

**World Bank Approach
to Safety Control and Risk Management
of Industrial Facilities**

by Roger J. Batstone

Paper to be presented at the International Forum on Safety Control and Risk Management, Yokohama International Conference Center, January 25, 26, 1989.*

As part of the international concern for the prevention of disasters such as the one that occurred in Bhopal, India, in December 1984, the World Bank's Office of Environmental and Scientific Affairs in Washington, D.C., recognized the need for a radical new approach to major hazard accident identification, prevention and mitigation in developing countries. The result was the publication of a new set of guidelines in December 1984 to help prevent such incidents.

As a funder of industrial projects throughout the developing countries, the World Bank has a great interest in protecting these investments, as well as people and the environment in the neighborhood of the plant site. It is a well-proven fact in industry that pollution prevention pays even in the absence of government regulations. In addition, it can be shown that major hazard accident prevention also pays. This new approach is leading to the development of less hazardous processes and reduced inventories of hazardous materials in process and storage, as well as to other measures to reduce the potential consequences of a major accident. It also led the World Bank to initiate guidelines and policies for projects it funds in the developing nations.

The World Bank Guidelines for Identifying, Analyzing, and Controlling Major Hazard Installations in Developing Countries accomplish three things. First, they make sure that people in control of operations that involve dangerous, explosive, flammable, and acutely toxic substances have identified in fine detail the dangers and potential consequences of major accidents in those operations. Second, they ensure that plant personnel take every possible measure to prevent any accidents from occurring through changes in plant design, layout and siting. Third, when accidents do occur, plant operators and local authorities will know how to control and minimize the consequences.

The origins of the approach outlined in the guidelines date back to the 1970s. Following the lead of chemical companies in Europe in the wake of major disasters in Flixborough, England, and Seveso, Italy, the European Economic Community developed the Seveso Directive in 1982 as a legislative approach to major hazard accident prevention. Following Bhopal, at the end of the December 1984, the Bank issued preliminary

* The World Bank does not accept responsibility for the views expressed herein, which are those of the authors and should not be attributed to the World Bank or to its' affiliated organizations.

guidelines based on this directive which applied generally to industrial processes and to the storage and transport of hazardous material, but not to the nuclear industry, to mining or other extractive operations, or to licensed hazardous waste disposal sites.

During the first half of 1985 experience on applying the guidelines to some twenty projects proved that they could be further simplified and also showed the need for a 'Manual of Industrial Hazard Assessment Techniques' to guide plant designers in the methods of major hazard assessment. Previously, only specialized experts in the field of hazard analysis had access to this technology. With the publication of the World Bank Manual in October 1985 and its widespread distribution worldwide, the technology of major hazard identification assessment and prevention has taken on a new impetus. Major accident hazard assessment and control goes much further than the requirements of conventional safety and loss prevention as routinely practiced in the chemical and petroleum industry. Many companies in these industries are unaware of this fact and, therefore, do not realize the potential that exists for reducing process and storage hazards. While it is less costly to make these adjustments at the design stage of a project, much can be done after a plant has been constructed to reduce major hazard accidents.

In the final guidelines, the Bank decided not to rely solely on probabilistic risk assessment (PRA) techniques prevalent in the United States nuclear industry or in the European chemical industry, finding that these techniques often ignore too many unknown factors, particularly, management, organizational and cultural factors which vary widely between different companies and cultures. Major hazard accidents occur much more frequently than would be indicated by the results of the typical PRA type assessments, and may lead to dangerous sense of complacency which further increases the risk. As a follow-up to a hazard analysis, PRA methods have an important role to play in deciding between alternative designs and control schemes to further reduce the risk of an accidental release.

In order to be better able to advise companies and governments in developing countries on these management, organizational and cultural factors which are critical concerns in preventing major accidents where major hazards cannot be eliminated, the World Bank is jointly sponsoring with the Danish, Swedish, Dutch and Australian governments a series of four workshops on Safety Control and Risk Management. An unbiased analysis of failures in organizational systems including those which lead to major accidents shows that at least 80% of the failures occur in the management/organizational hierarchy and less than 20% can be attributed to failures at the operator/equipment level. Many of these failures have occurred and are latent in the system prior to the accident. Findings and conclusions from the first workshop held in Washington during October 1988 are discussed in a later section.

In carrying out a major hazard analysis using the Bank's manual, the process starts with identification of a failure case scenario. This could be anything from the rupture of a pipeline to the failure of a process vessel or an uncontrollable release of a toxic chemical through an emergency or other atmospheric vent. The program leads the analyst through a series of calculations to estimate the acutely toxic effects at varying distances from the point of release, provides the time/concentration profile of the toxic gas cloud as it disperses downwind and estimates fire radiation effects, extent of flash fires, explosion damage, and fragment damage under critical meteorological conditions. These calculations are repeated for the full range of failure cases. All the information is plotted on a detailed map of the plant and the surrounding area, noting particularly sensitive danger areas such as schools, homes, and hospitals near the plant.

Following identification and quantification of the hazards, the manual suggests a number of corrective measures that can be taken. One example could be to investigate possible "knock-on" events in which a smaller accident could trigger a major one, such as a small fire which causes a vessel storing a toxic material to leak, producing a toxic vapor cloud. For such cases the manual suggests possible protective measures including fire and blast wall protection, remotely operated shut-off devices, equipment layout changes, process changes and so on to prevent such effects.

Another area of corrective measures aims to reduce the consequences of accidents by reducing the amount of hazardous material at the plant, by eliminating the hazardous material altogether, or by generating it as an intermediate through a new or modified process. One project the Bank has funded, in fact, involves a key improvement on the process Union Carbide was using in Bhopal. In the new procedure, methyl isocyanate (MIC) is not stored: rather, it is continuously manufactured and fed to further reactions in the process without intermediate storage. The maximum quantity of MIC in process at any time is four kilograms which would have minimal impact outside of the plant boundary in the event of an accidental release. By shutting off the heat supply to the MIC reactor, the formation of MIC can be stopped immediately. As greater attention is given to preventing major hazard accidents, further process developments along these lines will occur in the production and use of other hazardous materials.

The third area of emphasis aims to limit the impact in surrounding communities of major accidents which do occur. Possible measures here include providing escape routes, emergency and evacuation planning, public alert systems, modifying the siting of proposed plants and setting aside

safety buffer zones around hazardous installations. The events of Bhopal and in many other accidents throughout the world has led to calls for more education in communities of what chemicals and what processes are being used in their midst. In order to cover this aspect, the World Bank program requires companies handling and storing hazardous chemicals to develop on- and off-site emergency plans and to coordinate these plans with those of the responsible local authority, who are encouraged to inform and involve the local community.

For several reasons, the Bank's efforts have focused mainly on preventing hazards through the actual design rather than on emergency procedures to reduce the impact of a major hazard accident once it has occurred. Although there isn't any real difficulty in performing a hazard assessment on a plant at the design stage or even on one that is already operating, it requires careful work involving experts in various areas of processing, engineering, construction, operation and safety. The plant designers, contractors and operators have the specialized "know-how" that is required for this work. The World Bank does not have this specialized expertise, but by requiring developers to focus on this issue and to take mitigating measures to prevent major accidents hazards, the objectives of the guidelines are realized. In order to utilize its' technical resources most effectively, the Bank's safety and process experts review these hazard assessments and in some cases may require additional safety measures.

The Bank's industrial loan and project officers are very much involved in applying this new approach to major accident prevention. Bhopal has made all concerned keenly conscious of potential disasters especially in developing countries where training, maintenance, safety awareness and cultural differences increase the risk and often the consequences of accidental releases. For example, in one proposal examined under the guidelines, a company producing and storing large quantities of refrigerated ammonia was required to redesign its expansion plans based on the result of a hazard assessment. The firm had been operating under a false sense of security, since it was their impression that the prevailing wind was almost always seaward away from the surrounding community. While this was true during the daytime, at nighttime, calm inversion conditions prevailed, when a dense toxic gas cloud would spread towards nearby housing. Therefore, the plant presented a much higher risk to the surrounding community than the company had anticipated. High wall dyking around the storage vessels, as well as other safety measures, were required in this case to reduce the consequences of an accidental spillage of ammonia from the large storage facility.

The first World Bank workshop on Safety Control and Risk Management in October produced some substantial break throughs in communication between engineers/technical scientists and the social scientists dealing with the human software of the system including its management and organization and "hands-on" operators. In a way it has redefined the role of the engineer/technologist in safety control and risk management and if they can make the adjustment will draw them in a more productive and iterative way into the management decision-making process.

A clear conclusion of the workshop is that the conventional safety control and risk management approach in complex technological systems needs a fundamental reappraisal if major accidents are to be prevented or reduced. A number of elements of a new approach were identified at the workshop and are discussed below:

- i) The dominant probabilistic bottom-up safety approach of the engineers/technologists has many limitations and inadequacies/constraints which must be recognized and its use constrained to clearly defined areas of application. Other comparable deterministic methodologies which are also in use should similarly be evaluated for areas of application and efficacy.
- ii) These methodologies provide a useful comparison of the risk of different designs, and design improvements, and operational conditions, but the trend is towards on-line safety assessment systems to assist engineer/operators in on-line control of safety and to improve communications with management decision makers.
- iii) The engineering design conditions for safety of the system must be made explicit to decision makers and measurement and communication systems improved to warn decision makers when the system is approaching the safety boundary conditions, as well as the consequences of violating these conditions. For example, engineers working on the Challenger launch system prior to the disaster were in no doubt that before the launch the system was violating the safety boundary conditions (e.g., effect of very low temperature on the O ring seals, etc.). Their design criteria was violated and confirmed from evidence of previous low temperature launches. However, the decision-making process in NASA was inadequate to process such data and maintain the system within the reasonably well defined safety boundary conditions. As a result over two billion dollars has been spent on hardware/equipment modification to extend the boundary of the safety domain, with much less attention given to the decision-making management and organizational processes required to maintain the system even within the expanded safety domain. If NASA had recognized these deficiencies prior to the fatal launch these deficiencies could have been corrected at a very small

fraction of the cost of the hardware changes made subsequent to the disaster -- not taking into account the lost "productivity," credibility, etc.

- iv) From the above it is seen that the vital role of the engineer/technologist is to design, construct and maintain safe technological systems according to the constraints of current knowledge and also to make the current knowledge of boundary condition for safe operation sufficiently explicit or at least to identify any uncertainties and to communicate this information to decision makers.
- v) In addition to the identifiable failures which occur in such systems other "unidentifiable" failures are also present (called "resident pathogens" by J. Reason or "sleepy nonlinearities" by P. Kugler). As the safety boundary conditions are probed these failures many become more evident, if the system is being continuously monitored by trained specialists. As systems become more tightly coupled and more complex the scale of uncertainty increases and the boundaries of the safety domain become more fuzzy. However, some comfort can be drawn from the fact that prior to all major accidents there have been prewarnings of impending disaster which have unfortunately been undetected by the system, or have not been acted upon by management. P. Kugler work shows that with appropriate monitoring of the system these "undetected" system failures can be identified and even the type of failures and time to failure predicted as the boundary of the safety domain is approached.
- vi) For maximum productivity and efficiency, decision makers of high tech systems will frequently be operating close to and even probing the boundaries of the safety domain (e.g., the Challenger disaster, Spirit of Free Enterprise, etc.)
- vii) Thus the roles of the engineer/technologist and other specialists become clearer as our understanding of their important functions can be best integrated into the decision-making process, and it is recognized that constant system optimization requires probing the boundary of the safety domain in an effectively functioning communications and decision-making process. In an increasingly competitive international environment more and more companies are being forced to adopt such a model.
- viii) It also became clear at the workshop that the role of the human factors specialists is expanding from considering "operator error, and the operator/equipment interface into areas of management decision-making, communication and control.

- ix) However, a major challenge is to put in place management/organizational systems, which can adapt to these challenges and provide the continuing incentives to ensure high reliability of increasingly more sophisticated organizational systems.
- x) There is a need to identify high reliability adaptive management/organizational models, their characteristics, and replicability for various high tech systems. For example, the use of quality control circles after the Japanese management system approach, adaptive systems which form to respond to emergency and crisis situations, or some adaptive aspects of military organizations, air traffic control, etc.
- xi) For the first time in the field of safety control and risk management, a serious consideration was given to the important cultural implications of technology transfer, and management/organizational system design for different cultural environments. While the issue has hardly surfaced to date it is interesting to note that since the workshop two groups of researchers have identified promising approaches to incorporate these factors into the management/organizational framework.
- xii) As industrial expansion is occurring much more rapidly in LDC's the cultural variables are assuming an even greater importance.
- xiii) Examples of successful adaptation of organizations to incorporate operators/maintenance people of different cultures into high reliability technological systems have been identified and will prove to be useful models for more wide-spread application.
- xiv) A number of times experts indicated the frequent failure of the "quick-fix" reorganizational approach to resolving failures in organizational systems.
- xv) In a "macho" management system, common to many industries, safety is usually seen as a "whimp" factor by management and given low priority; not recognizing as Peter Benton pointed out the important role safety can play in achieving the high productivity/efficiency objectives of the company (see vii).
- xvi) Over emphasis on short-term management goals with a narrow focus on safety seems to be a recipe for failure.
- xvii) A refocus by researchers on the essential elements of successful organizational systems will be more productive than focusing on organizational systems that fail.

- xviii) The "trust" factor is an important element in maintaining reliable organizational systems (i.e., trust between humans themselves and the machine they operate).
- xix) Related to this factor is the important element of information flow and effective communication between and within all levels of the organization and the incentives which are set up to encourage this information/communication flow. (For example, incentives given to operators to report failures on the systems and incentives to encourage employees to take responsibility for their job performance. It is found that punishment of operator failure/errors is a disincentive to communication. Poor management/laborer relation has a similar effect.) Incentives for reporting of "near misses" is a vital element in the operation of a high reliability organizations.
- xx) Peter Benton gave a good example of a highly successful international banking company working at the boundaries of the safety domain and compared it with an old fashioned conservative operation operating well within the safety boundary but with very low financial returns.
- xxi) In addition to identifying priority research areas the next two workshops should focus on the outline of a policy guidelines for high reliability organizations and a guideline identifying the essential elements of such organizations, within a multi-cultural context, and including incentives required to maintain organizations in such a mode.
- xxii) During the next two workshops increased attention will also be given to regulations, macro economies, institutional, legal and other constraints and incentives in the performance of high reliability organization in order to develop outline policy guidelines for governments and multi-lateral lending institutions such as the World Bank.