balance between safety and other objectives more visible for management and decision takers at all levels of an organisation.

Optimising a company's view of its safety risk should certainly include an active understanding of the continuous trade off between the longer-term safety objective and the more acute productivity objective at all levels of the organisation. But following the first note to the ISO 31000 definition of a risk, that "an effect is a deviation from the expected – positive and/or negative" and against the often advocated principle that safety should always be a company's number one objective, I believe that optimising safety risk control measures in a business-wide context could also mean to consider tradeoffs such as lowering the level of some specific safety risk control measures in favour of meeting other business objectives. The prime constituent however, when doing so, should always be that this kinds of decisions, at all levels, are taken in a conscious and accountable way, based on all available information and with a true understanding of all the related or potential inherent and residual risks. Only a mature risk management system with well developed management and supporting processes can achieve this with reasonable certainty.

Conclusions

The concept of a safety management system as introduced by Directive 2004/49/EC is considered to be an important element within the European safety regulatory framework. It offers all elements to continuously improve and optimise the level of safety performance of railway undertaking and infrastructure managers.

At a higher degree of maturity, continuous improvement will however require a more holistic approach to managing safety risk along other business risks, finding the right balance between different business objectives at all organisational levels. This level of maturity will only be reached gradually, by developing and aligning the necessary support and management processes, driven by the management commitment to a constant questioning of its understanding of risks and existing risk control measures.

The reaction of different CEO's after major railway accidents in the recent past indicate however that there is still a long way to go before European railway undertakings and infrastructure managers reach this level of maturity.