CRITICAL ISSUES IN INDUSTRIAL RISK MANAGEMENT

Jens Rasmussen

ABSTRACT

Modern large-scale industrial systems require special precautions for safe operation and systematic risk analysis is frequently used during system design. The paper reviews a number of problems presently found in the use of risk analysis as a basis for effective risk management. There is a need for more explicit formulation of the preconditions of safe operation and for better communication to the operating organization. Operation in a competitive environment requires endless adaptation and optimization by management and, consequently, visible indicators of the boundaries of safe conditions are necessary. The paper adopts an integrated system point of view in order to identify cross-disciplinary issues involving social and management sciences as well as engineering.

INTRODUCTION

The technological development during the recent decades has focused the public attention on the safety of industrial installations. At the same time, changing technology makes it necessary to find new means for control of safety in large-scale industrial systems. This is the case, not only for protection of people and environment, but also for the security of financial investments.

There is a general trend toward large-scale systems, not only for industrial production units, aerospace systems, and air traffic control, but also for consumer goods distribution systems, information systems, and systems for financial operations. This trend causes a large potential for loss and damage in case of technical faults in equipment and of human errors made during operation and maintenance. It is, therefore, no longer acceptable that single component failures or human errors can release a chain of events leading to accidents and losses and a design philosophy of 'defence-in-depth' has evolved.

This philosophy implies that systems have numerous lines of defence such as protective functions, barriers against fault propagation, etc., which can serve to terminate accidental chains of events before serious loss and damage can occur. In addition, stand-by equipment is installed and is supposed to take over when operating systems fail. A disturbance, e.g., a fault or human error, can then only evolve into an accident when it coincides with the presence of other faults that make the safety measures inactive. The philosophy in this way implies that a very low probability of major losses can be obtained if faults are causally independent, even when the frequency of errors and faults individually is high enough to be known empirically.

This development has been very visible to the public, in particular with respect to the safety of large-scale industrial process plant such as nuclear power plants and chemical plants. For sake of clarity, the discussion in the following sections will focus on the safety problems of such installations because the formal methods of analysis are particularly well developed for this application. It is possible, however, to generalize also to other application areas, and recently events, such as the stock market plunge during October 87, illustrate that other system-related safety problems call for closer analysis. This aspect will be briefly discussed in a subsequent section.

CONTROL OF INDUSTRIAL SAFETY

The trend towards large-scale industrial process plants and the related defence-in-depth design practice have immediately two important implications. One is that the actual level of safety cannot be directly controlled from empirical evidence. For hazardous large scale installations, design cannot be based on experience gained from accidents, as it has been the case for accidents in minor separate systems when, for instance, considering work and traffic safety. The days of extensive pilot plant tests for demonstration of the feasibility of a design is over and safety target has to be assessed by analytical means based on empirical data from incidents and near misses, i.e., data on individual, simple faults and errors. Consequently, for industrial process plants, large efforts have been spent on developing methods for probabilistic risk analysis.

Another consequence is the fallacy of the defence-in-depth practice unless special management precautions are taken. Exactly because of the application of this design practice, systems will not respond actively to the individual faults and errors and recovery from latent failed states calls for a special care by the operations management.

Technological Risk Analysis

In a probabilistic risk analysis, a model of the plant and its function is used to predict the propagation through the system of the combined effects of different simultaneous faults and errors. For the unacceptable chains of events leading to accidents, the probability is estimated from empirical data collected for the individual errors and faults.

Typically, however, such risk analysis is considered only for the initial acceptance of a particular plant design. It is generally not fully realized that a risk analysis is only a theoretical construct relating a plant model and a number of assumptions concerning its operation and maintenance to a risk figure. This fact implies that after acceptance of a plant on the basis of the calculated risk, the model and assumptions underlying the risk analysis should be considered to be specifications of the preconditions for safe operation which, in turn, should be carefully monitored by the operating organization through the entire plant life (Rasmussen and Pedersen, 1984).

This use of a risk analysis raises some important problems: Risk analysis and, in particular, the underlying hazard identification are, at present, an art rather than a systematic science. We have stringent, systematic methods for analyzing specific accidental courses of events. However, identification of the hazards to analyze, in particular related to the influence of human activities during operation, maintenance and plants management, to a large extent depends upon the experience and creativity of the analyst. It is, therefore, difficult to make explicit the strategy used for hazard identification, the model of the system and its operating staff used for analysis, and the assumptions made regarding its operating conditions. In addition, the documentation of a risk analysis today is not designed for use during operations and maintenance planning and is not accessible for practical operations management.

The Fallacy of the Defence in Depth Philosophy

Another important implication of the very nature of the 'defence in depth' design philosophy is that the system very often does not respond actively to single faults. Consequently, many errors and faults made by the staff and maintenance personnel do not directly reveal themselves by functional response from the system. Humans can operate with an extremely high level of reliability in a dynamic environment when slips and mistakes have immediately visible effects and can be corrected. Survival when driving through Paris during rush hours depends on this fact.

Compare this to working in a system designed according to the defence in depth principle, where several independent events have to coincide before the systems responds by visible changes in behavior. Violation of safety preconditions during work on the system probably will not result in immediate functional response, and latent effects of erroneous acts can therefore be left in the system. When such errors are allowed to be present in a system over longer period of time, the probability of coincidence of the multiple faults necessary for release of an accident is drastically increased. Analyses of major accidents frequently show that the basic safety of the systems has eroded due to latent errors. A more significant contribution to safety can be expected from efforts to decrease the duration of latent errors, than from measures to decrease their basic frequency.

Recovery from latent errors in a system designed according to the defence-in-depth principle, however, requires special management structures and functions. It is necessary to maintain a reliable, empirical control of the possible existence of latent violations of safety preconditions as specified by a risk analysis. Present organization and management forms in industry probably still reflect a tradition which has evolved through a period when safety could be controlled directly and empirically. The new requirements for safety control based on risk analyses have not yet had the necessary influence on the predominant organizational philosophy.

Learning and Adaptation by Individuals and Organizations

The problem of violation of the preconditions for safe operation is increased by the fact that both individuals and organizations continuously are striving to optimize performance in terms of functionality, effort, and economic pay-off. At the individual level, development of skill and know-how depends on experiments and opportunity for changes in work procedures. At the organizational level, survival in a competitive environment presupposes optimization of operation, rationalization of work procedures, and modification of production process and equipment. This optimization will be guided by more or less directly observable evidence.

In contrast, the limits of acceptable optimization as they are defined by the preconditions for safe operation, as mentioned, are not directly visible when a system is based on the defence-in-depth principle. Correspondingly, analyses of industrial accidents typically indicate that pressure from functional or economic adaptation leads to a gradual erosion of the individual redundant safety preconditions until the time comes when violation of just one more precondition or a single component fault will release an accident. (Perrow, 1986, Rasmussen, 1987).

In the efforts to optimize operational reliability, it is frequently argued that high plant availability and smooth production are good indicators of plant safety (Atomic Industrial Forum, 1986): "It is an indirect index of safety, because poor availability is essentially related with defective equipment, operations, or regulation, and it has direct impact on economics." It is, however, a necessary but not sufficient condition for safety, and programs to increase availability should include explicit efforts to create also 'sufficient' safety indices.

This tendency of an organization to optimize and only to take into account the immediately visible empirical evidence can explain why accidents still can happen in spite of the large efforts to develop guidelines for risk management (see for instance Smith, 1987 and Cramer, 1987). Programs and organizations for risk management separate from the operational line functions will have no visible results, if they are successful, and will be the first victims of the organizations adaptation to economic pressures. The only realistic solution to this problem can very well be to introduce visible indicators of the performance of the risk management efforts. This will require that the current margin to the boundaries of the accepted risk level is made visible to decision makers. In addition, it should be considered that operation based on visible limits to the boundaries of accepted safety can have a positive influence on operations economy compared to 'blind' operation based on static and over-cautious safety factors.

In conclusion, operation of large scale plants is subject to optimizing, exploring behavior of individuals and organizations. Recent research, furthermore, indicates clearly that the organic interaction among members of an organization leading to high reliability depends on adaptive self-organization (LaPorte et al. 1987). Therefore, organizational learning and adaptation and the implied modification of procedures neither can, nor should be avoided and safety will depend on measures to support recovery from errors rather than on measures to decrease their frequency. Therefore, it is mandatory to make the limits of acceptable changes clearly visible at all levels in the organization.

The strive of organizations to optimize performance will depend on subjective values in addition to the economic and functional criteria. Analysis of the criteria which are in practise controlling adaptation and optimization is important. In addition the dependence of such criteria upon cultural differences will be important for generalization. It is important to realize that it is not only a question of more or less developed countries, but a general question of differences between regions and countries also in the technologically most developed part of the world. Implicit in the design of highly structured systems such as process plants is a number of assumptions about work allocation and training which can differ even among technically sophisticated countries.

Communicating Design Basis to Operations Staff

The conclusion of this discussion is that improvement of the safety of large scale industrial operations depends on more efficient means for transfer of information from plant design and risk analysis to the operating organization. It should be seriously considered, however, that operations management cannot read the safety report every time a decision is made. Consequently, we need decision support systems based on information from plant design and risk analysis which are able to alert decision makers when safety preconditions are violated and to supply a safety 'index' indicating the current level of safety.

In this context, the present development of general management and planning tools based on modern information technology is important. Tools are being developed for planning and book-keeping purposes within plant operation, staffing, and maintenance. Computer aided tools are introduced for design of plants and control systems, and methods for automated, computer-based risk analysis are emerging (Fussell, 1987, Amendola, 1984). A full-scale, probabilistic risk analysis for a specific plant is a very expensive project and the development of safety control tools should be considered also for plants for which a detailed risk analysis is not available. The design practice which have evolved for chemical installations results in a rather uniform, generic structure of plants within the same process category. Consequently, the first step in the direction of a systematic use of risk analysis in plant operation and audit could be the use of a prototypical 'default' risk analysis covering the basic features of a category of process plants. Such prototypical risk analyses could then be the adapted to the peculiarities of a particular plant with a reasonable effort.

EMERGENCY MANAGEMENT

The discussion so far has been focused on the control of safety during normal operation and use of systems. One important conclusion has been that control of safety is an important task of the operating organization itself, not a task for a separate safety organization. The tasks of the different levels have different time horizons. While the lower levels including the operating staff is involved in direct 'on-line control' of a dynamical system, the higher levels of management are typically involved in planning tasks of longer time frames. Another conclusion has been the need for better communication between design and risk analysis and the operation management. Similar conclusions can be drawn with respect to the emergency management which is required when an accident has occurred.

Organizations for Emergency Management

After an accident, the requirements for actions at the higher levels of management typically will change from strategical planning to tactical decision making. In order to control this shift to unfamiliar work conditions, special organizations are typically planned and normative emergency procedures are prescribed. Such measures are also intended to coordinate the co-operation between operations management and outside agencies and support systems. The essence of the discussion of organizational learning is that the actual, effective organization evolve from the formal organization through work. It can therefore be expected that reliance on the normal work organization through also periods of emergencies will be better than establishment of a special organization controlled (in a feedforward mode) by pre-planned procedures (Dynes, 1985).

Decision Support Systems

The task domain of emergency management has an unstructured nature and does not exist until an accident has happened. Furthermore, two different parts of the domain can be identified. One represents information about the potential source of accidents, i.e., information that can be supplied from design, operation, and risk analysis of the system in question.

Another domain represents the properties of resources available for emergency control after the accident has been initiated, i.e., services such as fire brigades, hospitals, transport facilities, etc. together with geographic and demographic information from the neighborhood. The information retrieval aspect of the decision task appears to be very important for emergency management. Large amount of information about very different aspects such as geographical features, meteorological data, road conditions and traffic data, physical and chemical properties of plants and substances, resources of medical centers, may be needed for advice by an accident manager. This information will be supplied by many different sources and, typically, not in formats suited for a stressed decision maker needing procedural advice on short notice. Database formats and retrieval tools therefore become central issues of decision support system design.

COMMUNICATION OF RISK CONCEPTS TO DECISION MAKERS

In addition to the problems caused for risk managers by the lack of explicit formulation and presentation of the assumptions implied in risk analysis, the very nature of analyses of causal chains makes it difficult the communicate results of risk analyses to non-technical people such as managers and decision makers.

Two kinds of description are used in engineering analysis. One is based on the physical sciences and represents the properties of system in terms of quantitative relations among measured variables. This representation is possible for relationships which can be considered 'practically isolated' from the complexity of the real world. The quantitative representation is particularly well suited for the analysis of optimal conditions and theoretical limits of physical processes in a technical system which, by its very design, carefully separates physical processes from the complexity of the outside world.

In accident analysis, however, technical systems can no longer be considered as having 'practically isolated' functions, well contained by system boundaries. Accidents happen when system boundaries break down. In this case, the preconditions for relational, mathematical analysis of system function also break down and formal methods are replaced by analyses of causal chains of events. Causal analysis depends on a description of the behavior of a system in terms of objects which interact in events. This kind of description is basically different from the quantitative, functionally relationship between measured variables expressed in mathematical equations.

It is very important to realize that causal analysis is useful for this purpose because it depends on the identification of objects and events which cannot be objectively defined. The behavior of the complex, real world is a continuous, dynamic flow which can only be explained in causal terms after decomposition into discrete events. Events and objects are formed from a categorization of human observations and experiences. Perception of occurrences as events in causal connection is not based on categories which are defined by lists of objective attributes but on categories which are identified by typical examples, by prototypes. This is the case for objects as well as for events. Everybody knows perfectly well what 'a cup' is. To define it objectively by a list of attributes that separates cups from jars, vases and bowls is no trivial problem and has been met in many attempts to design computer programs for picture analysis. The problem is, that to be 'a cup' is not an feature of the isolated object but depends on the context of human experience and needs. The identification of events in the same way depends on the relationship in which they appear in a causal statement.

An example: "the short-circuit caused the fire in the house." This statement in fact only interrelates the two prototypes: the kind of short-circuit that can cause fire in that kind of house. The explanation that the short-circuit caused a fire may be immediately accepted by an audience from a region where open wiring and wooden houses are commonplace, though not in a region where brick houses are the more usual kind. If not accepted, search for more information is necessary. Short-circuits normally blow fuses, therefore more analysis of the conditions present in the electric circuit is necessary; together with more information on the path of the fire from the wiring to the house. A path of unusually flammable material was probably present. In addition, an explanation of the short-circuit - its cause - may be needed. The explanation depends on a decomposition and search for unusual conditions and events. The normal and usual conditions will be taken for granted being implicit in the intuitive frame of reference. In causal explanations, the level of decomposition needed to make it understood and accepted depend entirely on the intuitive background of the intended audience.

Therefore, if a causal statement is not accepted, formal logical analysis and deduction will not help, instead further search and decomposition are necessary until a level is found where the prototypes and relations match intuition. In effect, without special precautions, causal explanations are only suited to communicate among individuals who share prototypical definitions of objects and events because they have similar experience and, therefore, common intuition. If this is not the case, it will be easy to give counter-examples which can not easily be falsified.

Since no two accidents will be identical and because it is impossible to analyze all possible causes separately, accident analysis depends on categories of causes, events, and consequences. Technical systems are particularly well suited for analysis in terms of causal chains due to their well structured and generally stable anatomy which will guide the course of events. This is the basis for the rather well-defined completeness of hazard identification methods like HAZOP which will cover all causal paths in the pipe-and-instrumentation diagram.

It is much more difficult to take the human influence on accidents into account. Objects, then, include mental concepts, events include decisions and actions, and the course of events will depend on human communication and mobility. In this case, great care is necessary for satisfactory documentation of the context in which the causal texture is identified and the paths selected, together with the stop-rules used for termination of the search. It is very difficult to state explicitly the completeness of a causal analysis including human activities.

The defence-in-depth design philosophy also creates problems for the communication of causal analysis to groups with different experience and background. In a system designed according to this philosophy, many errors and faults made by the operating staff and maintenance personnel do not directly reveal themselves by functional response from the system. Adaptation to task requirements which are very reasonable in the immediate context can therefore violate safety features without visible effect for the actor. It is easy, after the fact, to identify unacceptable violations of a design-in-depth design concept. Seen separately and in the situation, however, the violations can be reasonable and, in fact, necessary for the flow of work. What should be included in the management risk analysis is the possible coincidence, not only the individual act. Risk management, therefore, depends on an overview of the causal structure of major risks, not only on the monitoring of the individual work situations.

In this kind of system, it is mandatory not only that the causal structure underlying the designers' analyses are made explicit but also that it is understood and accepted by the operating staff and management which typically will have a very different experience and intuition than designers. The dependence of causal analysis on shared prototypes and frame of reference and the related problem of communication between different professions is now becoming an important problem for practical risk management in hazardous industries.

CONCLUSION

The basic conclusion is that a number of important safety issues are related to the properties of the integrated system involved in control of safety. Most of these problems require an inter-disciplinary co-operation between basic research in different academic disciplines and field studies in different application domains. Typically, such cross disciplinary studies are more difficult to have funded and organized than separate studies within an accepted professional paradigm because of the teaching obligations of university faculties and the similarly focused interest of research councils. For improvement of the safety of modern, large-scale systems, it is mandatory that safety is considered a control problem and that research is approached from an integrated systems point of view.

REFERENCES

Amendola A., (1984). DYLAM-1 A Software Package for Event Sequence and Consequence Spectrum Methodology. EUR 9224 EN. Ispra: EEC-
Joint Research Center.

Atomic Industrial Forum (1986): Measures for Improving Nuclear Power Plant Operational Performance and Availability. Bethesda, MD: September 1986.

Cramer, J. J. (1987): Structured Risk Management Programs. Presented at the International Symposium on Safety and Risk Management, Kanagawa University, Yokohama, Japan, November 1987.

Dynes, R. D. (1985): Organized Behavior in Disaster. Book and Monograph Series, Disaster Research Center, University of Delaware.

Fussell, J. B. (1987): Prisim - A Computer Program that Enhances Operational Safety. Presented at the Post-Smirt Workshop on Accident Sequence Modelling: Human Actions, System Response, and Intelligent Decision Support. Munich, August 1987.

La Porte, T. R., Rochlin, G. I. and Roberts, K. H. (1987): The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea. Private communication, to be published.

Perrow, C. (1986): Risky Systems: Inducing and Avoiding Errors. Private communication, to be published.

Rasmussen, J.: Approaches to the Control of the Effects of Human Error on Chemical Plant Safety. Invited paper for the International Symposium on Preventing Major Chemical Accidents. February 1987, American Institute of Chemical Engineers.

Rasmussen, J. and O. M. Pedersen: Human Factors in Probabilistic Risk Analysis and in Risk Management. In: Operational Safety of Nuclear Power Plants. Vol. 1, pp. 181-194, IAEA, Wien, 1984.

Smith, R. A. (1987): Chemical Plant Safety and Loss Prevention. Presented at the International Symposium on Safety and Risk Management, Kanagawa University, Yokohama, Japan, November 1987.

Waldrop, M. M. (1987). Computers Amplify Black Monday. Science, Vol. 238, p. 602-604