Safety Risk Management

*By **Peter Johnson**, Manchester, UK 44-(0)161-200-5000, johnsonpe@pbworld.com.*

A proactive and pragmatic approach to risk management can be achieved through an effective safety management system. While some of the approaches are similar to those used in risk analysis, safety risk management is a specialized field.

Poor safety management and cultural issues have been identified as the prime causes of a number of modern disasters, including the Clapham Junction rail crash southwest of London in 1988, Kings Cross underground station fire in London in 1987, the sinking of the Herald of Free Enterprise off Zeebrugge, Belgium, in 1987, and the explosion at the Chernobyl nuclear power station in the Ukraine in 1986. Development of an effective safety management system (SMS) and progression towards a good safety culture are key elements in moving towards a proactive and pragmatic approach to risk management and control. This article focuses on those issues that we address when helping our clients to develop effective SMSs and approach changes to organisational safety culture.

Effective Safety Management Systems

The function of an SMS is to provide a framework for managing all elements of an organisation that can have an impact on safety and risk. An SMS must cover, therefore, each of the following areas.

Organisational Policy. The SMS must emphasise safety as a primary element of performance rather than as an obstacle to performance (individuals or groups must not take any blame for choosing safety above another performance goal). The management of many organisations often stresses the importance of safety but, in fact, aims for the performance goal when faced with a conflict between the two. Their operators inevitably take the same approach rather than face the penalties often associated with poor performance, thereby exposing themselves and/or others to an unnecessary level of risk. By making safety an element of performance, choosing an option with greater risk will be seen as jeopardising performance and will, therefore, have an associated penalty. It then becomes a goal of the organisation and all individuals within to reduce the number of incidents occurring each month by reducing levels of risk where possible. Some organisations, notably in the aviation, rail and chemical industries, collect incident and near-incident data that are published regularly as a performance figure.

Organisational Structure. As a management system, an effective SMS should be integrated with all other management systems within an organisation to ensure that safety and risk are considered as parts of the strategy and planning of business goals. The SMS should include a clear definition of responsibility for each position in the organisation, identification of safety related positions/personnel and integration of safety functions into and across the organization.

By considering safety at the conception of business goals and decisions, safety will no longer be the "stumbling block" it is often considered to be during later stages of progress. Furthermore, the techniques used to assess safety risk will then be used in the broader context to assess project risk and/or assess different design options and can, therefore, be used to aid the decision-making process for business decisions.

Communication. Communication issues and organisational design have had a significant role in a number of major incidents and must be addressed within the SMS. Elements of organisational design and working methods can unwittingly create communication barriers (for example, "friendly" competition between departments) resulting in breakdown and failure to pass on potentially critical information. The fine details of organisational design should, therefore, be considered carefully and reviewed as part of the SMS and formal and informal communication channels identified and developed within departments, across departments and with associated or external organizations.

Decision-Making Processes. A clear definition of the decision-making process where safety issues are involved is needed and should be integrated with other decision-making and business functions (operators should not be placed in a position to resolve conflicts between safety and other performance goals).

Risk Assessment, Reduction and Control. A framework with strategy and methods used to assess, reduce and control identified risks must be clearly defined in an SMS, even if the risks are considered tolerable or acceptable. Without methods and procedures for assessing risk, there will be no benchmark with which to measure improvements achieved by risk reduction and control measures over time. It is important to ensure that such a framework is adaptable, flexible and comprehensive so that the following aspects are considered:

- **Effort**. The amount of effort and detail expended in risk assessment, reduction and control should be commensurate with the scale of consequence or risk likely to be encountered. For example, a qualitative technique may be used initially but, if found to be necessary, more detailed or quantitative techniques can be applied.
- **Output**. Output format required from the process of risk assessment is provided and reviewed to ensure that it can be put to greatest use (e.g., definition of risk categories and prioritisation).
- **Interaction**. An integrated approach needs to be taken that considers individual processes or items of equipment as well as the whole system, sub-systems, interactions and interfaces. Where humans will interact, human factors should be considered in appropriate depth, remembering that as much as 80 percent of failures can be human related.
- **Integration**. Disciplines other than safety need to be consulted and integrated into the process to ensure that constraints and other relevant issues known to designers, operators, maintenance staff, managers, etc. are included in the risk management equation.
- **Assessment**. A combination of top-down and bottom-up risk assessment techniques should be used. It is recognised that use of a single technique will identify most, but not all hazards contributing towards risk. A combination of two complementary techniques can be expected to identify 95 percent of hazards (including all major hazards) if applied correctly. A top-down approach considers a defined undesirable consequence to identify the different mechanisms that can lead to it. A bottom-up approach considers failures of individual components to identify if subsequent events can result in escalation to a hazardous incident.

Data Collection, Review and Feedback. These are key elements of a good SMS. Systems of data collection are needed for performance measurement (safety), incident/near incident information and trend analysis. Systems for feedback of risk management and review data into the organisation must be in place for continual improvement of the SMS and safety performance. This step ensures that the SMS changes and adapts to the ongoing development of an organisation over time and maintains an effective approach to risk management to achieve levels of risk as low as reasonably practicable.

Audit Systems. These systems are necessary to ensure an SMS performs as intended and to reinforce management commitment to safety.

An Illustration: Mechanical and Electrical Risk

As an example of comprehensive risk assessment, the assessment of mechanical and electrical risk is a well established field with a selection of mature techniques and methodologies available for identifying hazards and assessing associated risk (e.g., HAZOP, failure modes and effects criticality analysis (FMECA), fault and event tree analysis, etc.). As stated above, however, whole systems must be assessed rather than items of equipment or processes in isolation. Therefore, the techniques used to assess mechanical and electrical risk must be integrated with techniques used to assess the risks arising from interface hazards, human factors and other elements historically omitted from risk assessments, such as software and programmable electronic systems (PES).

Risk assessment techniques for human factors and software/PES are less well established than those for mechanical and electrical risk, although there are mature techniques available in human reliability assessment (e.g., task analysis, human error assessment and reduction technique, and the technique for human error rate prediction) and maturing techniques in software/PES assessment. It is crucial that significantly greater effort is placed in the assessment of these risks because:

- Human error is accepted as a major contribution towards risk, including management and operator failings.
- Software and PES are already used extensively in control systems and are being used increasingly to provide safety functions in operating systems.
- Greater use of such risk assessment techniques will accelerate their development and validation and allow collection of important failure-rate information that can be used by the techniques and in the respective industry.

The assessment of interface risks can generally be achieved by adapting a risk assessment technique to a given interface, or by a combination of techniques to address each element of a given interface (e.g. operator, management, mechanical, electrical, PES and/or external conditions).

Safety Culture

Organisational culture is a complex combination of attitudes, beliefs, values, opinions, motivations, rituals, habitual responses, etc. that characterise the ways in which individuals undertake activities in an organisation. Safety culture refers to the aspects of organisational culture that have an effect on safety (for example, attitudes to safety and perception of risk). Safety culture is, therefore, not a definite or well defined entity. It depends largely upon the prevailing attitudes towards safety/risk and the motivations of behaviors that can impact risk.

Attitudes and motives cannot simply be changed overnight by a change in policy or management system, so although an effective SMS is considered to be a necessary measure in achieving a good safety culture, it is not sufficient. Development of a good safety culture requires all individuals to accept the importance of safety, share responsibility for safety within the organisation and actively strive to achieve organisational safety goals. Such a culture is likely

(continued on the following page)

to be achieved only by concentrating on a long-term learning approach towards safety and risk.

It is essential that management accepts and promotes safety as an issue of prime importance. If those in managerial positions do not back a commitment to safety, it is unlikely that the remainder of the organisation will respect safety, so the standards of organisational safety and level of risk cannot be expected to improve.

Not only should management become more involved in the active reinforcement of safety principles, staff at all levels of an organisation should be encouraged to become involved through, for example, information dissemination, consultation and training. By involving everyone in an organisation, responsibility for safety and risk is shared (but should not be delegated), encouraging a positive attitude towards ensuring safe systems and operation. ◆

A brief description of Peter Johnson's background appears on page 9.