Bernhard Wilpert[1]

5. Management as risk facor in high hazard systems

Abstract

The paper discusses a frequently neglected topic in safety science: the influence of managerial behavior on safety and reliability of complex high-hazard risk organizations. Failure inducing factors may often be hidden in the organization far away in terms of time and space from actual accident trigger event. Direct managerial actions (e.g. personnel decision, deficient procedures, lack of control) as well as indirect managerial impacts (e.g. managerial philosophy, leadership style, safety culture) are identified as important ingredients of such latent pathogens.

Introduction

In the evening of July 6, 1988, at 22:00 hours, a gas explosion ripped through the Occidental Petroleum Company's oil platform Piper Alpha, 108 miles off the Scottish Northsea coast; a fire ensued, followed by another explosion. The whole platform was destroyed and 165 of 266 men on the site were found dead.

Lord Cullen's (1990) comprehensive investigation report identified a leak as presumed immediate trigger of the disaster. The leak was created by a safety valve being in repair when the night shift on July 6, without being aware of it, started a pump connected to the safety valve in question. Various shortcomings became evident: poor communication among shift teams, inadequate system of commisioning repair jobs, negligent use of prescribed procedures and respective controls. The catastrophe was further aggravated by poor emergency measures and relief operations due to shortcomings of information, lax training measures, inadequate relief supplie4s and superficial inspection habits. Besides, there had been various forerunner incidents during the years prior to the disaster which should have warned management. Furthermore, Lord Cullen detected imperfections in the overall safety management, i.e. in analytic safety analyses of Occidental Petroleum, in control and inspection methods and rule books of supervisory bodies.

The example of Piper Alpha shows the performance of a socio-technical system with high hazard potential which took as its motto reliability, efficiency, and safety. However, what happened in fact was the opposite: failure, inefficiency, and catastrophe. The example also illustrates the need for last of the three phases identified by Reason (1993) in the history of safety sciences: the first was the *technical phase* in which accident avoidance was aimed at through optimizing technical components; it was followed by the *human error phase* when improving safety was pursued by improving operator competence; but Piper Alpha shows that the underlying assumptions of these two phases insufficiently guide safety management: we need to consider the complex interaction of technical as well as human, social, organizational, and managerial factors as co-contributors of incidents and accidents. We presently operate in the *socio-technical phase* of safety sciences (Brascamp, Koehorst and van Steen, 1993).

Managerial action in complex systems of high hazard potential can have horrendous consequences for people and environments. The aim of this paper is to take a systemic look at dimensions of managerial actions which may influence the probabilities of systems breakdowns. This is done in three steps:

[1] I am grateful for the critical comments to an earlier version of this paper made by colleagues in the Research Center Systems Safety of the Berlin University of Technology: B. Fahlbruch, M. Fank, M. Freitag, R. Miller.

1. a discussion of theoretical approaches reflecting the relationship between management and organizational failure/success;
2. a discussion of various dimensions of management action which have proven to be of importance for systems safety;
3. three theses on the link between management and organizational learning.

Theoretical approaches: management and organizational failure/success

It is generally accepted that human action plays an important role in incidents and accidents. Various A studies of incidents in US nuclear power plants claim that upward from 65% of all systems failures are significantly influenced by human action and human error. But it is novel to consider management as risk factor. After all, what is meant is that management may possibly increase the probability of incidents with undesirable consequences for materials, people, and environment. The other way around seems to make more sense: if organizations are successful, this is attributed to good management. Thus, we construct causal links between management and success ex post. However, for concern with safety of high hazard systems it would be desirable to know in advance what the probabilities of systems success and failure are. Three theoretical approaches attempt to throw light onto this question (Starbuck and Milliken, 1988a):

Theory 1: Independence of probability of success from previous success/failure

This theory is reflected in the hard nosed probability assumptions of throwing dices or coins where each new attempt has the same probability to come up with a '6' or the head of the coin, independent of previous results. However, this radical probabilism has little explanatory value for living systems such as organizations, because it is based on the assumption that all conditions (hardware, procedures, competences of people, etc.) remain constant over time. Nevertheless, it may very well be that managers believe in the basic invariability of conditions for success and act acordingly.

Theory 2: Contrariness of probability of success after success/failure

This theory assumes that a series of successes (or even only one single success) will lead to increased self-assuredness and negligenece while the experience of failure will lead to increased effort and attention. In other words, success will lead to reduced succes probabilities, failure will lead to increased probabilities of success. A series of successes will, therefore induce management to fine-tune the system, reduce redundancies in the interest of increased efficiency, because success proves the basic functional health of the organization.

Theory 3: Previous success leads to increased, previous failure leads to decreased probability of success

This seems to be the theory with the highest degree of plausibility and conventional wisdom, after all, success appears to reflect competence and failure inadequacies of the system. Since expectations concerning success are not unchangeable dogmas but experience based hypotheses, such a theory seems to correspond best to human need to look for simple explanations. Wilde (1986), in his theory of risk homeostasis, has attempted to systematize this approach.

However, there is a fourth, systemic theoretical approach (Reason, 1990) which transcends the a.m. cognitive approaches in that it considers also management and organizational factors on the one hand and it offers a model linking such factors causally to success/failure on the other hand. Both aspects make this theory attractive in the present context:

Theory 4: Socio-technical theory of organizational health

The theory postulates that success in terms of system safety and reliability depends on the health of the whole organization in all its components. The theory distinguishes *active errors* from *latent errors*. active errors are triggering actions of operators whcih unleash an incident or accident. Such trigger actions are necessary, but in and of themselves insufficient requirements for and incident/accident. 'Rather than being the main istigators of an accdent, operators tend to be the inheritors of system defects created by poo design, incorrect installation, faulty maintenance and bad management decisions. Their part is usually that of adding the final garnish to a lethal brew whose ingredients have already been long in the cooking' (Reason, 1990: 173). We are dealing here with so-called resident pathogens which lie undetected in the system, often spacio-temporally far removed from the trigger action at the 'sharp edge' of the man-machine-interface. In addition, it is important to realize that stochastic processes play an important role in incidents/accidents. This means, that incidents and accidents can occur independently from the high safety standards of a given organization while an 'unsafe organization' may enjoy long periods without accident.

With this fourth approach we have the basic conceptual instruments to analyze managerial actions in their safety relevance.

Managerial action and safety[2]

In the following I distinguish *direct* from *indirect consequences* of managerial action and, in addition, I shall speak of safety consequences of specific *organization-environment relations.*

Direct consequences of management actions for safety

HUMAN RESOURCES DECISIONS

The example of Piper Alpha demonstrated already that insufficient training, whose planning and implementation is undoubtedly a managerial prerogative, may prove desastrous for triggering as well as managing an emergency situation. However, direct consequences for safety may also result from decisions regarding the composition of work teams. I am referring here to the requisite qualification mix in work teams or shifts to master given routine or emergency tasks. In a detailed analysis of an almost accident in a German nuclear power plant we have shown that Ashby's axiome of requisite variety (Ashby, 1969) had inadequately been taken into account (Wilpert and Klumb, 1991). In consequence, the possible implications of certain actions taken by the shift may not have been correctly understood and, thus, a potentially dangerous situation was produced.

PROCEDURES

Formal procedures and written rules and regulations are usually compiled in operational handbooks. They are to guarantee behavioral repertoirs of operators and plant personnel to achieve safe system conduct. There is, however, growing evidence that comprehensibility of procedures, their accessibility and applicability to given circumstances are often wanting. Recent studies show that the percentage of incidents and accidents in nuclear operations which are linked to poor procedures and documentation range from 13.5 – 34% (Wilpert, Freitag and Miller, 1993).

Content, formal structuring and user friendliness of such procedures must also be counted within the responsibility domain of management and engineers hierarchically located above operator teams. In case they are inadequately written, such procedures lie latent (dormant) within the organization as resident pathogens. In analogy to organic hidden illnesses they revceive their virulence if certain environmental conditions materialize and 'awaken' them. Thus, operator error and system failures may, therefore, be considered delayed consequences of inadequate procedures and system design, i.e. direct consequences of managerial (non)action.

CONTROL AND INSPECTION

Piper Alpha, like most high hazard organizations, had prescribend periodic inspections of

[2] Management may be difficult to define in corporate structures and in companies with many sites. This aspect and the problems which may arise from the relative distance of the central administration to different sites cannot be treated here. For purposes of this paper management on the corporate/central level and on the enterprise/site level are treated as one.

safety relevant system components, regular controls and continuous supervision of staff workin patterns. In that particular case these prescriptions were followed so carelessly that they proved totally inadequate to insure safety on the platform. Personnel on and off the platform performed during the emergency in ways which only increased the toll of the catastrophe. Combined with poor training and supervision the platform staff developed what Weick (1987) called 'trained incapacity' to cope with the challenge. Such processes of continuous but incremental deterioration have been shown to be in existence in many of the recent major industrial incidents and accidents (e.g. Clapham Junction; Herald of Free Enterprise).

FINETUNING

As pointed out above, theory 2 suggests that sustained success induces negligence. Starbuck and Milliken (1988a) speak of gradual acclimatisations of management ot previous success which induces managers to finetune the system. 'Finetuning' means the reduction of existing redundancies in the interest of savings and higher profitability since the antecedent success seems to prove that the system works so efficiently that additional efficiency appear to be possible. Starbuck and Millikan take the example of the Challenger desaster of January 28, 1986 to demonstrate how additional factors determine the ultimate outcome of organizational decision-making. Finetuning in the Challenger case was also the result of an intraorganizational conflict between managers and engineers. While managers focus their attention to the most economic solution of a problem, engineers tend to accentuate safety aspects. This is a consequence of differential socialization in different profesional groups. In situations of uncertainty, engineers tend to follow a path which increases safeguards and, thus, cost.

'Although engineers may propose cost savings, their emphasis on quality and safety relegates cost to a subordinate priority. Managers, on the other hand, are expected to pursue cost reduction and capacity utilization, so it is managers who usually propose cuts in safety factors. Because managers expect engineers to err on theside of safety, they anticipate that no real risk will ensue from incremental cost reductions or incremental capacity expansions' (Starbuck and Millikan, 1988a:333).

In the Challenger case some critical decisions which influenced the events of January 1986 were made already in 1982 – an almost classical example of spatio-temporal dislocation (or better: prelocation) of managerial actions contributing to the accident.

Indirect consequences of management philosphy and policy

Much more difficult than tracing direct safety consequences of management action is the identification of indirect influence and impacts of management attitudes and policies upon the safety of complex systems. The reason for this difficulty lies in the fact that policy guidelines and goal setting orientations of management can only be identified indirectly by their behavioral consequences among employees, they function like power lines of a magnetic field in orienting staff behavior. Some examples may serve to illustrate the dynamics.

REFERENCE SYSTEMS AND PERCEPTUAL FILTERS

The particular colouring and kind of perceiving of a given organizational environment, including danger signals emittted therefrom, will strongly be influenced by the kind of theory managers consciously or unconsciously hold regarding causal conditions for success as has been described above. Such theories are frames of reference and function as filters for those things that are perceived as relevant, important or unimportant. Frames of reference reduce uncertainties, stereotype and classify situations and facilitate quicker communication and reactions to environmental stimuli. Thus, they may be helpful if they represent adequate models of the world, but in case they are caricatures of it, they will induce inadequate decisions and actions (Starbuck and Millikaan, 1988b:55). Unsafe and unreliable system performance will follow suit.

ECONOMIC PRESSURE

Managerial pressures towards efficient goal achievement are rational means to pursue intended organizational goals. Such pressures are reflected in respective managerial decisions, but they are also mediated by symbolic action. Quite known is the proverbial chief executive who picks up a paper clip in his secretary's office and places it demonstratively on the secretary' desk while saying in unmistaken clarity: 'We really can't afford such wastage of resources'. Rasmussen (1992) has likened this all-pervasive managerial pressure towards efficiency to a force which interacts with the natural, also very rational inclination of employees to improve their input-output ratio in task completion. Both tendencies result in a 'cost-input gradient' which make employee actions to migrate into the direction of borders of acceptable safe behavior. Once these borders are irretrievably transgressed, an incident or accident occurs. We can see here, how two in and of itself quite sensible and rational strategies produce in their confluence an undesirable result. It seems to me that this description is much closer to the dynamics occurring in real life situations than the often quoted ethical conflict between economic and safety perspectives.

INFORMATION AND COMMUNICATION POLICIES

Reason (1990) has stressed that control of safe operations is a continuous process like flow production. Crucial conditions for safe operations are feedback loops about systems states. Thus, in line with conceptualizations of the International Atomic Energy Agency (IAEA, 1990), reliability and safety are aspects of performance quality. This implies the necessity to establish safety information systems which go beyond traditional documentations of past incidents and accidents. What is required is a continuous process of identifyinf indicators of safety.

Such indicators must also relate to what we called resident pathogens or latent errors. However, these are, due to their very nature, notoriously difficult to pinpoint. Their identification seems to require two organizational characteristics: a permanent search orientation of personnel and efficient institutionalized feedback loops to management and back from there to relevant organizational units. These conditions are by no means available everywhere as the frequently noted information breakdown prior to incidents and accidents demonstrate (Cullen, 1990; Wilpert and Klumb, 1991).

LEADERSHIP STYLE

One of the most informative investigations of the consequences of leaderhip style for group dynamic processes with safety implications is undoubtedly the work of Janis. In *Victims of group think* (1972) he shows how Kennedy's leaderhip led his advisory group of highly intelligent and experienced experts to adopt a consensus forging strategy which led right into the Bay of Pigs disaster. The selection of advisors, an unconscious directing of the discussion about associated risks, the search for quick consensus, all that produced a water tightening of the discourse against warning signals, self-appointed defenders of consensus, and an esprit de corps which made every obstacle to appear small if one only wanted to overcome it. The example illustrates also how under such conditions we may observe an 'evaporation of responsibility' which means nothing else but the impossibility to attribute guilt for a failure to a specific person or a single decision.

In later works (1989, 1992) Janis attempts to describe elements and processes which are important for good decision-making in large organizations. He summarizes them as 'vigilant problem solving', a procedure which starts with problem formulation, proceeds over utilization of informational resources and in depth analysis and evaluation to a choice decision with several feedback loops. Thus, Janis claims, typical shortcomings of suboptimal decision-making are avoided. Janis mentions three conditions which negatively influence vigilant problem solving: cognitive limits (time pressure), social limits (need for consensus), and egocentric limits (prestige orientation).

SAFETY CULTURE

A new concept is en vogue since the Chernobyl disaster: safety culture (IAEA, 1991). The notion fits well into the third phase of safety sciences described above. Coming from cultural anthropology the concept of culture entered organization sciences as organizational culture and, in the guise of safety culture, turned out to be a panacea for accidentologists (Wilpert, 1991). Generally we understand culture to denote the ensemble of values, attitudes, and norms which characterize a group and which are transmitted by a group to new members (Hofstede, 1980: ‘collective programming of minds’). I personally feel that this understanding is too limited, because it remains too much on the cognitive level and leaves out behavior, which is so important for safety (Wilpert, 1991). After all, we know from social psychology that between values/attitudes and behavior is often a considerable difference. More useful seems, therefore, a definition such as:

Safety culture denotes the collective consciousness and corresponding behavior of all systems members which impacts upon the safety of the whole system.

One research line which focuses on the role of management in implementing an organizational safety culture refers to so-called high reliabilty or reliability enhancing organizations such as atomic airplane carriers, nuclear power plants. A research group in Berkeley (Roberts, 1993) identified nine organizational values which are important conditions for fostering safety culture, among them interpersonal responsibility and trust, creativity and goal orientation, social support and tenacity. According to the Berkley goup three management strategies are likely to promote safety culture:

1. *Flexible decision levels* (migrating distributed decisions) which facilitates local control over important events also in lower hierarchical levels, but with the possibility to transfer the decision upwards again if necessary.
2. *Management by exception*: competent management which in case of an emergency knows when an action on lower organizational strata must be stopped.
3. *Promotion of a total organizational vision*: the transmission of a profound knowledge among all members what the organization is about.

Safety culture, if the notion is to make sense at all, must permeate the total system, i.e. it cannot be delegated to a specific unit in the system (safety department). It cannot be introduced per ordre de moufti but demands a long process of organizational development in which all levels must be involved. Safety culture presupposes an open learning system in the organization in which the free flow of information without barriers is possible (Wilpert and Klumb, 1993). Thus, safety in safety culture is an aspect of an organization’s high quality output. Up until now, however, the notion signals more of a program than a desirable reality. This may be illustrated by discussing the problem of organizational borders and safety:

Environment, safety, and management

We have become used to think of organizations as living open socio-technical systems which are in active exchange with their environments. However, where are the borders of an organization? Regulatory bodies of nuclear power plants are from the point of view of utilities part of the environment. However, from the point of view of society’s interest in nuclear safety both, nuclear power plants and regulators are part of the system safeguarding nuclear safety. Given the fact that in many industrialized countries the general public is rather critical of nuclear energy production (TMI and Chernobyl are the catch word of this climate) we have a peculiar indirect impact of the societal environment upon intra-organizational safety.

Nobody should be surprised that in a climate of distrust, claims and conterclaims, accusations and defense, management scrutinizes every bit of information about internal events which are given to the public. This keeps turning the spiral of distrust. Regulators on the other hand perceive the need to demonstrate to the public that they have done everything possible to meet their responsibilities of supervision. They do this through rules and regulations to licensees and inspection missions. This has consequences internally as well: also management has to protect itself. Management, therefore, also writes rules and regulations and procedures to be obeyed. Operators perceive a deluge of those. But they comply, make their check mark on the control list just to prove bureaucratically that they have done what was expected. Thus, instead of safety culture emerges its caricature: a bureaucratized system of self-defense.

What can be done? I shall try to formulate three theses which point into the direction into which managerial action ought to be directed if it wants to influence safety and reliability of high hazard systems.

Organizational learning and management

Thesis 1: Openness towards in- and outside is required

If the vicious circle of distrust, information hiding, accusation and defense is to be broken, industries dealing with high hazards must turn to a policy of intra- and extra-organizational openness. Towards the outside this means understandable information. Towards the inside this means the creation of an atmosphere which avoids individual guilt attribution, it means to foster and promote exploratory behavior, free flowws of communication, and learning from ones mistakes, even from those of management.

Thesis 2: Systematization of feedback control is required

Learning from one's own mistakes presupposes to take notice of one's mistakes, document, collect, analyze them and to draw the respective lessons from them by implemetning continuous change processes. This is systematic learning from experience befitting the 'motivated competence model' (Heller, 1992). Such systematization requires that the learning becomes institutionalized with respective feedback loops, incentives for communicative openness and disincentives for information hiding. Civil aviation and nuclear industry have already implemented such documentation, reporting and analysis systems. Chemical and pharmaceutical, ground transport and oil producing industries seem to be in need to focus on such measure as well.

Thesis 3: Systematization of feedforward control is required

Anticipatory and anylytical risk assessments are state of the art in nuclear and aviation industries. Particularly nuclear industry, due to its inherent hazard potential, has given great care to such procedures (Meyer-Abich and Schefold, 1986). These probabilistic analysis techniques must, however be linked to techniques which are based on learning from experience. Only in linking both control mdalities – feedback and feedforward control – with each other will we be able to minimize management risk in high hazard organizations to become a residual risk.

References

Ashby, W.R. *Introduction to cybernetics.* London: Chapman and Hall, 1956.

Brascamp, M.H., L.J.B. Koehorst and J.F.J. van Steen. Management factors in safety. In P. Kafka and J. Wolf (Eds.), *Safety and reliability assessment: An integral approach.* Amsterdam: Elsevier, 1993.

Cullen, Lord D.W. *The public inquiry into the piper alpha disaster.* London: HMSO, two volumes, 1990.

Heller, F.A. Decision-making and the utilization of competence. In F.A. Heller (Ed.), *Decision-making and leadership.* Cambridge: Cambridge University Press, 1992.

Hofstede, G. *Culture's consequences.* La Jolla, CA: Sage, 1980.

International Atomic Energy Agency (IAEA) *Quality management for nuclear power plant operation.* Technical Report Series, 315, Vienna: IAEA, 1990.

International Atomic Energy Agency (IAEA) *Safety culture.* Safety Series No.75-INSAG-4. Vienna: IAEA, 1991.

Janis, I.L. *Victims of group think.* Boston: Houghton Mifflin, 1972.

Janis, I. *Crucial decisions: Leadership in policy making and crisis management.* New York: Free Press, 1989.

Janis, I. Causes and consequences of defective policy-making: A new theoretical analysis. In

F.A. Heller (Ed.), *Decision-making and leadership*. Cambridge: Cambridge University Press, 1992.

Meyer-Abich, K.M. and B. Schefold. *Die Grenzen der Atomwirtschaft*. München: C.H. Beck, 1986.

Rasmussen, J. Perspectives on the concept of human error. Unpublished manuscript, 1992.

Reason, J. 1990. *Human error.* Cambridge: Cambridge University Press.

Reason, J. Managing the management risk: New approaches to organizational safety. In B. Wilpert and Th. Qvale (Eds.), *Reliability and safety in hazardous work systems*. Hove: Lawrence Erlbaum. 1993.

Roberts, K.H. Cultural characteristics of reliability enhancing organizations. *Journal of Management Issues, V,* 165–181, 1993.

Starbuck, W.H. and F.J. Milliken. Challenger: Fine-tuning the odds until something reaks. *Journal of Management Studies, 25* (4), 319–340, 1988a.

Starbuck, W.H. and F.J. Milliken. Executives' perceptual filters: What they notice and how they make sense. In D.C. Hambrick (Ed.), *The executive effect: Concepts and methods for studying top managers.* Greenwich, CT: JAI Press, 1988b.

Weick, K.E. Organizational culture as a source of high reliability. *California Management Review, 29* (2), 112–127, 1987.

Wilde, G.J.S. Beyond the concept of risk homeostasis: Suggestions for research and application towards the prevention of accidents and life-style related disease. *Accident Analysis and Prevention, 18,* 377–401, 1986.

Wilpert, B. System safety and safety culture. Paper presented at the IAEA/IIASA meeting 'The influence of organization and management on the safety of NPPS and other industrial systems', Vienna, March 18–20, 1991.

Wilpert, B. and P. Klumb. Störfall in Biblis A. Theoretische und pragmatische Überlegungen zu einer systemischen Betrachtung der Ereignisse. *Zeitschrift für Arbeitswissenschaft, 45* (1), 51–54, 1991.

Wilpert, B. and P. Klumb. Social dynamics, organization and management: Factors contributing to system safety. In B. Wilpert and Th. Qvale (Eds.), *Reliability and safety in hazardous work systems.* Hove: Lawrence Erlbaum, 1993.

Wilpert, B., M. Freitag and R. Miller. Analyse Human Factor-relecanter Apsekte anhand meldepflichtiger Ereignisse in Kernkraftwerken. Final Report. Berlin: Technische Universität Berlin, Institut für Psychologie, 1993.

Bernhard Wilpert is professor of Psychology at the Technische Universität Berlin, and Director of Research Center Systems Safety, Germany.