International Institute for Applied Systems Analysis
IIASA www.iiasa.ac.at

The Influence of Organization and Management on the Safety of NPPS and Other Complex Industrial Systems (Report of an IAEA/IIASA consultants meeting in Laxenburg and Vienna, 18-22 March 1991)

Wahlström, B. and Swaton, E.

IIASA Working Paper

WP-91-028

July 1991

Working Paper

THE INFLUENCE OF ORGANIZATION AND MANAGEMENT ON THE SAFETY OF NPPS AND OTHER COMPLEX INDUSTRIAL SYSTEMS

Report of a consultants meeting jointly organized by the International Atomic Energy Agency and the International Institute for Applied Systems Analysis held in Laxenburg and Vienna, 18-22 March 1991.

WP-91-28
July 1991

IIASA

International Institute for Applied Systems Analysis □ A-2361 Laxenburg Austria

Telephone: (02236) 715 21*0 □ Telex: 079137 iiasa a □ Telefax: (02236) 713 13

FOREWORD

An analysis of causes for human errors reveals that deficiencies in organization and management often provide an environment making errors more likely. There is also a considerable difference between the operational performance of similar industrial plants. A closer analysis often reveals that the differences can be attributed to the managing practices. Accepting organization and management as one important precursor for operational safety, the aim is to identify good managerial structures and practices as well as characteristics of unsafe operational practices. Such information can provide guidance for the operators of the installations and also support regulatory agencies. The ultimate aim should be to detect and correct organizational deficiencies before an incident or accident brings them into the open. It is therefore not sufficient to blame individuals nor training, because management and organization establishes priorities, structures, and practices that enable tasks to be accomplished.

A consultants' meeting organized jointly by the International Atomic Energy Agency (IAEA) and the International Institute for Applied Systems Analysis (IIASA) was held in Laxenburg and Vienna, Austria on 18-22 March 1991. The objective of the meeting was to assess the extent to which research within the management sciences can provide guidance for the practical problems of managing organizations, where safety is the major concern. The influence of organization and management on the safety of complex industrial installations was discussed during the meeting and the exchange of ideas and experience between different industrial sectors and the academia proved fruitful. In spite of the difference among national and company practices it is still expected that there are many possibilities for an exchange of good managerial knowledge, experience, and practices. The report collects both the contributions offered by members of the Expert Task Force and the findings of the discussions that took place during the meeting.

Specific reference is in the following text made to the nuclear industry with the understanding that the issues have a wider application to chemical plants, off-shore installations or more generally to industries where safety is a major concern.

B. Wahlström
IIASA

E. Swaton
IAEA

SUMMARY

The importance of organization and management has been demonstrated convincingly in all modes of operational performance in complex industrial systems. In spite of this awareness there have been relatively few attempts to systematically study the components and structures involved. This document intends to provide a starting point for systematic approaches by interfacing theoretical models with practical experiences.

The first chapter relates the overall notion of safety to organization and management. It is noted that the relative absence of particularly significant events at most of the industrial facilities can be partially attributed to the ability of the management to provide the resources, guidance and decision making capacity ensuing in safely constructed, operated and maintained plants. This also means that safety is incorporated into business plans and work designs as an integral part for efficient and economical production. However, our understanding of what constitutes effective management and organization for safety lags far behind our knowledge of most of the more technical issues in plant operation. Thus tools need to be established to develop a systematic understanding of management and organization effects on plant safety. Proper and objective research will require access to various, until now scattered data sources monitored by individual plants, industrial organizations and regulatory bodies and the provision of opportunities to collect new data on diverse practices.

In the second chapter the current state of knowledge on good practices is analyzed. Particularly in the nuclear power industry documents have been issued containing some of the key safety related challenges managers are faced with and also provide recommendations on strategies to cope with these challenges. However, experience in the industry demonstrates that management and organizational aspects still do contribute considerably to operational safety problems at installations. Thus, some of the strengths and weaknesses of the good-practice approach are addressed and possible improvements in the process for developing and disseminating this information discussed. In addition, several significant limitations to "absolute" good-practices as opposed to flexible adaptation to changed circumstances are presented.

The elements to be considered when studying organization and management in general are outlined in the third chapter. At present there are only incipient theories available which attempt to depict safety management of complex industrial settings. At the onset the multi-level nature of the focal system has to be considered where the situation has different aspects on the different systems levels. Furthermore, the various productive processes require specific safety conditions and thus somewhat adapted safety and management approaches. Emergency conditions are a third area of consideration for related practices. In general, only partial theories are available for these areas, which do not easily lend themselves to being combined in a systematic fashion. Three fundamental elements, namely *hierarchical levels*, *actors* and *time* are discussed.

The fourth chapter is devoted to identify some emerging themes which appear to be applicable in most industrial settings. Here the starting point is a closer scrutinization of the process of problem-solving and/or adaption. The three most complex and critical phases of this process are presented, including the establishment and promulgation of clear safety policies, the systematic

collection and analysis of data on performance with ensuing generation of adequate solutions and also new approaches, and finally the comprehensive implementation of these insights among the entire installation staff.

In the conclusions and recommendations a number of research questions are formulated and suggestions for future investigations within complex industrial facilities are made.

CONTENTS

THE INFLUENCE OF ORGANIZATION AND MANAGEMENT ON THE SAFETY OF NPPS AND OTHER INDUSTRIAL SYSTEMS

1. Managerial and Organizational Approaches to Safety in Complex, Potentially Hazardous Settings.

1.1 A broad view of safety.

The roles of management and organization in assuring the safe performance of complex technologies, such as a nuclear power plants, chemicals production, and off-shore installations, are now obvious from experience. Among the serious and significant events characterizing the history of industrial installations are several where management failures were either primary or contributing causes (TMI, Chernobyl, Piper Alfa). In a similar sense, the relative absence of especially significant events at most of the world's plants can also be partially attributed to the ability of plant and utility management to provide the resources, leadership, and decision-making that leads to safely constructed, operated and maintained units. But while the importance of management and organization is clear, our understanding of what constitutes effective management and organization for safety lags far behind our understanding of most of the more technical issues facing the operators and regulators of the plants.

Although it is possible to state the problem succinctly, in practice the issue of management and organization for safety is broad and complex. The aim of this working paper is to describe the universe of questions, issues, topics, and unresolved problems of this domain. As a whole, then, this paper has two goals: First, to suggest frameworks by which conceptual models might be further discussed and developed, and second, to provide thereby an agenda to organize future work and priorities.

Today, there is little doubt that managerial practices and organizational structures influence the safe performance of complex industrial systems. Instead, we work from the assumption that safety of workers and of the public can no longer be regarded as a separate industrial function, skill, or concern that must be mandated. Rather, in tandem with modern industrial practice, safety matters are integral to every function, from the long-range planning in executive offices to the maintenance work being performed on shop floors. This modernized view incorporates safety into business plans and work design as an integral part of goals for efficient and economical production.

Although the industry generally subscribes to this view of safety, there is at the same time a tendency to believe that the "safety problem" is merely an artifact of the public's perception of risk and hazard. The industry also believes that when plants are operating at top power production performance, they are simultaneously maximizing safety. That is more a goal at the moment, however, than a fact, and one objective of this paper is to contribute to making it so. Effective practices occur in every plant, throughout each of the complex industrial systems, but currently it is very difficult to use this information effectively. Thus, one of the main issues we discuss is: How to structure, organize, and systematize practical knowledge that exists in many forms.

It is evident that higher management has a profound influence on the safety of industrial installations. The roles are however different at different levels in the organization. The chief executive officer (CEO) of a large industrial conglomerate has one role and the plant manager has another, but both should participate in the definition of company approaches to safety. In the present report no large difference is made between the different managerial positions with the understanding that approaches to safety will be largely similar.

Thus, when we define management, we must define it broadly to include not only the plant manager, but also the line of management extending upward to the CEO, and downward to the first line supervisor. We must also recognize that even direct workers, such as those in self-managed workgroups may perform some activities that have traditionally been the domain of management. Further, we must also recognize that external actors, such as financial holding companies or regulators can also take on the role of manager in some specific cases. When we investigate or conduct research on management, therefore, we must be willing to accept the fact that different organizations, different cultures, and different political systems will distribute the management function in different ways.

An historical perspective is also needed on the very concept of safety in order to understand its social evolution and current conceptualization. Today we regard safety as consisting of the avoidance of injuries to all employees and the public and damage to the environment and property. In the past, we have perhaps been less conscious of the potential threats to employees and the public, and in the future, our concern may be greater still.

Along with a sense of history, we must also consider the future. Existing plants are aging, and management will be responsible for laying out and implementing a strategy for assuring the continued safe performance of existing plants. Similar changes are happening in the work force, as the original generation of staff must be replaced with a new, and perhaps different type of worker. Many utilities will face potential severe economic challenges in the future that will tax the ability of management to assure that resources and skills are available to operate the plant. At the same time, technology itself is changing, opening new options for existing plants and plants yet to be designed and constructed. These changes will also provide challenges to effective management and organization for safety.

1.2 Some Issues in Research.

To develop the tools by which the goal of a systematic understanding of management and organization effects on plant safety can be accomplished requires a research perspective on managerial and organizational issues. For the nuclear power industry in particular, this perspective introduces a new voice into what has been chiefly the purview of regulators, especially perhaps in the USA. The arrival of independent researchers – those whose research concerns stem from the theoretical interests of several disciplines – represents not only a new institutional actor, but one whose objective is understanding rather than criticism. If properly and objectively conducted, research can extend management's understanding of how to effectively assure plant safety. However, such research will require access to the various scattered data sources, maintained by regulatory bodies, by industry organizations, and by individual plants. It will also require access to the opportunity to collect new data on management and organization practices. Such data are essential for systematizing and recasting information in useful ways, but these data are often closely held and unavailable for reanalysis, perhaps because of the regulatory atmosphere and attendant antagonisms.

These data, in their various forms, are needed for developing the conceptual models that represent the essential issues involved in managing and organizing daily productive operations. The aim of the research community should be to cooperatively develop studies of operating practices that are of interest both to broader disciplinary questions and to those plant operators eager for validated practical knowledge. Further, the international character of this work opens new questions, as we begin to understand better the conflicts among different models of operations that rely on different assumptions -- most notably, perhaps, the differences between tighter and looser regulation of operating procedures and the differences in trust that they imply.

2. Good Practices: What Do We Know From Experience?

While it is widely recognized that much has yet to be learned about how to safely manage and organize nuclear power plants (NPPs), it must also be recognized that much useful industry experience exists to guide this learning process. And, while management and organizational factors have been increasingly cited as major contributors to operational safety problems, the management and organizational systems of most NPPs appear to operate fairly effectively in assuring safe performance. Thus, there would appear to be considerable "good practice" information available to augment the "bad practice" information available from analyses of events. In fact, many such good practices have been compiled into one or more of the good-practice documents related to management and organization (IAEA; INPO). These documents identify some of the key safety-related challenges facing NPP managers and provide recommendations on specific practices for meeting these challenges. Some of the practices reflect the detailed approaches that have led to successful performance at particular plants, while others are more general recommendations aggregating the experience of several or many utilities. Examples of what some industry experience has identified to be good practices can be found in Appendix A.

The existence of these good practice documents speaks to the fact that considerable information exists on how to organize and manage for safety. However, the experience of the nuclear industry world-wide amply demonstrates that management and organizational issues continue to contribute significantly to operational safety problems at plants. Thus, it is important to consider the current state of good practices, the usefulness of the good practice approach, and ways that the process of developing, diffusing, and implementing good practice information can be improved.

Given the existence of such "good practice" information, why do management and organization-related safety problems continue to exist? It is clearly the case that current understandings of good practice, though highly useful, are not sufficient to guide the managers of hazardous industrial installations in the very difficult task of continuously assuring safety. In this section, we would like to address some of the strengths and weaknesses of the good-practice approach, and to recommend both some improvements in the process for developing and disseminating information on good practices, and some higher order good practices that do appear to be emerging from both industry experience and systematic research. We will refer to these higher order good practices as "good principles." Some initial discussion of good principles can be found in Chapter 4.

What lies behind the inadequacy of current good practice information? One obvious factor is that much of it has not been systematically collected and verified, and that some of the information that exists is not sufficiently precise or accurate. However, there are several more significant limitations to the good practices approach to assuring safe management and organization.

In general, expectations for safety performance have increased in most countries over time. This has been due both to public/regulator pressures, and to recognition on the part of plant operators of the need for enhanced safety based on their operational experience. As the expectations for safety performance have increased, additional demands have been placed on the management and organizational systems. These increased demands have led to changes in what constitutes a good practice. For example, the TMI accident had substantial effects on the definition of what constitutes an adequate system for screening the operating experience of the industry. What existed as adequate practice before the accident, would no longer be considered to be adequate.

In a similar sense, there have been other major changes in the operating environment of many utilities. These have included changes in the cost, quality and availability of labor, technical information, fuel, and parts. These "economic" changes have affected substantially the management and organization systems required to be economically viable, with resulting effects on safety, as well. Thus, these other changes have led to a reconsideration of what constitutes a good practice.

Plant and organizational aging have also required adjustments in what constitutes good management and organization practice for safety. The needs of the mature workforce are not the same as the needs of the young workforce. The loss of key staff present with the utility since construction of the plant requires new systems for retaining plant specific knowledge. The aging and replacement of components may dramatically affect existing workflow systems and the required skill base of the organization. Thus, for several reasons, what constitutes a good practice will necessarily change with time.

Even more important, however, is the fact that good practices exist only relative to an intact, systematic management system. When good practices are reported, they are necessarily abstracted from this more complex system with some substantial degree of information loss. The logic of the good practice, however, remains tied to the other elements of the system from which it was abstracted. For example, the success of a recommended good practice for root cause analysis may depend upon the communications systems, authority relationships and technical skills present in the organization. Unless similar conditions exist in other organizations, this good practice may not be exportable with the same degree of effectiveness.

There are a number of factors that can cause NPP organizations to vary to the point that the transferability of good practices is in doubt. Some of these factors include:

- Willingness to learn from experience, training
- Regulatory philosophy and requirements
- Public attitudes and expectations
- Economic pressures
- Labor force characteristics
- Cultural differences
- Ownership structures
- The unique history of the organization
- Other, existing management and personnel practices
- Technology

Specific good practices may well exist among NPP organizations that are similar on these dimensions, but to the extent that they vary, particularily good practices can still be hard to identify.

It is extremely important, therefore, for those organizations, such as leading utilities, regulators, industry groups, and even the research community, that are in a position to identify and communicate good practice information, to recognize that much of the good practice information is, in its specific application, context specific. These organizations must be willing to learn about the context, and provide advice tailored to that context. Managers of industrial facilities in turn, must recognize that the good practice information available may need to be substantially adapted in order for it to help at their particular plants.

3. Elements in the Consideration of Organization and Management.

Today, good practices as well as all operating actions are guided by implicit traditions, assumptions, inferences, theories, understandings, and experience. The role of research is to describe, clarify, and systematize them. At times, the role of research is to bring tacitly held assumptions up to close scrutiny. Although it is commonly believed that a Probabilistic Risk Assessment model, for example, is only a *technical tool*, we suggest that it must also be considered as a *social product*, the end result of a social process that represents the judgments, values, and particular perspectives of its creators or those who apply it. Similarly, many self-evident management practices may also need to be reexamined through the eyes of research. The appearances of universality need to be modified with acknowledgements of their contingency and context-dependence if such tools and practices are to be maximally effective.

At the onset, one has to realize that at best what we have presently are incipient theories that try to cover safety management of complex industrial settings comprehensively. As discussed previously, the redress of this situation is seriously hampered by access problems to data on managerial practices and organizational processes in real life situations. In addition, the subject matter of concern is very complex, spanning several levels of analysis and differing operating conditions.

For example, it is important to note that the multi-level nature of the focal system implies that the problems pose themselves differently on different systems levels - the governmental/regulatory, the public discourse level, the corporate/company level, the plant and operational level, and individual behavior. A developed and verified theory of management and organization for safety must be capable addressing the different levels and of describing and explaining the ways that the levels are interconnected.

The picture is even further complicated when the intrinsic cyclical nature of a production process such as that of NPPs, sets specific safety conditions for the different systems levels depending on the particular phase of the productive process (construction, start-up, production, outage, decommissioning). In addition, the damage potential and the speed in which emergency situations tend to develop in NPPs, set particular constraints on organizational and managerial action models to cope with these requirements. Therefore, what can be offered presently are bits and pieces of theoretical fragments which are often hard to relate to each other in a systematic fashion.

Time represents another dimension to be considered using a systems approach. Management concerns not only the specific operational needs of the day, but also planning and strategic decision-making for the future. The time dimension has further to be sub-divided into long-term (production phases) and short-term (operation, crisis, restoration) considerations (cf. Box 1).

Returning to the different levels of analysis, at the *institutional level*, we need to be concerned with the way in which the nuclear utility fits in the wider organizational environment. This includes aspects of the economic system, affecting the profitability of the utility in the present, and its economic viability in the future. It also includes the role of government including any support for the industry that may be forthcoming, the level of control that the government exerts over the operation of the plant, and whether the relationship between the utility and the government is cooperative or conflictual. A third aspect of the institutional level includes the relationships between the utility and other organizational members of the industry including vendors, suppliers, sub-contractors, and the like.

The nature of the institutional context can vary enormously. For example, we have noted variation ranging from fragmentation and encapsulation leading to interest and pressure groups with specific ideological orientations, to other situations where practices of self-evaluation and self-policing suggest a greater openness and perhaps cooperation among institutional actors. What constitutes effective management in a context characterized by conflict may be (at least in the short run) very different from what constitutes effective management in a context characterized by cooperation.

There are resources that management does not control, that are set by institutions external to the organization. Although efforts should be made to negotiate with the external environment for resources and relaxation of unduly constraints, management should only be held responsible for what they do with the resources they can reasonably control. For example, utilities should take a role in creating an intelligent partnership with regulators rather than a grudging compliance or antagonistic avoidance.

Hierarchical levels

- institutional
- corporate/company
- plant
- department
- group
- individual

Actors

- governments
- operator (utility)
- vendors, architect engineer
- regulator
- labor unions
- employees
- public
- media
- researchers

Time

(long-term)
- design and construction
- start up
- production
- outage
- decommissioning

(short-term)
- routine operation
- emergency and crisis
- restoration

Box 1. Three dimensions on which issues of organization and management have to be considered.

A number of safety-related issues operate at the corporate/company level. For example, at the *corporate/company level* safety notions often become fragmented and are considered as unique variables rather than integrative properties of the whole organizational system. The non-systems approach can lead to competitive initiatives within the firm. For example, nuclear safety can become disintegrated with the notion of industrial safety. Theoretically based principles can, however, be identified in certain industries (such as the petroleum industry) where the notion of industrial safety tendentially encompasses risk management both in the area of individual hazards as well as environmental damages.

At the plant level, existing formal (functional) organizational structures and actual operational functioning are often not consonant with each other. What is lacking here are conceptual tools to relate requirements under different task situations such as routine – crisis – emergency situations and requisite resource allocations to each other. A possible theoretical approach might entail clarifying the coexisting of tightly and loosely coupled subsystems (Perrow, 1984).

Group processes. A rich sociopsychological portfolio of concepts relating to group processes to help understand and optimize their outcomes in view of task requirements does exist (Janis and Mann 1971; Janis, 1972). They must however be adapted to the specific situations of industrial installations – e.g. task forces, safety committees, review teams, project groups. Similarly, traditional preoccupations with human factor aspects of safety focus on cognitive-psychological aspects of individual operators. Largely unexplored remain the social, that is, managerial, organizational and cultural dimensions contributing to (un)safe behaviors.

PRA, as relatively well developed technique, is considered as an important managerial tool for improving management of safety of physical assets. The PRA tool has its largest value in comparing the risks of alternate projects/processes and should not be used for an absolute determination of risks. By and large unnoticed are the social (collective) judgmental processes in the development and application of these analyses which determine their outcomes. This is but one example of many so-called "technical" analyses that should be reexamined in light of their concomitant social processes. An important unresolved theoretical problem on this level is how and whether *probabilistic models* of engineering sciences in PRA and behavioral scientific *causal models* of human behavior can be related (J. Rasmussen, 1989).

Within the various levels of analysis, it is important to be able to characterize the primary actors. Among the *regulatory actors* there seem to be different implicit "theories in use" (Argyris, 1970) that guide the development of regulatory frameworks. They can be characterized by their extremes: On the one hand we can observe highly differentiated and formalized regulatory systems to cope with a wide variety of specifically spelled out risks. On the other hand, one can note approaches that are guided by what might be called "performance criteria" that can be fulfilled by different means. On the whole one must say that this domain is "undertheorized". More theory development is required. A fully developed theoretical perspective on the regulatory actions would assist in reconsidering the perceived distinction between industrial and nuclear safety. A necessary approach to develop such a theoretical framework would be to study the safety theories in use of various high risk industrial settings in comparative perspective.

Vendors, designers and architect engineers represent a group of actors with a large impact on actual plant solutions. The relations between vendors, designers, regulating agencies and utility companies constitute intricate interorganizational networks which clearly have impact on safety of NPPs. The interorganizational communication and decision making processes imply inordinately long time horizons, the fading in and fading out of different cooperating parties, which cannot yet be conceptualized and described on a theoretical level except in approximate terms by network theory. The introduction of technological innovations (hardware, software, maintenance techniques) poses a large gamut of theoretical and practical problems that are exemplified by notions such as artificial intelligence and expert systems. Past experience shows that such innovations influence the division of labor between automation and the human systems and therefore can have much more profound implications on managerial systems than originally thought.

Labor, including organized *labor unions* are another group of actors in the picture. Taking into account different socioeconomic and industrial relations systems a traditional concern of unions has always been to contribute to safeguarding workplace safety and fostering accident prevention. Concerns for environmental protection are also growing. Theories of bargaining and interest group representation are of relevance here. Their potential to contribute to industrial safety and the conditions of nuclear power operations will have to be explored.

The *employees* within the organization are perhaps the most important actors for implementing a continuing safety. Only commitment and involvement at all levels can bring in the necessary adherence to high safety standards.

The *public* also provides important interactions between the other actors. Theories of risk communication and risk perception (Renn, Swaton, 1984; Jungermann et al, 1990) are clearly of relevance in this context. It can be shown from a variety of case studies that public opinion climate with regard to NPPs affects reactions of regulatory agencies and of nuclear power utilities: increase of rules and regulations, of proceduralization and "regulation overload" on the one hand and "play down" of information given to the public on specific events. Both contribute to spiraling of public distrust, information hiding, and defensive siege mentalities.

4. Provisional Frameworks for Organizing Good Management Principles.

Although the current level of knowledge and the contingencies that face individual utilities limit the availability of truly useful good practices information, at a more general level there are some emerging themes that appear applicable in most applications. This chapter considers some of those themes.

The modern idea of safety as integral to all productive processes in hazardous industrial organizations has several implications for operations. Nuclear power particularly demands an attitude that prioritizes safety and quality before quantity; safety has, then, at least equal consideration to business factors such as profit or production. An integrated view of safety implies furthermore that the long-range perspective should take precedence over short-range demands that can result in false economies, along with risk to the public.

One point of departure for organizing disparate good practices and observations is a framework that examines the process of problem-solving or adaptation. This framework emphasizes how plants continually improve their practices by internal and external feedback systems, rather than the particular content of the practices themselves. We schematize the three most complex and critical moments of this process:

4.1 Setting and Re-Setting Goals/Policies.

Management's first responsibility is to establish and promulgate clear safety policies for and to every level of the organization. A second responsibility is to establish an assessment process that evaluates the relationship between policies and practices, in order to improve both as needed. On-going programs for safety improvement should be part of the organization's regular planning process.

Management should pay attention both to details and to the big picture in the process of setting plant goals. Management should ensure that the goals are clear and understood among all affected parties. This requires time for discussion among a broad group including workers and regulators.

Management should assure common understanding of the whole process of setting goals, sensing needs for improvements and implementing them. Again, time spent in preparation will ensure that affected parties understand the need for new practices and the way in which the organization has planned a transition from current procedures to new ones. This includes an understanding of how goal accomplishment will be measured.

In the definition goals and policies it is still a need to define responsibilities and accountability at each level of the organization. A superficial assessment process cannot be expected to function.

4.2 Sensing and Diagnosing Conditions.

Management needs tools that can systematically gather basic data on performance and then analyze their significance and organizational implications. Once the implications of the analysis are understood, new solutions and new approaches can be generated. More kinds of knowledge than are conventionally relied on in technical environments are necessary for understanding plant practices, especially data on human organization and management in such areas as operations and maintenance.

Diagnosing current practices requires broad sensing of the internal and external environment. The industry can no longer think of itself as insulated and protected from the environment. Taboos on considering safety and performance relevant information cannot be tolerated, either within or outside the plants. Internal to the plant, information should be sought across functional areas. Everyone should feel that they have a contribution to make in identifying areas where improvements to safety are appropriate. External to the plant, information should be sought from many areas of the environment, including vendors, suppliers, regulators, other utilities (of whom those with similar plants, practices, or problems may be most informative), public interest groups, and other industries (such as chemical process, airlines, military). Mechanisms for information exchange provided by IAEA, INPO, NUMARC, WANO and so forth should be utilized actively.

The information required for an assessment includes goals and expectations, the outcomes or products of practices, the opinions of those in the work system who carry out or are affected by the practices, and external information about similar situations in other nuclear power plants or other industries. The use of outside observers or the rotation of plant personnel to external posts can assist in providing such comparisons. Assessment involves comparisons between outcomes and goals or expectations. Trends over time can be particularly valuable, since changes in practices have delayed effects on outcomes. The better our understanding of goals and outcomes and our conceptual models of plants, the easier it is to attribute changes in outcomes to changes in practices.

A fault-free or blame-free system of error detection and reporting is critical to effective safety management. A balance should be sought between, on the one hand, appropriate and just sanctions for failing to perform appropriately and, on the other, a managerial environment supporting the active search for precursors and unsafe conditions. The detection of problems with current practices or with an implementation effort should be encouraged by accepting "bad news" as an opportunity for learning rather than an occasion for blame and punishment. Punishment tends to prevent the flow of information and thus reduces the capacity of the organization to adapt.

Determining the salience and relevance of each of the many sources of data and information requires conceptual frameworks that place them in proper contexts. People in the plant become maximally useful for detecting information and developing solutions to problems when they have a broad understanding of the relationships among work systems. The importance of systems understanding for all employees cannot be overemphasized; efforts to provide more generalists training, cross-training, etc. will contribute to the goal of transforming data to information. Managers with knowledge of systems details and workers with knowledge of the larger, more global picture of work systems and the organization are equally important.

Assessment should provide sufficient detail to distinguish good and bad aspects of any management practice. Even systems that are working well may have areas in which improvements can be made. Also systems that are working poorly may have useful ideas that can be the core of new practices. Assessment practices should have usable outcomes. They should be reviewed and used in the process of proposing future plans covering plant safety, worker safety, regulatory compliance, resource allocation, and so forth.

Root cause analysis is presently the chief example of a major diagnostic tool for determining the most informative interpretation of operational data, and its further development and refinement deserves high priority in both research and practice.

4.3 Implementation of New Policies.

Good communications is the key to implementation. This is enhanced by an open, inquiring atmosphere, shared understandings implying some breadth of knowledge, common language for discussing safety and organizational issues, and other aspects that are the products of management attitudes, personnel systems, and training. Implementation of new practices is another opportunity to learn. Follow-ups are essential to capitalize on that learning to improve the implementation process. Thus, evaluation of new practices should be built into the system. For example, OSART and ASSET are now carrying out follow-up missions that provide further information on plants and on the nature of the response to such missions that are useful for assessing the missions themselves.

The implementation process must be designed with an understanding of contingencies that affect quality such as (but not restricted to): career paths, union structure, authority beliefs, education and skill level of work force, regulatory structure, ownership structure of the utility, and strategic resource constraints arising from the market and business conditions of the utility.

The primary resource for the development, implementation, and use of good practices is people who have the skills, commitment, and resources. It is critical that the organization place high priority on maintaining and developing human resources. This would include a concern for the career path of people in the organization, the conditions necessary to maintain commitment, and the long-term integrity of the organizational knowledge base involving succession/turnover, skill development, and ways to share and preserve knowledge possessed by individuals. For example, if young people see no career prospects in the industry, then only lower-quality people will enter the industry, resulting in a degradation of the human resource.

The additional demands placed upon management, including top management and first-line supervisors, to strive constantly for good practices and safety, should be supported through management skills development. Management skills development should include goal setting, resource allocation, team building, communication, and conceptual frameworks. Pressures on first-line supervisors should be recognized, and appropriate resources brought to bear in terms of good communications, conceptual frameworks, and skill building. These things take time to fully develop. The automatic response of simply adding more managers may be counterproductive by adding to the coordination complexity and further reducing available resources.

Implementation should include a self-check system in which workers and managers are considered responsible for their own actions. Although there will always be monitoring and quality checks, everyone should feel responsible for what they do. Responsibility and accountability for performance should be enforced by the entire line organization. Managers should look for opportunities to hold people accountable in a constructive way. Managers should also demonstrate their commitment to safety through attention and consistent actions.

The additional demands placed on everyone to process more information should also be recognized. Appropriate strategies are to spread information processing over time (permit time for training and skill development), over people (accept input and participation from, and delegate responsibility to, those lower in the organization), and provide better mechanisms for handling information such as better conceptual frameworks for understanding the plant and computer support.

Resource allocation is an important way of communicating and supporting goals in organizations. This does not substitute for the communication of goals by written, verbal and other techniques. Thus progress can be made towards achieving goals through good line management and supporting line management where resource allocation is required. Resources must be allocated appropriately up and down the organizations.

5. Conclusions and Recommendations.

Proposals for future action. Apart from the various proposals already made above, the following general proposals are made to promote theoretical understanding of industrial safety

There is a need for providing better access to and analyses of existing data bases (reports, quantitative, qualitative, methods) on international, national, company, industrial levels.

Respecting the needs for anonymity, an awareness of all parties involved should be created that the demands of developing adequate theory of safety management requires empirical evidence available only through cooperatively developed programs of studies in operating plants.

A program of basic studies of psychological and social processes are necessary for understanding the fundamental dynamics involved in such puzzling issues as, for example, why the development of safety programs so often depends on the experience of a serious incident in an industry.

There is a need for a better definition of performance in safety oriented organizations and the identification of good practices. Because of changes in standards and conditions of operations, good practices should always be seen as transitory. They must continually be re-evaluated in the context of the day and of developing trends. Because the contribution of a practice to safety performance depends upon its relationship with other elements of the management and organization system at an NPP, along with the special constraints facing that NPP, highly detailed and prescriptive good practices that fit the needs of all or many NPPs are unlikely to be identified. Instead, it is more useful to identify "good principles" which must then be made operational in the context of the particular NPP with management and organization strategies that make sense in that context.

There are a number of research questions which may be taken up for further investigations. At the institutional level such questions are:

- How does a situation of economic scarcity (or economic bounty) affect the ability of management to assure the safe operation of the plant?

- How does the extent and nature of integration of the industry affect the ability of management to assure the safe operation of the plant? For example, what different management issues are raised for utilities in highly integrated industries (eg. Japan) versus utilities in somewhat less integrated industries (eg. U.S.)?

- What regulatory philosophies and approaches promote or inhibit effective management for safety at the plant level? How can management provide the right kind of buffer between the regulator and the day to day operation of the plant?

Some of the suggestions for future investigations within the companies may include the following considerations:

- The role of chairman/chief executive in safety, how they communicate their expectations, how they demonstrate their own commitment and how they ensure accountability throughout their organizations.

- The use of the root cause analysis technology in identifying organizational deficiencies and in improving organizational efficiency.

- The design of efficient means of achieving commitment and involvement of employees at all levels; what are the best ways of communicating with employees on issues of safety.

6. References

Argyris, Ch. (1970), Intervention theory and method, Addison-Wesely, Reading, MA.

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

Janis, I.L. (1972), Victims of groupthink, Moughton Mifflin, Boston.

Janis, I.L., Mann, L. (1976), Decision making, a psychological analysis of conflict, choice and commitment, New York.

Jungermann, H., Rohrmann, B., Wiedemann, P.M. (1990), Riskokonzepte, Risikokonflikte, Risikokommunikation, Kernforschungsanlage Jülich GmbH, Jülich, Germany.

Perrow, C. (1984), Normal accidents, Basic Books, New York.

Rasmussen, J. (1989), Human errors and the problem of causality in analysis of accidents, unpublished paper.

Renn, O. Swaton, E. (1984), Psychological and sociological approaches to study risk perception, Environment International, Vol.10, pp.557-575.

28.8.1991

APPENDIX A

EXAMPLE GOOD PRACTICES

1. SAFETY CULTURE

The essential prerequisite for achieving high safety standards is a clear and unambiguous policy statement. The policy should address the prevention of ill-health and injury to all employees and the public and should make it clear that ALL injuries and events are significant. Classification of injuries as not being of safety significance because they are below scale on the INES should not be allowed. Otherwise two separate safety systems will exist in one organization - a nuclear safety system and industrial an safety system.

Total commitment to safety by all employees in an organization can only created when they recognize their own personal responsibility for safety and believe that there is genuine concern by management for their personal welfare. Achievement of total system safety, both human and technical is dependent on the existence of a single safety culture which must be properly defined.

Attention is drawn to the definition of safety culture (cf. Box 2) in Safety series No 75-INSAG-4. This definition is somewhat restricted because it addresses only nuclear safety. It is suggested that consideration be given to amending "Nuclear plant safety issues" to "All safety issues".

It is extremely unusual to find any other type of industry, and particularly in the large process industries, where there is such a sharp distinction between industrial and technical safety.

Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.

Policy level commitment
- statement of safety policy
- management structures
- resources
- self-regulation

Managers commitment
- definition of responsibilities
- definition and control of safety practices
- qualifications and training
- rewards and sanctions
- audit, review and comparison

Individuals commitment
- questioning attitude
- rigorous and prudent approach
- communication

Box 2. The definition of Safety Culture and its major components.

2. POLICY

The policy statement in which management commitment and objectives are defined should include the following features:

- safety is given at least equal consideration to any other business factors such as profit or production
- safety is a line management responsibility and must be exercised at each level of the organization
- regular review of safety performance at each level from the board of directors downwards
- On-going programs on safety improvements are included in the annual planning process of the organization; progress is regularly monitored.
- involvement of all employees in safety
- avoidance of injuries to all employees and the public and damage to the environment and property.

3. POLICY IMPLEMENTATION

Implementation of policy requires the following:

- key performance goals must be set which are realistic and capable of being realized. Related performance indicators must be clearly defined.
- All managers must demonstrate their commitment to safety through their actions.
- Audits of safety standards and practices, both internal and external, must be regularly carried out. Both management systems and technical systems should be included.
- The organization should expect contractors operating on its behalf to achieve the same standards of safety as itself.

4. ORGANIZATIONAL REQUIREMENTS

In addition to the policy itself a statement of arrangements for meeting policy requirements within the organization should be produced. This should include

- Statements of line responsibilities and accountabilities at each level in the organization. Advisory roles should also be defined.
- Specific arrangements for the involvement of all employees in safety.
- Requirement for each unit to have a detailed operating procedures manual including a comprehensive safety section.
- Details of safety review processes.
- Training arrangements.
- Use of personal protective equipment.
- Emergency response arrangements.
- First aid and ambulance arrangements.
- Incident investigation procedures including root cause analysis and follow up.
- Arrangements for communication on safety and reporting of safety performance to all employees.

The policy and arrangements should be communicated and explained to all employees.

5. OTHER CONSIDERATIONS

- Project development and approval must insure full compliance with company and regulatory standards for health, safety, and the environment.
- High design standards must be set and maintained. Standards must be revised in the light of experience.
- High quality safety advisers should be appointed and assignments in safety should be regarded as important in career development of potential senior managers.

APPENDIX B

ASPECTS OF SAFETY RELEVANT TO MANAGEMENT AND ORGANIZATION

The role of management in assuring safety performance has been discussed in general terms in the main text of this report. However, it is also useful to consider that many aspects of safety that can be linked to management and organization. The following list is intended to demonstrate such couplings.

SAFETY FAILURE MODE	POSSIBLE MANAGEMENT FAILURE
Non-availability of safety systems and equipment	Decision to excessively limit preventive maintenance due to budget considerations
Human actions leading to the initiation of plant transients	Inadequate communication between operations and maintenance about the availability of systems
Component failures leading to the initiation of plant transients	Inadequate emphasis by management on taking responsibility for quality
Human actions leading to the complication of transients	Inadequate management support of training including simulators
Component failures leading to the complication of plant transients	Inadequate management attention to setting maintenance priorities based on risk
Lack of protection of workers from radiation and other workplace hazards	Lack of management direction in planning of task activities
Inability to operate in a way that assures regulator and public confidence	Attitude on the part of management that outsiders have no legitimate concern with safety
Inability to control the volume of waste	Short-term orientation on the part management

APPENDIX C

Presentations by the participants

N. Adamova, A. Procenko:
Socio-psychological problems of risk perception and control in the USSR

J.S. Carroll, C. Perin:
Organization and Managmenet of Nuclear Power Plants for Safe Performance

J. Olson, J. Thurber:
Learning in nuclear power plants.

R. Nakazono:
Organization and management of WANO.

C. Perin:
Social and cultural logics of nuclear power plant operation.

A. Rastas:
Management related practices in Industrial Power Company Ltd (Finland).

B. Thomas:
The ASSET services: Prevention of incidents the path to excellence in operational safety.

B. Wahlström, E. Swaton:
Influence of organization and management on industrial safety.

B. Wilpert:
System safety and safety culture.

N. Adamova
A. Procenko

SOCIO-PSYCHOLOGICAL PROBLEMS OF RISK PERCEPTION AND CONTROL IN THE USSR

Though the main object of modern technologies is to make life safer (even in the sense that public enrichment leads to protection of its every member) people express increasing concern about the fact that instruments, which free man of natural dangers at the same time give rise to a new risk in their life.

It can be distinguished three main types of problems on risk contacts, on which we'll concentrate our attention:

a) Scientific and methodic problems of the very process of risk analysis and estimation considerably affecting the risk contacts;

b) Risk recipients and their informants problems;

c) Problems depending on the organs of power and political, economic and social system.

At first we'll make several explanations and notes on the first type difficults. Though they concern the scientific and methodic field of risk analysis and estimation, that seems to be the most common and undistinguished base for different countries, however, there are some features for our country in this field too.

Some problems on risk contacts arise from the absolute belief mistakenness in scientific researches on risk control and estimation and in the very contacts on risk. (In our country it's aggravated sometimes by inconfidence in science because of the Leesenko's teaching, anticybernetics, which discredited it). It can't demand for the dicision of all problems in the field of risk from information arising as the result of scientific researches. Very often the researches carried out can't answer the appearing questions and the results obtained are called in question.

"A" group problems in the USSR

1. Perhaps, lack of our modern safety concept should be considered the most important problem. There is a very wide spread and therefore particularly dangerous mistake in the public concept: all dangers and, hence, risk can be completely eliminated. It should be said that such a viewpoint is typical not only of people not dealing with this problem but also of some specialists. Its direct effect is the following idealist formula: any public health protection expenses are justified for there is no price for it. However, the only exuse of such a viewpoint is their professional ethics only: to make everithing possible to save the people's life. The following safety assuring principle reflects this viewpoint: introduction of all the protection measures, which are practically realizable, i.e. the establishment of danger level as low as practically achievable, called ALAPA. Such a principle seems to be extremely attractive but unscientific and impracticable in most cases, which are of practical importance. This principle is incorrect.

However, such an approach, unfortunataly, has become the state norm in some countries including the USSR on some problems. For example, such a basic document regulating the labour safety fundamentals in the USSR "System of labour safety standards" postulates: "Labour safety is the state of labour conditions when there is no industrial danger. But there are a lot of negative factors arising from the consecutive attemp to carry out this principle.

2. An important component part of risk control and analysis including contacts with public is the risks comparison. We have no such developed methods ready for use.

This methods should considerably be based on the technological schemes, methods and control equipment, types of equipment, regulations used in the USSR. Thus, many branches and kinds of activity aren't ready yet to the risk analysis, exciting the experts' and public confidence.

"B" group problems

The key question of risk understanding, important for the contacts with public can be summed up as following:

1. What social objects, values or reasons advance the persons or social groups when solving their individual attitude to the specific risk sources.

2. In what way people process the information on the risk sources and what logical structure and method of reasoning they keep to while giving full opinion on acceptability of risk they understood.

3. What base cognitive or motive is used when people select information from different sources available and why they break their own rules of understanding, analysis.

The feature of risk understanding and perception process in the USSR should be considered in the light of above-said. Let's consider possible effect of some phenomena, which have been appeared in the country lately.

1. Openness (glasnost)

The politics of openness realized lately has caused the development of some features in risk understanding and perception by the public and persons, making decision.

1.1. Those persons, who had no opportunity for many years to express and defend their opinions on risk problem, have obtained this opportunity now and realize it to the far greater degree than in other countries. The object of this statements is not only search for the better decision important for them, sometimes it's self-expression simply or expression of opinion on some risk not concerning its direct.

For example, people living a long way from atomic power stations (APS) sometimes speak more active than those living nearby.

1.2. Much improved information come off the press as the result that the opportunity has appeared "to speak all you want". But in the same way press, radio, TV gives much useful information on the risk sources, which were prohibited to speak about earlier and such information was withdrawn by censorial organs.

Other misunderstandings appear due to stereotypes dealing with the way the press and recipients perceive information on risk. For instance, it is mistaken to see journalists and press as essentially independant reason on risk contacts. The problem often lies on the border between science and journalists, press. Both sides rather need better understanding of the problems of each other than numerous complaints to the disappointing results of contacts.

1.3. Public participation in reaviling the enterprises, its production or some other activity, dealing with great risk, makes it easy the realization of work on risk optimisation on solving these problems.

Resume: it's necessary to reveal the groups of people, acting reasonably and rationally and to encourage their assistance in its activity.

1.4. The flow of claims and proporsals from public has grown rapidly on risk and safety problems to those, often not dealing with the problems touched upon, and the fact that there are no answres from them, its delay, diversification, incompetence and sometimes simply contradictoriness provoke people, spread distrust in administrative, managerment istitutions and often leads to nihilism aggravated.

2. Political movements. Social organizations. Careerism.

At the glastnost and political changes period many different political movements and parties have appeared and appear now in the country as well as different social organizations including those armed with the aimes and slogans, concerning the man and nature safety. Just the same is observed among the persons who decided to devote themselves to political, social or administrative activity.

It has the following effects:

2.1. Potentially strong support on the side of all these movements for the development of necessary structures for solving the risk analysis and control tasks and human health and environment protection problems (scientific research, examinations, educational and informational works arrangement among public, real steps on risk control etc.) already gives and will give positive results.

2.2. At the same time certain movements and organizations use struggle against the existence of some plant, power station, production to achieve their political aimes only, without thinking of the effects of these actions; it's important for them this struggle to become a certain symbol, under which people should unite, considering that they fight against stagnation phenomena.

2.3. Many people have obtained opportunity now through elections to take part as leaders in political, social, administrative activity. Among them there are somebody, who actively use popular slogans to provide their own career. Using public lack of information, incompetence, they put forward the slogans or support the movements including those supposedly aimed at ensuring the necessary environment conditions and human safety and really causing damage to his life.

3. Secrecy

The system of restricting redundant and irregular from the viewpoint of formation has existed for years and existing now results in:

3.1. The public as well as state and local organs of power or specialists have no information they need. It gives rise to the contradictory reports of these organs on risk, provokes public inconfidence in these organs and, hence, makes their contacts on risk with public ineffective.

3.2. Lack of official information enjoing the confidence is one of the main reason for hearsays appearing and their distribution among population; for the same reason the information obtained as the result of contacts with friends and acquaintances enjoys much confidence.

For instance, the research carried out by the group of sociologists in Gorky, 1989, in connection with atomic heat supply station has paid attention to the public attitude to different sources of information. The analysis shows that on confidence degree the information obtained from talks with friends and acquaintances takes the 3-d place after the information obtained from specialists, and information from meetings with local powres found itself on confidence degree on the 13-14-th place. Though it's rather unexpectedly the inhabitants of this town moved the hearsays to the 15-th place.

GORKY INHABITANTS' CONFIDENCE IN DIFFERENT SOURCES OF INFORMATION (DATA OBTAINED IN CONNECTION WITH THE DISCUSSION OF ATOMIC STATION PROBLEM)

Source of information	Confidence degree
1. Meetings with specialists	1-2
2. "Leninskaya Smena" newspaper	1-2
3. Conversations with friends, acquaintances	3
4. Other sources: press, radio, TV	4-10
5. Statements at meetings	10
6. Meetings with informals' leaders	11
7. "Voices" of foreign radio stations	12
8. Meetings with local powers	13-14
9. Hearsays	15

"C" group problems

1. Political and socio-economic situation in the country that existed and existing now has deformated greatly some public priorities in different fields of life in comparison with other technically developed countries. Therefore it's difficult and sometimes incorrect to rely on experience, methods and recommendations obtained in these countries. In any case its should be handled with much care.

Unfortunately, periodical study of public opinion by means of public opinion poll is in its initial stage now in our country. It concerns the field of human and environment safety. We have only fragmentary data often with lack of statistics and incomparable with data availible of other mainly foreign researches. However, let's give the results of the research, which still illustrates the public position unexpectedness on risk in deeper understanding (i.e. not only natural or technological accidents risk or other dangerous activities, but also risk dealing with socio-economic processes).

PROBLEMS CONSTITUTING MAIN PUBLIC FEAR AND ANXIETY SOURCES

Phenomenon, field of activity	Rank
1. Crime growth including organized one .	1
2. Environment pollution	2 [1] (4,2,4,4)
3. Atomic power station building	3 [2] (1,1,3,3)
4. Low level of medical care	4
5. The cost of living growth	5
6. AID distribution	6
7. Lack of necessary goods	7
8. Alcoholism growth	8 [3] (3,4,2,1)
9. Drug and toxic addiction distribution	9

10. Lack of discipline and order 10
11. Thermonuclear war threat 11
12. Dissoluteness 12
13. Low level of democracy 13
14. Road-transport accidents .... 14 [4] (2,3,1,2)

Figures in brackets mean the following: in square brackets are the ranks of four chosen technological risks from the given list; in round brackets - the first figure is the women' opinion, the second is the students' one, the third is the businessmen', the fourth is statistic data on fatal outcomes from the mentioned reasons.

2. The economic situation which has been established, the forms of property in natural resources including, lead to irresponsibility in respect of nature protection: as a matter of fact there are no prices for water, earth and other natural resources; in conditions of lack of private, cooperative and other kinds of unstate properties it's practically impossible to protect something from somebody. Hence, it follows a very poor public activity on nature protection (all state means no one's), green peace movements are headed by separate organizations and their leaders.

3. Lack of strong system of responsibility for risk analysis and control.

A lot of organs of control on different level are or to be responsible for human and nature safety and, hence, to carry out contacts with population on the problems of risk control.

In the conditions of unclearly determined responsibility for the information and dicisions adopted, public confidence in opinions and dicisions of some officials and specialists considerably falls.

3.1. Openness. Contacts on risk is a double-sided street. This bilateral process must show the spirit of open exange for muttual understanding and not a series of reports for local powers and public.

The organizers of meetings with public and local state and social organs usually consider these contacts as the mean of introduction of their concepts or the instrument of education of uninformed public only. In this case it's impossible to achieve the objects needed.

3.2. Use of "affecting strategies". Those responsible for the risk analysis and control in the ministries and departments, at the enterprices practiclly always use the "affecting strategies" method in contacts, making possible to substate the viewpoint of their interest and need while composing reports.

4. Extreme monopolism in the field of control and production as well as scientific and technical.

In the field of production it:

- makes the exposure and introduction of technologies optimal from the viewpoint of risk;

- hampers realization of some sanctions against enterprices, departments;

- public don't believes in departments, their wish to reduce risk as in conditions of lack of competition monopolists have no stimuli to do it.

In the field science and technology it:

- doesn't stimulate the development of new progressive technologies and, hence, results in the public inconfidence in researches and resumes of the branch science.

CONCLUSION

At the same time political, social activity of people in the USSR at present and strong dynamism of phenomena in different fields of social, political, economic, spiritual life create the unique conditions for studing public opinion on the problems of interest with the aim to improve theory and to develop proper organization and methods of work on contacts with public, risk control. Besides the conditions mentioned below, it favour the following factors:

- prompt feedback in the process "information on some activity or object - contacts with population - response - decision - second response";

- presence of factor of muss undisguised public behaviour in the situations attended by risk (flat objection to some dangerous technologies, unceasing process of technological and natural accidents, absentee earlier in the USSR).

Such researches are of great value not for the USSR only but for other countries too, obtaining unique opportunity to get important scientific data in the field of contacts with population on risk and its control. (Perhaps, it should think of organization of researches together with foreign organizations and specialists).

Massachusetts Institute of Technology

Center for Energy Policy Research

THE MIT INTERNATIONAL PROGRAM
FOR ENHANCED NUCLEAR POWER PLANT SAFETY

Organization and Management of Nuclear Power Plants for Safe Performance

Progress Report

Excerpted from NSP 91-002PR **June 1991**

A Joint Center of the Department of Economics, Energy Laboratory, and Alfred P. Sloan School of Management

E52-590
Sloan School of Management
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

John S. Carroll
Professor of
Behavioral and Policy Sciences

Telephone: (617) 253-2617

This report covers our first year of studies of enhancing nuclear power plant safety, and as such it should be read as work-in-progress only. We are glad to share it widely, however, in order to contribute to ongoing discussions of research design, methods, and goals. We welcome comments and references.

John S. Carroll

Constance Perin

THE MIT INTERNATIONAL PROGRAM FOR
ENHANCED NUCLEAR POWER PLANT SAFETY

Organization and Management of Nuclear Power Plants for Safe Performance

Progress Report

Excerpted from
January 1990 - June 1991
Progress Report

June 1991

This is the second progress report for the MIT International Program for Enhanced Nuclear Power Plant Safety. It is our plan to publish two reports each year: a mid-year report in January and this annual report. Reports will be provided to all program participants and sponsors.

THE MIT INTERNATIONAL PROGRAM FOR ENHANCED NUCLEAR POWER PLANT SAFETY

BACKGROUND

The MIT International Program for Enhanced Nuclear Power Plant Safety is a cooperative research program developed to create new knowledge of and insight into nuclear power plant operations so as to enhance safety. The program is international in its scope and participation because the issue of nuclear safety is itself an international issue–a serious accident at any specific nuclear plant will have a profound effect on every nuclear plant in the world. And the program focuses upon operating plants rather than new design concepts because the creation of improved practices, procedures, policies, and structures can help sustain the nuclear option worldwide. Finally, the range of work is much broader than technology but encompasses managerial and policy-related research as well.

The foundations upon which the program is built are five-fold:

-- The sponsors must be distributed from around the world and represent all the major nuclear nations.

-- Sponsors must be active participants in the program, sharing knowledge, experience, personnel, and critical judgment.

-- The research projects must reflect the priorities of the worldwide industry to assure relevance as well as interest.

-- The program must be multidisciplinary to reflect the true dimensions of the problem of safe operations.

-- The focus of the work must be located at a disinterested organization (such as MIT) to assure the perception and reality of neutrality regarding specific research results.

There are other national and international organizations with deep interests in nuclear safety. Within the United States we have the Electric Power Research Institute and the Institute of Nuclear Power Operations; the most prominent international organizations are the World Association of Nuclear Operators, the Nuclear Energy Agency of the OECD, and the International Atomic Energy Agency. All of these organizations are major contributors to improved plant safety and operations. We believe our program fills an important niche and is complementary to these existing efforts, and we believe it is important for our program to be cooperative with those efforts. The program is a vehicle to conduct research that is relevant to safety, that is credible to the international nuclear community, and whose results are available to all.

At the initial meeting of program sponsors in June 1990, we presented the three major program areas and a set of projects within the areas. The program areas are:

(1) The Science and Technology of Service and Maintenance;

(2) The Science of Management of Nuclear Power Plants; and

(3) The Role of Public Policy in the Safe Operation of Nuclear Power Plants.

The current level of funding for the program supports four projects: three in the Service and Maintenance area and the one in the Science of Management area. As sponsorship funding increases, we will begin other projects.

Organization and Management of Nuclear Power Plants for Safe Performance

ANNUAL REPORT
JUNE 1991

Prepared by
John S. Carroll, Professor, Sloan School of Management
Constance Perin, Research Associate, Sloan School of Management

INTRODUCTION AND BACKGROUND

The Need for This Project

The organization and management component of the The MIT International Program on Enhanced Nuclear Power Plant Safety addresses the following question:

> *How should nuclear power plants organize and manage their human and technological resources to maximize their safe and efficient operation?*

The importance of management and organizational factors is confirmed by research on predictors of variation in performance and safety. The USA, with its large number of utilities and early entry into the industry, has the highest diversity among nations in technology and in performance. Although research shows some impact of technology (Beckjord et al., 1987; INPO, 1988; Samanta et al., 1988), regulatory structure (Suzuki & Hansen, 1988), and industrial structure (Lester, 1986), much of the variability in performance cannot be attributed to these factors. For example, Swiss and Japanese plants operate at similar very high levels of utilization (power production as a percent of potential production) and they have very few unplanned outages or other safety incidents, although their reactors vary substantially in design (Beckjord et al., 1987).

Yet it comes as a challenge to current organization theory to account for organizational and management factors in "high-reliability organizations" such as nuclear plants, chemical process plants, nuclear aircraft carriers, and air traffic control. Conventional organizational theory, having been developed in "trial-and-error" organizations, may need to be modified to address the organizational, managerial, and resource issues central to the safety dynamics of high reliability organizations, which are characterized by tightly coupled subsystems whose misalignment bears the potential for grave consequences (LaPorte & Consolini, 1989; Perrow, 1984).

This project is therefore different in several ways from current efforts to improve nuclear power plant operations and management. Most take place largely within a regulatory framework concerned with evaluating individual plant performance through quantifiable indicators that can be compared easily across plants. Regulators identify unsafe outcomes such as Licensee Event Reports, generic issues backlog, and unplanned outages. Such indicators of safe practices are of limited help in improving safety, according to close observers, because "they have been developed incrementally over time to deal with specific issues as they have arisen and are not part of a broader logical framework" (Marcus et al., 1990, p. 24). Only recently have the Nuclear Regulatory Commission and its researchers recognized these limitations to the theory and measurement of safety by calling for attention to "unsafe behaviors" as well as to unsafe outcomes.

We see the control, coordination, and communication practices that nuclear power plants use in carrying out work as holding the key to a broader logical framework through which to improve their organization and management for safe performance. Our project, moreover, takes this work systems approach within a research rather than a regulatory or evaluative mode. Without the implied threats and demands of that mode, we seek to describe and understand plant operations and provide systematic information about organizational and managerial processes implicated in safe performance. This approach is not limited to measures that will have direct regulatory usefulness, nor to measures that are quick and easy to develop.

This report presents some of what we have learned inductively from observing and analyzing the control, coordination, and communicative processes involved in work systems that are central to plant operations. Our studies have been supported by the interest in new ideas and willingness to cooperate among many nuclear power plant operators, industry groups, regulatory bodies, and research colleagues. During our field studies, we have been impressed with the high levels of conscientiousness and concern with continual self-improvement and learning among power plant staff at all levels.

OBJECTIVES

Currently, the industry relies on dissemination of reports of best practice from "successful" plants to improve technical, procedural, and managerial practices incrementally. Lists of desirable plant characteristics (e.g., Institute of Nuclear Power Operations, 1987) have similar intent. Although this approach is useful in the absence of a theoretical understanding of safety in high reliability organizations, we question its assumption that an unsystematic number of "best practices" can cumulatively improve safety performance. Similarly, Systematic Assessments of Licensee Performance and International Atomic Energy Agency (IAEA) advisory services staff their reviews by functional areas and provide recommendations and suggestions for improvement by functions, also assuming that functional integrity guarantees system integrity.

Instead, we view "best practices" along with industry traditions, assumptions, and experiences, as incipient theories of safe performance. Building on these, our aim is to develop a systematic basis for understanding variations in the organizational and management characteristics of safe performance, and thereby to establish the grounds for changes in fundamental organizational paradigms and values. A specific objective is to provide "self-design" tools for simulating the processes involved under different constraints, so that plant staff can select the most appropriate configuration and management policies for their organizational situation.

The Study of Work Systems

In looking at the social and cultural organization of plants' work systems -- e.g., preparation of maintenance work packages, planning and scheduling, performing surveillances, staff recruitment and training -- we intend to complement previous work on reducing human error that focuses on individual behavior. Rather than focusing on single variables, work systems represent the interdependencies of social and technical systems within nuclear power plants (Egan, 1982; Rasmussen, 1988) as well as beyond them, to their complex institutional environments.

We begin by taking note of the dynamics of the production process itself. Plant cycles are defined by anticipated refueling and maintenance outages; unplanned outages interrupt normal operations. The additional staff needed for planned outages increase the on-site population two- and three-fold. Coming down and starting up mark major transitions; shift changes signal minor transitions where good communication becomes essential. The tempos of work are also fluctuating -- even normal operations oscillate beyond a steady state now and then, when unexpected minor repairs are needed, for example. Such characteristics suggest that management must organize the dynamics of transitions, gaps, interstices, and fluctuations that are at the center of safe performance.

The technologies involved in producing electricity also share the characteristics of a dynamic system, given the high interdependency among components, large and small. These mandate a refined division of labor in which the design and operation of components and subsystems are assigned to specialists who must themselves collaborate and therefore understand enough about each others' area of expertise to communicate clearly. In nuclear power plants where the technology is organized as a series of barriers against core damage, all employees need to maximize their capacity to recognize problems and visualize their systemic implications. The dynamics of production therefore also include the tensions in the relationship between small details and larger systems, which also must be organized and managed to maximize safe performance.

The dynamics of plant cycles and those of components within technical systems demand a high level of attention, vigilance, compliance to procedures, communication within and across departments, and commitment to safety. The capacity of employees to meet these demands calls upon two underlying processes: First, to keep learning from their own and from others' experiences, and second, to maintain their "mental maps" of plant systems and the complexities of particular tasks in good repair. As will be seen in the outline of our second year of work, these two processes organize our search for more systematic footing for safe performance in nuclear power plants.

Research Phases

The overall plan of research consists of five phases or subgoals within the overall goal.

Phase 1: Description

The first step has been to develop preliminary data that represent the detail and complexity of the organizational and managerial dimensions of nuclear power plants' work systems. These describe how human and technical resources are related in practice, and how they are understood.

Phase 2: Concepts and Framework

We seek to understand these phenomena as being in some ways similar to other industrial and technological settings and in some ways unique to nuclear power plants. Our concepts must be broad and comprehensive enough to include several levels of analysis, such as the interactions between the plant, utility, customers, regulators, suppliers, unions and the public; the structure and culture of the plant and the relationships of its functional groups; the regional and national institutions, demography, and culture within which the plant operates; the dynamics of operator teams and other work groups; and individual decision making. The framework has to include adaptation to the internal and external demands on the organization as well as factors that enable and inhibit adaptation.

Phase 3: Properties and Configurations

The next task is to identify and/or represent patterns in the understanding, organization, and management of the production process. We will base these on both direct observations and trend data. Research procedures involve a range of activities including analyses of existing data, opinions of experts, intensive on-site fieldwork in selected plants, questionnaires, and studies of group behavior in control room simulators as well as in task forces and committees.

Phase 4: Prototypes/Demonstrations

Scenarios, configurations, and alignments for various work systems during each plant cycle will be described. Using questionnaires, interviews, on-site observation, and expert evaluation, we will ask those in each work system to review their practices against such alternatives. We will design research to follow changes, as invited.

Phase 5: Management Implementation

The knowledge we obtain from our research must translate into practical tools for safety enhancement as well as generating principles to guide organizational and managerial policies and practices. These are tasks for our sponsors as well as other utilities to undertake. To help make this transition, we will participate with them in a phase of "technology transfer."

Project sponsors and scientists agreed that the top priority in the first year was to pursue Phase 1 descriptive research and Phase 2 concept development. The fieldwork has included interviews, on-site observation, and examination of existing records in nuclear power plants and associated institutions (e.g., corporate offices and regulators) with the aim of developing careful portrayals of work systems, organizational processes including cross-boundary relationships, and institutional relationships.

The goal of fieldwork is not to develop single-site case studies but to outline the topography of nuclear power plants' work systems and activities in order to begin to analyze the organizational and managerial principles behind them. How a plant integrates functions and acknowledges interdependencies among work systems has been a focus for team training, field observations, and data interpretations, for example:

- Bridging between departments and shifts (e.g., shift supervisor on loan to scheduling department, job rotation).

- Tracking and analyzing plant data and developing plans to deal with their implications (e.g., interpreting industrial safety trends).
- Preparing work packages and scheduling work.
- Designing continuing training programs in all functions and at all levels.
- Prioritizing resources by functions.

RESEARCH PROGRAMS

Research Preparation

In July 1990, Dr. Perin made reconnaissance visits to two operating nuclear plants to consolidate the project's approach to intensive field studies. Based on interviews with plant staff about the work systems of various departments, we developed fieldwork strategies designed to maximize our observations of control, coordination, and communication processes; this work became one component of field worker training and site selection (Perin, August 1990; October 1990). Additionally, Dr. Carroll visited the Nuclear Regulatory Commission Region I offices to investigate the Systematic Assessment of Licensee Performance process through interviews with team members who had just completed the review of a plant.

During the fall of 1990, Prof. Carroll recruited and trained four research assistants to begin fieldwork. Ellen Banaghan, Juan Jaliff, Bhavya Lal, and George Roth have varying backgrounds in management research, nuclear engineering, and nuclear plant operations. Training included readings on organizations, nuclear power plants, and research methods, discussions, exercises, and a field trip to a nuclear power plant. Dr. Perin, other MIT faculty members, and two visitors with research experiences in nuclear power plants gave talks during the training phase: Alfred Marcus (University of Minnesota, senior author of NUREG/CR.5437 on organization/management indicators) and Anne Sutthoff (Science Applications International Corporation, who has visited over 40 plants to make assessments of emergency planning and organization/management characteristics).

Fieldwork and Analysis

USA Field Site Selection

A plan to select fieldwork sites was developed, based on several attributes: a comparison of technology (PWR vs. BWR), age (pre- vs. post-

TMI), plant-corporate relationship (sole nuclear site run by that company vs. one of several geographical sites), and operating history. These criteria were developed through discussions with faculty, sponsors, and other experts. Due to limited resources and the special difficulties of language barriers, site selection at this time was limited to USA plants. Profs. Hansen and Carroll contacted approximately 10 utilities to solicit cooperation.

After considerable negotiation, four utilities agreed to host a researcher at a plant:

Belvedere. Belvedere is a pre-TMI BWR plant that is the only nuclear station owned by a utility with several other fossil plants. After several years as a troubled plant, Belvedere has improved dramatically in the last several years.

Brigham. Brigham is technically a similar plant to Belvedere, owned by a company that manages only this plant. They have had a very good operating record, and operate the plant with fewer than one-third of the employees on-site at Belvedere.

Partridge. Partridge is a post-TMI PWR plant. It is one of several nuclear plants owned by its utility. It has had a good operating record.

Potomac. Potomac is also a post-TMI PWR plant but is the only nuclear station owned by a utility with several other fossil plants. Potomac has had an excellent record of operations.

USA Fieldwork and Analysis

Each research assistant spent three to four weeks at one plant, attending meetings, interviewing a broad range of staff in the plant and outside the plant, collecting relevant written materials, and observing work processes in detail. At the end of each day, they transcribed their fieldnotes on laptop computers.

Return visits of 2-5 days duration have already occurred to Partridge and Potomac plants, and others are scheduled. During these visits, team members examine changes, observe operations in different phases (e.g., scheduled outages), and ask new questions emerging during the team's analysis of field notes. They also present a summary of observations from the fieldwork, as a way of providing feedback, listening for reactions to test our understanding and reveal new information, and suggesting alternative ways for plant staff to think about their activities. As one plant manager put it to his staff, "The value to us of this research is a new perspective on what we take entirely for granted."

Since their return from the field in February, team members have met approximately twice a week. Members have organized and expanded their fieldnotes to capture important details and make them maximally usable as data sources. Our meetings are forums for wide-ranging, incremental discussions about our observations, comparisons across plants, and tentative interpretations. Team members have written memos about a range of topics, drawing primarily upon their own fieldnotes and experiences. This accumulation of memos, discussions and reactions has been coalescing into the conceptual framework that will guide our second year of refining issues, concepts, and work system configurations.

International Observations

To develop an international perspective within the team, Dr. Perin accompanied an Operational Safety Review Team (OSART) mission to a European plant and an Assessment of Safety Significant Events (ASSET) mission to a Latin American plant, as an observer at each under IAEA auspices. All IAEA missions are conducted by volunteers recruited from operating plants around the world; each team member is an expert in a functional area. The three-week OSART mission was one of the largest, with 17 members from Western and Eastern European Countries and North America. The two-week ASSET mission, with an international team of ten experts, was held at a newly commissioned plant operating for just eight months. Dr. Perin observed plant operations and took note of the understandings of safety and plant management and organization underlying the team members' assessments. She also interviewed them individually about their home plants' operations for their insights into organizational and managerial issues.

At the invitation of the IAEA and the International Institute for Applied Systems Analysis (IIASA), Dr. Carroll and Dr. Perin participated in a week-long technical workshop in Vienna and Laxenburg on "The Influence of Organization and Management on the Safety of NPPs and Other Complex Industrial Systems" (see Section 6.4). The workshop was attended by European and Japanese nuclear power and oil industry experts, behavioral scientists conducting research in nuclear power plants, and representatives of WANO and IAEA. The group drafted a report outlining a research agenda.

In May, the researcher who had visited the Potomac site will spend approximately one week at a German PWR plant. This will provide not only information about this plant, but also help us better design longer data-gathering visits to plants in France and Japan (see Section 6.0).

RESEARCH RESULTS

Based on five person-months of on-site observations at nuclear power plants in the USA and abroad, the research results at a first level of analysis can best be understood as a set of observations about plants' work systems and conceptual or mental models. When organized by plant, these observations provide a "case study" of separate plants. Two of our research assistants wrote Master's Theses based on their field experiences (Banaghan, 1991; Jaliff, 1991). However, the major purpose of the research is not to "assess" plants, nor is even one month of study is sufficient to "understand" a plant. More importantly, we have been using our collective work to develop hypotheses to guide future detailed studies.

Observations

In our memos and discussions, team members present observations and issues in various ways. The first step is simply to notice something, separate it out as an "observation," and present it as interesting or relevant. As these are discussed and related observations are brought up, the discussion moves toward greater understanding in unanticipated ways.

- Observation #1: At Potomac, management instituted "generic work requests" designed to deal with hot jobs or minor items. The usual instructions to an Instrumentation and Control (I&C) technician might be "troubleshoot, repair and replace as necessary." These came to be overused for all kinds of general activities in order to speed up work and reduce paper flow. Craftspeople insist that about half of all such work requests ought to be regular ones.

- Observation #2: At Brigham, work processes depend on face-to-face contact and knowledge of individuals' skills. The assistant foreman of I&C talks to the Shift Supervisor (SS) upon arrival at 7 a.m. By the time Maintenance Work Requests (MWRs) are discussed in the daily operations meeting at 8 a.m., work has already begun on some items, preceding the paper work.

- Observation #3: At Potomac, coordination between control room, maintenance, and scheduling is carried out by a SS on Loan, who is rotated through this position.

- Observation #4: At Brigham, a position was created in 1989 called Operations Planning Coordinator, who must understand the work that needs to be done and ensure coordination between workers and shift supervisor. The OPC was a Control Room Operator who spent a year working for the Maintenance Foreman, and thus was in a good position to know the work and the individuals.

- Observation #5: At Partridge, for easy maintenance work, a Leak Crew consisting of an operations person and a maintenance person provides a fast way to do these jobs. These jobs are at the discretion of the SS.

- Observation #6: At Belvedere, Maintenance Work Packages are written by a separate Planning group, who are part of a separate department reporting to the VP of Nuclear Operations. Belvedere locates its Planners next-door to both maintenance and ALARA, which enhances coordination.

- Observation #7: At Brigham, people log MWRs in a log book on the SS's desk. This naturally involves some face-to-face interaction that can be important in providing extra information, especially if key safety systems are involved. Similarly, in a European plant, every work package is hand-carried to the control room where the craftsperson and the SS conduct a "face-to-face" so that each has a clear understanding of the scope and implications of the work.

- Observation #8: At Partridge, the MWR procedure has MWRs go through a SS and then to an Operating Engineer (there are 3 OEs for 2 units, each requiring an SRO license). However, there is instead an MWR Coordinator who has signature authority for the OEs, and who runs a meeting every morning to coordinate reviews among ALARA, maintenance, and fire marshall.

- Observation #9: At Belvedere, operations gets excellent training, but craft are given basic training without systems training (nor do clerical staff get systems training). Similarly, at a well-functioning European plant, an OSART team found that technicians skilled in one specialty were unconcerned with how it fit with the next. They didn't follow through on or regard themselves as accountable for the ultimate outcome of the larger piece of work to which they had contributed.

- Observation #10: At Brigham, the daily operations meeting is attended by foremen and assistant foremen level, who are considered "the people who run the plant." Managers who run special meetings (ALARA review, Quality Audit Exist, outage work) facilitate discussion of issues and ask for recommendations of workers for proposed actions.

- Observation #11: At Partridge, there were many separate people and programs working toward improving the plant, scattered all over. They began to realize that "if you put the problems in little boxes you never find the big problems." Now they are trying to slowly incorporate all the investigations of issues into the Deviation Reporting process.

- Observation #12: Many of the procedures at Belvedere were written by external consultants; as a result, some procedures ignore plant layout or have become outdated. Updates are being done without the systematic participation of the craft.

- Observation #13: The BWR specialist on an ASSET team suggested that vacuum breaker failure can result from the presence of hydrogen which causes internal explosions. Breaker failures have conventionally been attributed to manufacturing defects. His own plant had this problem, yet his BWR users group could not accept the possibility until one of them also experienced it.

- Observation #14: At Partridge, there is a very extensive performance appraisal process for managers and professionals, including assessments of skill development, which has noticeable impact on wages. However, the performance appraisal for union workers is abbreviated, provides little feedback, and has little impact on wages.

Inferences and Issues

The discussion of such observations involves trying out various comparisons and inferences. These are tested in team meetings, where consistent and inconsistent observations are discussed. Building on these observations, our analyses evolve into layers of understanding of the nature of and relationships among these observations. This particular set of observations might generate a set of simple comparisons or first-order inferences: (1) the MWR procedure is complex because it involves several steps and coordination among different functional groups; (2) different plants set up the structure in different ways. Variations include the number of separate groups and the nature of reporting relationships; (3) there are various complaints that people do not know how their own tasks fit into the bigger picture of the plant.

Continued discussion often leads to somewhat deeper understanding, or second-order inferences: (1) several plants seem to find liaison or linking roles between Operations and Maintenance to be important, and the incumbent of this linking role must have sufficient experience and credibility to different groups, sometimes provided by job rotation; (2) because the MWR process is so cumbersome, procedures have been created to expedite simpler work; (3) there are several examples of practices (behaviors) that diverge from procedures, or where important consequences of the way things are done (e.g., face-to-face discussions) are not explicitly recognized in the procedures; (4) plants differ in how much participation is encouraged from craft/union employees.

Going yet further, we might generate third-order inferences from these observations and inferences: (1) The continual process of bridging gaps formed by the dynamics of the production process occurs on two levels: social and conceptual. On the social level, organizational mechanisms are used to integrate across occupational groupings, organizational units, and geographical spaces. On the conceptual level, as specialists, people have to live in their "small worlds"; yet, they are called upon to include in their "mental models" of their work the interdependencies within a bigger picture. Some of this gap-filling is done by linking structures and procedures that enforce the exchange of information; some is done by job rotation, cross-training, and systems training; some is done by task forces that assemble broad knowledge and create cross-training situations; much is accomplished by informal means including personal communication (often face-to-face) and the proximity of units to facilitate such communication; (2) There is a continual process of adaptation occurring as plants experience their own problems or issues and try to deal with them. Plants are frequently innovating in structures and procedures, resulting in even more variety among plants. This innovation is at every level of the organization, and includes situations where more effective and/or efficient practices have diverged from procedures. "Compliance" seems to be an overly-simplistic way to characterize good plants, because it presumes a higher degree of stability than observed.

From these inferences, we can further distill our observations into "issues" that seem to capture important concerns or tensions in management and organization. Each issue represents a choice or variation:

- The plant may have cultures that support safety and effective operations or that place safety in a lesser role. Cultures may be carried by employees having different occupational histories, such as those previously working in the Navy or in fossil plants or those trained in the Midwest work ethic, or cultures may be defined within the plant by the values and standards of managers and other key personnel.

- Plant employees may value excellence and continual improvement, or they may be satisfied with the status quo, what is often called "complacency."

- The plant management may respond to corporate demands for efficient power production and profit or it may demand recognition of the special needs and circumstances of nuclear power.

- Plant employees may see the institutional environment as full of opportunities and proactively manage this environment by selectively adopting elements provided by the NRC, INPO, consultants, or they may see that environment as posing threats that must be defended against or minimally responded to.

- Plant management may understand safety as an "add-on" to production technology or as being integral to all activities.

- Plant employees are continually managing normal operations, yet must prepare for transitions to outages; they must act in both "worlds" at the same time.

- Plants are structured as functional organizations, yet their daily work systems cut across functions and require constant interfaces of departmentalized groups.

- Plants can rely on proceduralization, with procedures written by those who have the authority to write them, or plants can trust the skills and training of employees by permitting those closest to the work to determine the details of activities and to contribute to procedure writing.

- Plants can have easy communication between groups or have barriers arising from bureaucratic procedures, different "mental models," or physical location that prevent the flow of information.

- Plants can base their training on a systems perspective that recognizes that all employees should understand how their work fits into the bigger picture, utilizing cross-training, job rotation, or other mechanisms, or can maintain a specialist focus to assure efficiency.

- Plants can create an atmosphere in which errors are avoided and information about problems is concealed, or can structure incentives to reward error-acknowledgement in the interests of continual improvement, without encouraging error.

The Management and Organizational Implications of an Incident

The case of an "Unusual Event" observed at one of our four plants illustrates the kinds of questions our research approach to work systems can raise about the dynamics of daily operations and safe performance. Although reportable in that category by NRC regulations and therefore a factor in the NRC's future Systematic Assessments of Licensee Performance (SALP), this event occurred in the balance-of-plant and did not degrade any barriers to nuclear safety systems; the plant responded well. Especially because it is only an "Unusual Event," we see it as an important pointer to broader questions for our study, which we raise below.

Roof Fire in Turbine Building

A ceiling fan installed over two feedpumps in the turbine building fell down. The fan bounced off a steel beam on its way down and hit the floor, not the equipment. No one was injured. The other two fans were then secured with rope, on the theory that continuous vibrations had weakened the third fan's supports. The feedpumps were protected with scaffolding.

Maintenance and Engineering debated how to repair the remaining fans, given the complication that no spare parts were available from the original manufacturer. To replace them required a Permanent Design Change, but with all the fans out of service, the plant manager was concerned that power reduction would become necessary unless the primary loop water chemistry stayed within certain bounds. If no fans were working, plant procedures would prevent the Hydrogen Water Chemistry Control system from being activated for injection, a job scheduled to occur in about 15 days. A week had been used in the debates, and one manager commented, "Many people have their fingers in it, but there is no owner. It's like a football, between Engineering and Maintenance."

Maintaining power generation had priority over costs, and funds were authorized for whichever alternative was selected. An intermediate step between repair and replacement of the two fans was decided on: To weld them in place until a permanent solution was arrived at. Because welding replaced bolts, a Temporary Modification had to be initiated and processed within five days, the Maintenance Work Package prepared, along with a Joint Process Control sheet from Engineering for the welding procedure, a Hot Work Permit approved by Fire Protection, and so on. The work was carried out on a bitterly cold Friday night with snow falling and 30 mph winds. The fire watch observing the welding saw smoke and gave the alert. The whole organization and the local Fire Department made a good response. The smoke indicated a smolder, without flames. The Unusual Event was declared at 9 p.m. and it was secured 30 minutes later.

The following Monday the Maintenance Section Manager led a critique meeting, which about 30 people attended, including those involved in processing the work package and those who handled the Unusual Event. In an open, blame-free atmosphere, several conclusions were agreed on:

- The potential for ignition had not been recognized by any reviewer, although the drawings and the welding procedure were available.
- The welding procedure had been changed from stitch to continuous the day before the work.
- A Temporary Modification is reviewed less thoroughly than a Permanent Design Change.
- Review responsibilities do not overlap and people downstream tend to rely on those upstream.

This event points up several questions that illustrate in a single work system the relationship between control, coordination, and communication processes and safe performance on the one hand, and, on the other, the significance of mental maps for problem anticipation:

- Managerial criteria used in deciding what to do did not overtly include the quality of the performance of this single task. A generally lower priority to performance quality is reflected by the sudden change of welding procedure, the apparently prevalent practice of reviewing Temporary Modifications less thoroughly, and the performance of this outdoor task during unfavorable weather. The task seems not to have been viewed in terms of what was best for the plant as a whole.

- A surprisingly large number of people participated in the review of the event, rather than, as might be expected, a lesser number of key people who are accountable. Although this level of participation is important to plant-wide, timely feedback and continuous learning, it seems also to reflect unclear delegation of responsibilities. Neither Maintenance nor Engineering owned or was instructed to own the problem.

- The organizational system permits each reviewer to act independently of every other, rather than explicitly acknowledging functional interdependencies by requiring overlap among reviews and reviewers. As a consequence, the working image of the system as a whole tends to blur.

Mental Models

Embedded in such observations and issues is evidence for the fundamental importance of the mental models with which plant staff understand and recognize problems.

The definitions, categories, and theories in daily use form an infrastructure of allowable causality that structures attention and resources. Some of the most fundamental of these definitions are in dispute -- safety, risk, root cause. Definitions regarded as being technical can be cultural and institutional as well -- for example, the equivalence often made between availability and safe performance.

An international team of experts performing root cause analyses found it difficult to use the zero safety-related category of the International Event Rating Scale: They could not disallow any activity a place in their native theories of causation. Another team found it difficult to accept one plant's separation between "industrial safety" practices and "plant safety" practices.

Nor was the conventional Quality Assurance distinction between "plant" and "balance of plant" clear-cut to some experts: They believe that events in the balance of plant can affect reactor safety systems.

Subtle definitions can have large consequences. Two workers at a European plant made an incorrect cable connection on a Friday night under pressure to start up one reactor after a scram. An investigation found that although the control room had been consulted while planning the work, because this was defined as an "informal" meeting, no notes were taken and the log books were not updated. Moreover, the participants put this in the category of a "minor" repair only because it came after the completion of a "major" replacement of steam generators.

Differences in the occupational cultures of project/design engineers and systems engineers can result in differences in their causal understandings, the one grounded in long-range time horizons and individual components, the other in daily concerns and the relationships of components in action. The scarcity of hands-on, systems engineers may be based on a social logic that accords higher prestige and pay to project engineers, especially those who are "outside the fence." Or a plant may use a cultural logic that assigns functions different rankings in a hierarchy of value, as when Operations has a higher rank than Maintenance, but without considering the consequences for communication and morale. How employees see relationships between the "little picture" of their particular task and the "big picture" of the system in operation is another way these logics influence the quality of work. One European plant has instituted a mandatory "face-to-face" between craftspeople and the control room staff to be sure they know where their task fits in, and to get their suggestions before work begins.

Organizational and managerial criteria used in OSART missions are, by the program's own admission, less well developed than those used in reviewing functional and technical areas. One source of this neglect may be a widespread tendency to define "human error" as only <u>individual</u> or <u>personal</u> error, rather than including collective <u>organizational</u> and <u>managerial</u> policies and practices in causal analysis. The categories used for analyzing human performance in root cause analyses, for example, presently are personnel, procedures, and equipment, unmediated by organizational and managerial policies. But these are also human practices that can be in "error."

<u>CONCLUSIONS AND SECOND-YEAR GOALS</u>

Our understandings of work systems lead us to conclude that a theoretical approach is needed that takes account of the unique characteristics of the production processes of nuclear power plants, the information-processing and communicative skills they require, and their status as high reliability organizations. Our continuing field studies and other data collection in the USA and abroad will concentrate on evaluating and extending this preliminary conceptual framework by examining organizational learning activities and by discovering the contents of mental models governing technical practices and organizational systems

Building a Conceptual Framework

The analysis of nuclear plant management and organization typically focuses on standardization and control as in, for example, the Brookhaven National Laboratories' Nuclear Organization and Management Analysis Concept (Haber et al., 1988). Ideally, top management is the source of policies that will be translated into standards of operation; the engineering groups develop these policies into criteria or guidelines; the middle line of managers interpret these into standards for roles, tasks, and procedures; operations, maintenance, and other functional groups implement these standards, with layers of monitoring to ensure compliance. The image is of a machine, or a machine bureaucracy, centrally controlled from the top.

This image of plants assumes: (1) Standardization of technical work is the key to safety; (2) compliance to standards is a major concern; (3) standards are developed by technical specialists; (4) control is from the top-down, embodied in the rules and standards; (5) what matters is the rational division of labor; the organization can be analyzed into parts that can be separately rationalized and then combined according to the demands of their particular tasks; (6) the structure and procedures remain static unless they are deliberately changed, typically as a result of external information from NRC or INPO that is interpreted through top management and engineering into new standards; and (7) slack can be driven out.

Based on our research into work system practices and our reading about the demands on other high reliability organizations, we believe an adequate framework must recognize the dynamics and complexities of the production process, analogous to an image of a living organism in a dynamic ecological setting: (1) Self-assessment and adaptation are the keys to safety; standardization is a way to make that process easier, but not at the expense of rigidifying the organization or stifling its creativity; (2) creating a technical and social system in which compliance takes place is critical, but compliance must be accompanied by intelligence and vigilance to maintain a continuous adaptation process; (3) standards and practices must be developed collectively, acknowledging interdependencies and distributed knowledge; (4) there are many kinds of control in complex organizations, and the interdependencies among groups may override conventional hierarchies of roles and functions; (5) the division of technical labor is socially organized; the understandings people have of the place of their work in the organization matter a great deal to performance; the wider contexts of work provide meaning and external interdependencies; (6) nuclear power plants are continually adapting their routines, driven by external information and the problems and innovations of other plants, internal information and innovation from within, continual readjustments in a "living" organization, changes in the workforce, cultural attitudes, technology, regulation, plant cycles, etc.; (7) resource investments must be made for an uncertain future, typically by investing more in people than is required by the immediate tasks.

A good example of this image of the nature of management and organization spontaneously arose during one research assistant's return visit to the Potomac plant. The researcher presented the generic diagram of nuclear power plants represented by a mostly-hierarchical form with large technical supporting groups and smaller administrative supporting groups. Managers at the plant recognized the model, but they felt it missed some aspects of the organization they thought were important. Their alternative was a portrayal of the organization as a set of intersecting circles. Some, they said, may be more "central" in the sense that they interact with more groups or in more intensive ways. However, the impression was of interconnections and interdependencies rather than the hierarchy, linearity, and boundedness of the machine bureaucracy image. Each image leads to different expectations, which influence the capacity to recognize problems and invent solutions.

Organizational Contexts for Safety

Our field studies make it clear, first, that data on plant operations must be characterized by the phase of operations because each demands somewhat different organizational and managerial activities. These differences may be crucial to optimal safety performance. Talking about the differences between being on-line and in outage, operators say, "We live in two different worlds." In our work from now on, we will make observations across the cycle, with special attention to their intersections and transitions.

Second, our observations of plant work systems and other data confirm that the operations and activities of plants differ within each phase by the tempo of work. We postulate three tempos: Routine, Escalating, and Emergency (we may find others). In a well performing plant with an excellent safety record, when an extra pump was suddenly needed to drain water, the call went out to bring an extra on-site "pump" but in the rush of events it was heard as a call for "the pumper" supplied by the local fire department; this miscommunication under high tempo activated the emergency response system and unnecessarily involved the local community.

Third, the occupational cultures of executives, managers, supervisors, engineers, operators, and craftworkers can differ enough to affect communication, coordination, and morale, and whether staff members come from a Navy or fossil tradition introduces further complications. Project or design engineers maintain a "hands-off" attitude, aloof to operating needs; skills in hands-on systems engineering can be scarce. Craftpersons' expertise may be discounted and degreed engineering expertise overvalued. Quality control procedures may require craftpersons to supervise one another, yet, as buddies (or as relatives), they may avoid doing so. Our studies will note these dynamics and how they relate to recruiting, training, socializing, and rewarding employees, and to other organizational policies and practices.

Finally, the contexts for safe performance are also influenced by regulators, industry groups, IAEA, and vendors. We will examine their roles in the ecologies of work systems and whether they inhibit or facilitate these high reliability organizations in meeting the demands of adaptability, interdependence, and vigilance.

Organization and Management for Learning From Performance

From our first year of observations, we entertain the hypothesis that the ability to utilize feedback effectively and seek sources of relevant information is a key characteristic of plants that are successful and safe in the long run. Studies of Three Mile Island, Chernobyl, Bhopal, and Challenger accidents have made it apparent that most of the information needed to prevent them was available but had not been absorbed into operating practices (Marcus et al., 1990). In practice, nuclear power plants are continually adapting to internal and external pressures. Numerous mechanisms exist in the regulatory and industry environment to provide feedback and to identify and disseminate technical and procedural issues and advances. Plants and utilities have various formal and ad hoc groups to investigate events, collect suggestions, and identify and prioritize potential improvements.

Yet whether and how management and staff foster adaptive and flexible environments is only one part of the story in nuclear power plants. There is scattered evidence of unintended consequences of regulators' disciplinary threats on organizational learning. Employees at all levels and in all functions may do only the minimum required in order to avoid reprimand; they may see excessive proceduralization as implying distrust, which may foster low morale and inefficiency, as when craftspeople see their skills reduced to rote performance. In some European countries whose regulators are moving away from an "envelope" approach to performance standards and the greater trust of craftspeople that it implies, this issue is particularly salient. At the same time, however, regulators as well as industry groups (INPO, WANO) and the IAEA put a high priority on free information exchange and continual improvement of both practices and employees' levels of skill.

Internal pressures are also important: Although there are many instances of interplant exchanges of staff and ideas, there is also evidence that plant management can be closed to new or different ways of operating. A European plant manager observed that "surprisingly few USA plant managers" had taken up his offer to visit and exchange operating experiences; a UK shift supervisor recounted that his plant management had not until very recently exchanged operating experiences with a "sister plant" about 200 miles away. Moreover, the flow of information into plants is so great that each has some system of screening and prioritizing it. The task of translating operating experiences from other plants to one's own situation can be difficult. When contextual data are lacking, the translation may not even be undertaken.

We are also interested in studying managerial practices to reinforce continual learning, such as delegating accountability, exercising vetoes, encouraging problem-ownership, allocating slack to avoid crises, and building consensus. Feedback between organizational levels is important. Job rotation is another method for assuring continual learning. For example, in one plant where compliance and work quality had been troublesome, management introduced more stringent proceduralization not only to fulfill regulatory requirements, but to assure greater accountability as well. Middle-level managers were designated procedure "owners" with decision-making authority over writing and updating. But the crafts were left out of the loop, despite the likelihood that their hands-on experience would feed forward into procedure improvement.

Continuous learning is especially evident in the ways that plants adapt external management consultants' recommendations to their own experiences and expertise. We have noted several instances where conventional management models are implemented, only later to be found unsuitable for nuclear power plant operations. One European manager questioned whether an employee improvement suggestion program, with nonsalary rewards and incentives, is appropriate "when safety concerns should be part of everyone's job." At one plant in the USA, for example, a surveillance procedure involved going in and out of the same fire-proof rooms several times, climbing up and down stairs. Outside consultants had written the procedures based on system schematics without having seen the actual room layouts.

Current management paradigms advocating decentralization, marketization, and computerization have also been widely adopted, not always with the expected results. Despite having computer access to trend data, for example, managers can fail to use them diagnostically. At one European plant, a rising rate of industrial accidents was not further evaluated for its possibly wider implications for reactor safety system operations.

Mental Models and Root Causes of Performance

Experts recognize that each incident or event in a plant is the product of a variety of causes, rather than a single cause. Thus, TMI involved a stuck valve and operator misunderstanding, but also inadequate instrumentation, incorrect procedures and training, and failure to transmit information within the industry about this type of event. Not only are there combinations of causes (e.g., operator error, mechanical failure), but each "cause" is embedded in a causal chain in which it is produced by some "deeper" cause (e.g., operator error by improper training, in turn caused by failure to transmit information; mechanical failure due to poor maintenance, which can be blamed on poor supervision, etc.).

The ability of plants to anticipate and recognize problems, utilize performance information, and predict future states of the plant depend on how well current "mental models" or "plant models" (including PRAs) can assimilate new data. How problems are acknowledged and explained depends in part on shared understandings of plant functioning already in place, which represent beliefs about cause-effect relations. Some beliefs are substantiated by documentation, while others remain conjecture, such as sources of component failures or the risk interactions of components and operators. Mental models to confront such uncertainties develop over time and make use of plant and industry experience.

The mental models even of the most expert of plant staff, regulators, or consultants are not necessarily correct or complete. Studies of the general human processes involved in causal attribution suggest that two mechanisms are often at work: "Functional blindness" and "self-protection" (cf. Nisbett & Rose, 1980; Fiske & Taylor, 1984). In nuclear plants, functional blindness might take the form of seeing the plant from a narrow perspective, thereby identifying as causal factors only those things that are salient within one's expertise. Self-protection can take the form of blaming others or of denying a problem. For example, when faced with a problem, one plant manager exclaimed, "We have a SALP 1 rating -- how could anything be wrong?"

FURTHER STUDIES AND OTHER ACTIVITIES

We operationalize those two main concerns into sets of specific work plans for data collection. Insofar as they lend themselves to reanalysis, we will also examine archival records for their possible contribution to evaluating and extending our conceptual framework (e.g., SALP reports, IAEA's Incident Reporting System, OSART and ASSET public reports).

We will be carrying out work abroad and at previous and new USA nuclear power plant sites. Arrangements are currently being made to send Dr. Carroll and a research associate to France. After approximately one week at Paris Headquarters, one research associate will spend approximately five weeks on site at a power station. Similarly, arrangements are underway to send a research associate to Japan, with the plan of spending several days at the Tokyo headquarters of two utilities, followed by three weeks of fieldwork at one site and one week at a second site.

We hope to observe directly some organizational learning activities, including changes and failed change efforts in return visits to the organizations we are already familiar with. We will solicit the participation of new sites that have a special interest in the second-year studies.

Studies of Organizational Learning Activities

In order to compare across plants and countries, at each site we will be characterizing these major issues and activities in terms of the detailed tasks they entail:

A. Procedure rewriting, component and systems walkdowns, and dissemination;

B. Feedback reviews, based on internal and external performance information, including links with contractors and vendors;

C. Job rotation, cross-training, and succession plans and practices;

D. Resource flows among site and off-site engineers;

E. Adaptation of external consultants' recommendations for organizational and managerial structures and practices.

We will investigate these activities through a combination of onsite data collection and analyses of industry reports. At each plant, we will interview key actors, collect relevant records, and observe how these activities are carried out and evaluated by participants.

Studies of Mental Models

To document the contents of mental models by occupation and organizational role, we will draw on several data sources and methods:

A. Content analyses of plant archival materials (e.g., plant safety committee incident analyses; HPES reports) and, external to plants, SALP, OSART, and ASSET reports, and INPO's "Lifted Leads." The goal is to establish a set of causal categories and their relative frequencies (perhaps subdivided by certain factors such as type of event, type of plant, country), describe the linkages among categories (i.e., what root causes typically underlie which surface causes), and also create hypothetical scenarios to use in further judgmental studies.

B. Interviews with appropriate plant staff and experts to examine how their assessments of causal categories are linked to their everyday work and the design of work systems. These interviews would explore a range of routine activities and decisions, such as prioritizing maintenance work backlogs and interpreting various kinds of organizational data.

C. Discussions of realistic scenarios, including suggested concrete corrective steps. In a more structured, experimental environment, these basic scenarios would be varied by manipulating particular factors (presence of a design flaw, incorrect procedure, classic human error, etc.). The analysis would examine whether differences in causal judgments tend to cluster and whether they are associated with various characteristics of the individuals such as professional background, years of experience, and national culture.

D. At an organizational level, this "beliefs" assessment would allow us to ask whether organizations with overall judgment patterns of a particular sort also exhibit safety-relevant behaviors, where variations of judgment patterns exist (e.g., managers attribute cause differently from workers, systems engineers from maintenance people), and to find out what is associated with the degree and nature of such intraorganizational differences.

E. Participation in technical workshops with IAEA staff responsible for the International Incident Reporting System, which is reconsidering its categories.

<u>Comparisons with Other Industries</u>

To keep refining the distinction between the safety concerns of nuclear power plants and those of other types of complex industrial organizations, we will undertake several comparative activities. We will be observing fossil power plant operations. Under Kent Hansen's direction and at the request of the U.S. Department of Energy, we are developing a study of organizational and managerial issues in nuclear waste management at DOE sites. We are keeping abreast of work in other kinds of high reliability organizations and with MIT colleagues' on-going research in industries where safety and health are important considerations (e.g., chemical industries).

Planning for a Scientific Conference on Organizational and Managerial Issues for Safe Performance

Members of this research project have participated in several conferences organized by organizations with "missions." This includes the annual meeting of NRC contractors and the workshop on organization and management at IAEA/IIASA. Each such conference has been disappointing because the opportunities to exchange information and thoughts about organization and management were very limited. These limitations were due to restrictions on the numbers of participants, the range of topics, pressure to produce a particular product, or time constraints.

We have become aware of more relevant and interesting work that makes valuable connections to our own. Some of this work is in the nuclear industry, but some is in chemicals, airlines, and military, for example. Even NRC contractors have expressed a wish to "open up" their ideas in a forum that would be more receptive to issues without requiring immediate regulatory relevance.

Accordingly, we believe that a conference would be an important intellectual event and that our auspices could maximize its value. The ideal time would be in the late summer or fall of 1992. We envision two or three days of activities, with approximately 25 participants.

The conference should be predominantly self-funding (participants pay their own travel and a nominal registration fee). Our project can provide travel reimbursement for the truly indigent and host events such as a cocktail party and dinner.

REFERENCES

1. Banaghan, E. A. (1991). *Developing Performance Indicators for Complex Organizations: A Case Study in Nuclear Power.* Cambridge, MA: M.I.T. Sloan School of Management, M.S.M. Thesis.

2. Beckjord, E. et al. (1987). *International Comparison of LWR Performance.* (MIT EL 87-004). Cambridge Ma: M.I.T Center for Energy Policy Research.

3. Egan, S. (1982). "To Err is Human Factors." *Technology Review*, pp. 23-29.

4. Fiske, S. T. & Taylor, S. E. (1984). *Social Cognition.* Reading, MA: Addison Wesley.

5. Haber, S. et al. (1988). "An Organizational Model of a Nuclear Power Plant." Brookhaven National Laboratories.

6. Institute of Nuclear Power Operators. (1987). *Performance Objectives and Criteria for Operating and Near-term Operating License Plants.* (INPO 85-001). Atlanta, GA: Institute of Nuclear Power Operations.

7. Institute of Nuclear Power Operators. (1988). *Performance Indicators for the U.S. Nuclear Utility Industry*. Atlanta, GA: Institute of Nuclear Power Operations, March.

8. Jaliff, J. O. (1991). *Organization and Management Characteristics of a Nuclear Power Plant*. Cambridge, MA: M.I.T. Sloan School of Management, M.S. Thesis, June.

9. LaPorte, T. R. (1989). "High Reliability Organization Project." University of California, Berkeley, January.

10. LaPorte, T. R. and Consolini, P. M. (1989). *Working in Practice But Not in Theory: Theoretical Challenges of 'High Reliability Organizations'*. Unpub. ms. Department of Political Science, University of California, Berkeley.

11. Lester, R. K. (1986). "Organization, Structure, and Performance in the U.S. Nuclear Power Industry." *Energy Systems and Policy*, v. 9, no.4, pp. 35-384.

12. Marcus, A. A., Nichols, M. L., Bromiley, P., Olson, J., Osborn, R. N., Scott, W., Pelto, P., and Thurber, J. (1990). "Organization and Safety in Nuclear Power Plants." Division of Systems Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, NUREG/CR-5437. Washington, DC: U.S. Nuclear Regulatory Commission

13. Moray, N. P. and Huey, B. M. (eds.). (1988). *Human Factors Research and Nuclear Safety*. Washington, DC: National Academy Press.

14. Nisbett, R. E. and Rose, L. (1980). *Human Inference: Strategies and Shortcomings of Social Judgment*. Englewood Cliffs, NJ: Prentice-Hall.

15. Perin, C. (1990a). "Research Note on Field Study Sites." August.

16. Perin, C. (1990b). "Organizational and Managerial Processes in Nuclear Power Plants." October.

17. Perrow, C. (1984). *Normal Accidents.* New York, NY: Basic Books.

18. Rasmussen, J. (1988). "Safety Control and Risk Management: Topics for Cross-Disciplinary Research and Development." IChemE Publication Series No. 110; Washington, DC: Hemisphere Publishing Corp., pp. 1-15.

19. Samanta, P., Wong, S., Higgins, J., Haber, S., and Luckas, W. (1988). "A Risk Methodology to Evaluate Sensitivity of Plant Risk to Human Errors." In E. W. Hagen, ed., *1988 IEEE Fourth Conference on Human Factors and Power Plants.* New York, NY: Institute of Electrical and Electronics Engineers.

20. Schroeder, D. M. and Robinson, A. G. (1991). "America's Most Successful Export to Japan: Continuous Improvement Programs." *Sloan Management Review*, v. 12, no. 3, Spring, pp. 67-81.

21. Suzuki, T. and Hansen, K. F. (1988). *A Comparison of Nuclear Safety Regulation Systems and Their Impacts on LWR Performance in Japan and the United States.* (MIT EL 88-019WP). Cambridge, MA: MIT Center for Energy Policy Research.

Program Participants as of June 1, 1991

1. International Participants

Country	Organization
Finland	Imatran Voima Oy Teolisuuden Voima Oy
Germany	Kraftwork Union AG
Japan	Mitsui, Inc., Ltd., agent for: Chubu Electric Power Company, Inc. The Japan Atomic Power Company The Kansai Electric Power Company, Inc. Kyushu Electric Power Company, Inc. The Tokyo Electric Power Company, Inc.
South Korea	Korea Electric Power Company
Switzerland	Swiss Nuclear Operators Group
Union of Soviet Socialist Republics	Institute of Nuclear Safety of the Soviet Academy of Sciences
International	World Association of Nuclear Operators–Paris Center International Atomic Energy Agency–Division of Nuclear Safety

2. U.S. Participants

Boston Edison Company
Commonwealth Edison Company
Consumers Power Company
Duke Power Company
General Electric Company
The John D. and Catherine T. MacArthur Foundation
New York Power Authority
The David and Lucile Packard Foundation
Public Service Electric & Gas Company
Stone & Webster Engineering Corporation
Yankee Atomic Power Company

Key Contact Persons in the Program

Prof. Kent F. Hansen, Program Director
Room E40-483A
Tel.: 617-253-7384
Fax.: 617-253-8013

Dr. Tatsujiro Suzuki, Associate Program Director
Room E40-261
Tel.: 617 253-8306
Fax.: 617 253-8013

Prof. Richard Lyon, Science and Technology of Service and Maintenance
Room 3-366
Tel.: 617-253-2214
Fax.: 617-258-5802

Prof. John Carroll, Science of Management
Room E52-590
Tel.: 617-253-2617
Fax.: 617-253-2660

LEARNING IN NUCLEAR POWER PLANTS

JULY, 1991

Jon Olson
Battelle Human Affairs Research Centers
Seattle, WA U.S.A
(206) 528-3230

James Thurber
American University
Washington, D.C. U.S.A.
(202) 885-6247

While this paper draws on observations made during several different projects for the U.S. Nuclear Regulatory Commission, the U.S. Department of Energy, and several private firms, the views expressed here do not necessarily reflect the views of these organizations.

1.0 INTRODUCTION

Over the past decade, the research question concerning the role of organizational factors in nuclear power plant (NPP) safety has changed substantially. The question is no longer, "Do organizational factors influence plant safety?" Numerous incident investigations and empirical analyses within the nuclear and other safety-sensitive industries have answered this question in the affirmative (NUREG/CR-3737; Perrow, 1984; Starbuck and Milliken, 1988). Nor is the question exclusively, "How do organizational factors affect plant safety?" While much has yet to be learned about the nature and size of organizational influences under varying conditions, several theoretical discussions and empirical analyses have been published recently that constitute good progress in answering this question (NUREG/CR-3215; NUREG/CR-5437; Haber, et al., 1988; Osborn and Jackson, 1988). Instead, the research question must be increasingly phrased as follows: "Given that organizational factors are crucial to plant safety performance, what should be done to assure that organizational factors contribute to, rather than detract from safe performance?"

The initial reaction to this question is frequently to attempt to develop a model standard for organizational factors for the industry. Such a standard would include detailed guidance on reporting relationships, the configuration of tasks within departments and departments within the plant, limits on spans of control or the number of vertical ranks, required coordination and communication mechanisms, and the like. However, such an approach is of limited use either for utility management or for regulatory purposes. Existing organizational theory and research very strongly suggest that effective organizations can and must take substantially different forms depending on the demands of the specific organizational context and the history of the specific organization. To apply common, detailed design and management requirements to all nuclear power plants would not be sensitive to the real need of the individual utility to respond to the contingencies of size, local culture, labor relations, ownership structure, and the countless other factors that management must take into account when devising a workable organizational strategy. Thus, while an idealized model can inform and guide the regulatory process, it does so more by providing an inventory of organizational factors and relationships among those factors for consideration on a case-by-case basis.

In addition to attempts to develop a formal model of organizational influences on safety, work is also being conducted in an attempt to identify organizational factors that inhibit or promote improvement in performance. In many ways, this research area may be even more fruitful, both for operators and for regulators. From the regulatory side, interest in management and organization is highest when performance has slipped to the point that it is no longer acceptable. It then becomes management's role to institute organizational systems to assure performance improvement. Regulators need a sophisticated understanding of what types of programs are likely to work within particular organizational contexts if they are to have the confidence that performance will actually improve. From utility management's side in this situation, existing practices have proven inadequate, and new knowledge is needed in order to understand the best strategy and implementation plan for achieving improvement.

The issue of organizational improvement, however, is not limited to the case of the problem plant. Industry and regulatory performance standards seem to be steadily increasing. What was acceptable performance ten years ago is now no longer considered to be adequate. Further, many utilities are pursuing excellence or total quality as a goal, and the demands placed on the organization for continuous improvement are much greater than in the past.

Understanding the organizational constraints and strategies for achieving continuous improvement in the nuclear power industry remains an unmet need.

However, the very process of improvement is, in itself, not well understood. Few objective criteria exist for evaluating alternative plans and strategies. Further, organizational theory and utility experience indicate that the process of improvement or learning can not be reduced to the development and application of formal improvement programs. While these programs are essential in a degraded plant, detailed attention must also be applied to more general organizational factors including management attention and values, availability of technical and other resources, and the nature of inter-departmental relations, if the formal programs are to meet with success.

The purpose of this paper is to consider the following questions:

- What is the relationship between organizational learning and safety performance in the context of the nuclear power plant?
- What does the process of learning look like? What are its essential elements?
- What organizational factors appear to promote or inhibit organizational learning?

2.0 APPROACH

Several sources of information are used to support the discussions in the following sections. One source is a systematic review of eight Diagnostic Evaluations (DEs) conducted by the Office For the Analysis and Evaluation of Operational Data (AEOD), of the U.S. Nuclear Regulatory Commission (NRC). The DEs are intensive investigations of the root causes of actual or potential performance problems at selected NPPs. In most cases, a plant is selected for a DE when it displays subaverage performance over several years. The exact nature of the DE depends on the performance problems triggering the NRC's concern. Thus, different investigation protocols have been used for the different DE's leading to some differences in the types of organizational factors evaluated and the level and type of information available to address the issues surrounding organizational learning. Nonetheless, the DEs provide a rich and generally consistent source of information about management and organization factors in general, and the problems associated with organizational learning in particular.

The review consisted of abstracting from the DEs any information associated with plant improvement programs, operating experience review programs, equipment performance and trending programs, root cause analysis, plant safety analysis review programs, and quality assurance programs directed at plant performance, including corrective action programs. Also abstracted from the DEs was information on any organizational factors that were specifically cited as contributing to the level of performance of the various learning-oriented programs.

The second basic source of information comes from a series of case studies of organizational learning. These case studies were devised to get directly at the process of learning and the management strategies and organizational factors that either promoted or inhibited learning at the various sites. As opposed to the DEs, these case studies tended to focus on average or better than average performers. Thus, these case studies are more useful for presenting information on the positive, or success aspects of learning.

The case studies include three commercial nuclear power plants and one DOE research reactor. In all cases, the organizations had a recent history of sound performance. All of the organizations were small by industry standards, with the three commercial units highly similar in basic design and operating philosophy. Thus, the successes and strategies derived from these case studies may not be generalizable to the broader range of plants (e.g., larger, newer, more complex operating environments). Nonetheless, valuable, if initial information is available from these case studies.

The method used at each site involved interviews of approximately 10 individuals including plant management, the heads of major plant functions (e.g., operations, maintenance, engineering, QA), and individuals charged with responsibility for the major plant improvement programs (e.g., HPES, operating experience review, equipment history programs). In addition to basic questions about the organization and performance of the plant, the individuals were asked questions concerning the nature of the plant improvement programs, if they had contributed to improved performance, how this contribution was made, where the programs had failed and why, and how the programs could be improved. From these questions, considerable information on the organizational context of learning was derived including information on the role of inter-department cooperation in learning, the significance of corporate support and resources, the need for prioritization, and strategies for follow through.

Finally, the information from the DE's and the case studies has been augmented with lessons learned from other organizational studies conducted by the authors and others. Several of these studies concern organizations within the nuclear industry, and more specifically, facilities within the Department of Energy.

3.0 THE RELATIONSHIP OF LEARNING TO PLANT SAFETY

The theoretical discussions in NUREG/CR-3215, NUREG/CR-5241, and NUREG/CR-5437 all point to the significance of learning in assuring plant safety performance. In the case of NUREG/CR-3215, the case is made in terms of the need for innovation. The nuclear technology is an incomplete technology in the sense that much is still being discovered relative to such factors as:

- The risk significant interactions of components and systems;
- Factors contributing to the wear and aging of components;
- The performance of components and systems under extreme conditions;
- The interaction of the operator and the maintainer with plant hardware.

While it has been argued that within a complex, tightly coupled system, there will never be adequate understanding of the relationships among components and systems (Perrow, 1982), NUREG/CR-3215 argues that the more innovative the plant -- the more it can learn from research, from industry experience, and from its own operating experience -- the fewer safety significant problems it will experience over time. This perspective is adequately illustrated by the TMI-2 accident -- an accident that may have been avoided had the utility been better able to learn from industry operating experience.

The argument made in NUREG/CR-5241 is somewhat different. Here, there is an additional concern with the role of learning in managing backlog. Plant systems are constantly degrading through use. As plants age, the burden of maintaining the plant as-built becomes increasingly demanding as more and more components reach the end of design life. Only through effective preventive and corrective maintenance can the plant stay ahead of the effects of aging. However, the ability to stay ahead is strongly influenced by the ability to learn from operating experience. In cases where inadequate design or incorrect maintenance or operation lead to premature failure of the component, the burden of maintenance is unnecessarily increased. Organizations that can learn from operating experience and solve root causes of premature failure, have relatively more resources to apply to preventive and necessary corrective maintenance activities. Organizations that cannot learn from operating experience see their maintenance and corrective action backlogs grow to the point where they are sometimes overwhelmed by the volume of work to be conducted, and enter a significant downward performance spiral.

This scenario is illustrated by several of the DEs. In four cases, poor root cause analysis and management support for corrective actions were viewed by the reviewers as significant contributors to the continued material degradation of the plant and the inability of the plant to avoid what were fundamentally avoidable performance problems. In three cases, plant operators had reached the point of no longer requesting maintenance on certain key items because they felt that either the maintenance would not be preformed, or that it would be performed in a manner such that the underlying problem would not be fixed.

Finally, in NUREG/CR-5437, another aspect of the relationship of organizational learning to plant safety is introduced. Here, problem solving on the part of plant personnel is introduced as a potentially significant type of activity for managing human relations and behavior in the plant. By emphasizing problem solving and improvement, management is able to communicate a series of values that have potential positive effects on plant safety. For example, the workers involvement in problem solving may have some aspects of job enrichment inherent in it. Being part of the process of discovery is inherently rewarding, and can offset some of the tedium associated with other aspects of some jobs in nuclear power plants. The problem-solving orientation may also increase the worker's attention to the job, as the worker tries to understand the implications of his own and the system's performance. The worker may also derive satisfaction and commitment from the experience of being listened to as an expert by management and co-workers. Thus, the emotional benefits accruing from a problem solving orientation in the plant, may have more generalizable positive effects on worker performance and plant safety. Among the high performing plants that comprised the case studies, numerous examples of these positive effects were noted.

The DEs also provide support for this perspective, although in the negative. In several of the plants, workers cited management as being unresponsive, or even punitive when problems were brought to their attention. The reviewers noted that this type of management reaction significantly lowered morale and communicated to the workers that safety was not valued, and that worker care in their jobs and for the plant was not warranted. In several of the case studies, workers cited problem solving activities and management support for worker participation in problem solving as key aspects of plant success and key contributors to staff morale.

To summarize, then, there are several ways that learning contributes to plant safety performance:

- By avoiding unnecessary, repeat failures, either through a review of the plant's own operating experience or through a review of outside experience and research

- By fostering innovation and discovery to offset existing design deficiencies

- By promoting work attitudes and behaviors that are consistent with safe performance in general.

4.0 THE PROCESS OF LEARNING

Understanding the role of learning in nuclear power plant safety first requires a discussion of what is meant by learning. Several different, though related approaches can be taken to the concept.

Learning can be defined objectively at the organizational level in terms of organizational outcomes. An organization can be said to have learned if it manifests a change in a particular outcome. From the safety perspective, an organization has learned if it avoids repetitive errors and failures, either in terms of a general class of phenomena (e.g., a decline in the number of scrams) or a more specific class of phenomena (e.g., a decline in the number of scrams induced by poorly written operating procedures). This approach to assessing learning underlies the statistical analyses conducted under other tasks in this project.

However, learning can also be manifest in other outcomes that may be more difficult to measure. For example, an organization that searches its environment and learns from the operating experience of others, theoretical discussions by experts, and other sources may end up avoiding problems in the future that have not yet manifested themselves as events. Thus, the error or failure rate may not change, but learning has happened. While this aspect of learning is conceptually straightforward, it causes some significant measurement problems -- how to assess the number of failures avoided. Understanding this type of learning may depend on the observation of learning-relevant behavior.

This leads to the third perspective on learning -- learning as a process. This perspective focuses on the various organizational processes that, if effective, lead to changes in outcomes. Figure 1 provides a description of these activities, and serves as point of discussion.

4.1 Problem Recognition

The first stage in the learning process is problem recognition. In order to start the learning process, it is necessary to identify a deviation from a desired state. If everything appears to be working normally, or within expected parameters, learning is unnecessary, and learning behavior is largely inefficient. If there is a deviation from expectations, however, both the stimulus and the need for learning may be present.

Problem recognition, however, is itself a complex phenomena. Nuclear power plants vary substantially in their performance on this aspect of the learning process. Nor is this variation due to the number of problems experienced. Some problem-laden plants are unable or unwilling to recognize the number of problems they have. On the other hand, some of the high performance plants observed in this study were highly active in the problem solving area.

Of primary concern is the value placed on problem recognition, and nuclear power plant organizations vary substantially in the degree to which they promote problem recognition. A

LEARNING PROCESS

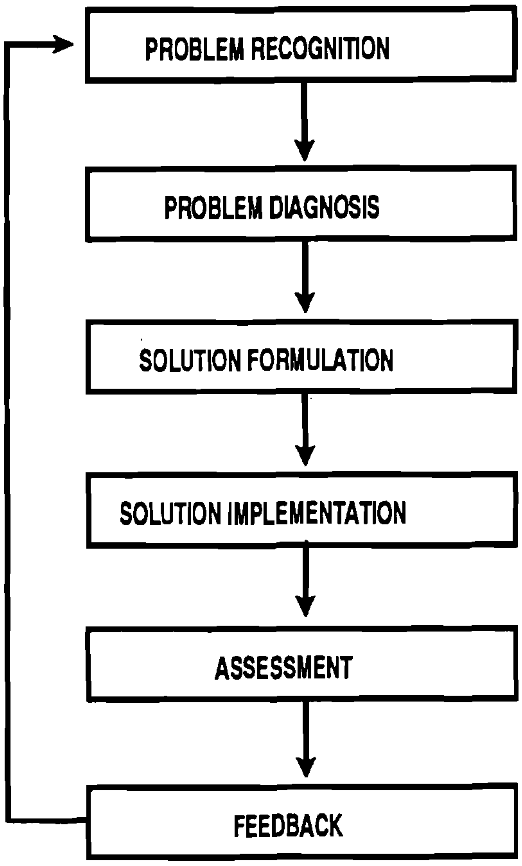


FIGURE 1

significant contrast is between those organizations that view problem recognition as a first step to improvement and those that view problem recognition as an impediment to the normal conduct of business. Among the case studies and the DEs, considerable variation was observed in the basic orientation to problem recognition. In the case of one DE plant, inoperable equipment was so common that it had ceased to be viewed as a problem important enough to warrant action. In two other cases, workers reportedly feared that the identification of problems would lead to punishment by management. In one of the case study plants, several respondents stated that their long history of good performance had led to overconfidence, resulting in a series of avoidable forced outages. The respondents indicated that they had temporarily lost their ability to identify developing problems.

Another key aspect of this difference is the "problem-space" that is searched to identify problems. For example, some plant organizations search only that problem space represented by their own operating experience. These organizations are essentially blind to the lessons to be learned from the operating experiences of other nuclear power plants and related industries. This pattern of behavior was evident in one DE, where the plant had not even adopted the lessons learned from the Diagnostic conducted two years earlier in another plant in the same utility. Apparently, the organization was not motivated to learn from external experience. In another case, the operating experience review was so ineffective and poorly staffed that the relevant parts of the organization were not gaining access to information about external operating experience. Thus, while the organization may have been properly motivated, it was not effective in bringing external operating experience into the problem space.

Other plants, however, have complex systems for expanding the problem-space searched to other plants, both in the U.S. and elsewhere, and expend considerable resources in this activity. In general, this characterized all of the case study plants and at least one of the DE plants. In these cases, plant personnel were highly involved in owner's group committees, INPO supported data bases, EPRI projects, and so forth. This involvement reflected a recognition that there was plant-specific value in reviewing the experiences of other utilities. Interviews from the case studies supported the notion that this investment, if properly managed, improved the safety performance and operating efficiency of the plant.

A second way that the initial problem-space can vary is in terms of the types of failures that trigger problem recognition. In some plants, problems may go unrecognized until some external agent, such as INPO or the NRC brings them to the plant's attention. Some plants may only recognize that a problem exists when major equipment failure causes an unscheduled shutdown. At the other extreme, in some plants problem-recognition is triggered when an operator realizes that he almost made a mistake (e.g., left out a step in a procedure), and the problem solving apparatus is activated to try to understand why the mistake nearly happened.

In terms of the formal definition of the problem, plants vary in terms of the degree that they search human performance as well as equipment performance problem-space, and the extent to which they search failure or failure precursor problem space. Several of the poorly performing DE plants, for example, had not established any variant of INPO's Human Performance Evaluation System (HPES). All of the case study plants had strong HPES programs in place. Similarly, most of the poorly performing DE plants were cited for having insufficient root cause analysis programs. Specifically, they were found to have exerted little or no effort in tracing back from the proximate cause of equipment failure to the root causes of the failure. This placed them in a situation of making repeated errors and never recognizing or fixing the underlying problem.

The social and technical organization of the plant can also influence the approach to problem recognition. For example, certain systems (e.g., balance of plant systems) can be placed outside of the normal problem-search space. The existence of the non-safety related category of components can lead to certain types of problems, including safety-related root causes from remaining undetected. At times, regulatory pressures and initiatives have had the effect of excessively limiting the problem space searched by a particular utility, either by creating categories of problems that are outside of regulatory concern, or by emphasizing a particular type of problem to the point that the utility is distracted from other aspects of the legitimate problem space.

Similarly, in a plant dominated by operations culture, maintenance-related problems may be placed outside of the problem space. A preliminary conclusion from the case studies is that plants that maintain a balance of influence among plant functions (e.g., operations, maintenance, and engineering), and that have positive working relationships among these functions along with effective means of communication seem to be in a good position to more systematically and comprehensively recognize and characterize the nature and cause of problems. Organizational rank may also be a factor, with management activities placed outside the problem space and direct worker activities placed within.

Thus, in many ways, the social and technical organization of the plant, its culture, and the regulatory and business environment it faces can shape the way that problems are defined at the plant level. To assure that problems are fully identified, at least within acceptable cost/benefit limits, these barriers to problem identification must be overcome.

4.2 Problem Diagnosis

The second stage in the learning process is problem diagnosis. While it has some obvious overlap with problem identification, organizations vary substantially in the amount of effort put in to understanding the nature of the problems noted. This activity goes beyond the discovery of the existence of the problem to the clarification of what the problem is. This clarification has both a technical basis and an organizational basis. The technical basis involves establishing fact: what caused the failure, what was the precise nature of the failure, what were the effects of the failure on related systems and components?. To answer these questions, technical input from a variety of sources (e.g., chemical analyses, design engineers, human factors experts) may be required. The process of providing these inputs, however, is an organizational one affected by the level of resources available to support problem diagnosis, the skills of the technical staff, and the ability of the organization to assimilate relevant technical information from outside the organization.

The organizational basis of problem diagnosis, however, also involves establishing the organizational meaning of the problem: what individuals or groups are "to blame", who should have input into defining the nature of the problem, what type of evidence qualifies as fact, and so forth? Such factors as the nature of labor-management relations, relations among plant groups, and the relative power of different groups help condition how organizational interpretation of the problem is established for the problem.

Problem diagnosis can be divided into three types of activities:

Classification: the problem fits into a particular category of problems. It is like or unlike problems previously encountered.

Causal analysis: the problem resulted from prior conditions and actions.

Consequence analysis: the problem is important or not important for specifically identified reasons.

In the cases reviewed, the activities of classification, causal analysis, and consequence analysis were handled in different ways, were subject to different impediments, and contributed differently to long-term safety performance.

One key area of difference was the availability and quality of technical resources. One of the primary deficiencies noted in the Diagnostic Evaluations was the level of technical support for problem diagnosis. Many of the plants experienced poor equipment performance, including significant numbers of repeat failures. All eight of the plants reviewed were evaluated as having poor root cause diagnosis systems. A number of factor contributed to the inadequacy in root cause analysis system:

- Inadequately trained or inexperienced engineering support
- Lack of onsite engineering support coupled with poor support from corporate engineering
- Inadequate staffing of engineering support relative to the backlog
- Lack of training in root cause analysis, including human error analysis
- Lack of root cause analysis skills and technical knowledge among maintenance, operations, or quality assurance staff
- Lack of equipment history data to support trend and pattern analysis
- Poor communications among departments, leading to a restriction of information flow concerning failure and cause information
- Lack of trust between departments or between management and labor leading to blame placing or the hiding of root cause information
- Lack of interest on the part of workers to get to the bottom of recurring problems due to past lack of management follow through in the past

The case study plants, on the other hand, present a nearly opposite picture. In all of the plants visited, repeat failures were uncommon, and the root cause analysis efforts appeared to be well developed, supported, and successful. Some of the factors that appeared to contribute to this success were:

- Strong, onsite engineering

- Low turnover among plant personnel, leading to a high level of resident plant knowledge

- Very good communications among departments, leading to the open sharing of failure and cause information

- Formal programs for broadening workers' experience and plant knowledge including SRO training for plant engineers, involvement of maintenance in the design support for plant modifications, involving operators in root cause analysis and other task force activities, involvement of plant staff in industry activities such as owners groups, and job rotation for management personnel.

- Good labor management-relations leading to labor buy-in with improvement programs and a non-punishment orientation toward personnel errors. The non-punishment orientation was viewed by managers of the high performing plants to be a necessary condition for the type of open flow of information that allows for the discovery of true root causes.

- High credibility and trust of the individuals responsible for the various root cause programs, based on plant knowledge and experience, good people skills, and technical ability.

- Well developed equipment history data programs, and a high level of participation on the part of workers in recording information on equipment failures.

- A manageable backlog of problems so that technical support for the root cause analysis program was not overburdened.

- Well developed systems for identifying the importance of a failure so that appropriate resources could be directed toward it.

- Good work attitudes, including a sense of ownership in the plant and the equipment.

The ability of the plant to successfully diagnose the nature, causes, and consequences of problems, therefore, is strongly tied to organizational factors. Where management does not allocate sufficient technical resources in a way so that they are brought to bear on the problem, where communications among departments and between labor and management are inhibited by organizational structure or a lack of trust or respect, and when plant personnel are taught by the system to take a very narrow view of their roles and responsibilities, root causes do not get discovered, and the problem diagnosis stage of learning is inadequate.

4.3 Solution Formulation and Implementation

As in the cases of problem identification and diagnosis, the development and implementation of solutions to operational problems have both a technical and an organizational basis. The case study plants and the DE plants provide several important points of contrast in terms of how, and how effectively solutions are formulated and implemented.

4.3.1 Technical Solutions

One of the major weaknesses reported among the DE plants was their inability to develop and implement solutions to ongoing equipment and programmatic failures. One of the major causes of this failing was the lack of availability of appropriate technical expertise for the development of technically sound solutions. In contrast, one of the obvious strong points of the case study plants was the uniform availability of this technical expertise. This contrast can be made in three more specific areas: engineering expertise, the technical expertise present in QA, operations and maintenance, and the ability and willingness of the organization to access the technical expertise and experience of the wider industry.

The availability of engineering support, itself, has several dimensions. One key dimension is the quality of that expertise. Such expertise was clearly lacking in two of the DE plants. All of the case study plants and several of the DE plants, however, were noted for having highly qualified engineering expertise within the company. In the case study plants, this meant not only that degreed engineers were available, but that they had extensive plant knowledge and experience. In three of these plants, engineering support was located on site, and the average plant experience level of the engineering staff was quite high. In the fourth case study plant, certain aspects of engineering support were located offsite, a fact that was judged to constitute a programmatic weakness by several of the department managers interviewed at that site.

One of the most consistent findings from the DE plants, in fact, is that the location of engineering support offsite significantly and negatively affects the quality of engineering support provided to the plant. Because offsite engineers frequently lack plant knowledge, and because the drawings, specifications, and procedures with which they must work are frequently poor or out of date, the solutions that are developed offsite frequently are judged by onsite personnel as being unworkable or inadequate. When plant personnel are confronted by these inadequate solutions, they are less likely to foster the open communication with engineering necessary to promote improvement of the solutions, leading to even less access to engineering support in the future. Thus, the quality of technical support for solution formulation is very much dependent on the physical and organizational location of plant engineering, and the quality of relations and communications between engineering and the other plant functions.

Engineering is not the only potential source for technical solutions to problems. In fact, all of the high performing case study plants were characterized by the involvement of personnel from all or most departments in the development and implementation of technical solutions. Management in these plants provided two key resources that made the wider involvement in solution formulation possible and effective.

The first resource is access to the process of solution formulation. At the high performing plants, operators, maintainers, and others were not only expected to assist in the development of solutions, but organizational resources and mechanisms were provided to assure that they did. This included the creation of special task forces, with operators and maintainers working with engineers to diagnose the problems and come up with consensus solutions. It also included making staff time available for operators and maintainers to participate in these activities.

The advantages of opening up the process to staff other than engineers are several. Respondents at two of the case study plants indicated that this strategy leads to better technical solutions, since the people with hands-on experience frequently have information and insights not available to the engineering staff. These people are also frequently most aware of the operating history of the problem equipment, including its typical failure modes. Another advantage is that by involving plant staff in the development of the technical solution, they are more likely to assist in the implementation of the solution. When staff are not involved in the development of the solution, as suggested by several of the DEs, they are more likely ignore or actively oppose the implementation of the solution.

The second major resource that management makes available to plant staff to assist in their participation in solution formulation is technical training. In one of the case study plants, several mechanisms were used to expand the technical knowledge available to both engineering and non-engineering staff. One of these mechanisms was to provide financial support and encouragement for operators to earn engineering and science degrees. A second mechanism was the provision of SRO training for engineering staff. A third mechanism was to provide opportunity for job rotation among managers and supervisors to give them wider exposure to the plant and the organization. A forth mechanism was to recruit and assign individuals with engineering and plant experience to the Quality Assurance organization. Taken together, in the context of a team approach to solution formulation, higher levels of technical expertise could be directed to the solution of problems.

In contrast, several of the DE plants were criticized for not involving non-engineering staff in the solution of problems. For example, seven of the eight plants were evaluated as having poor teamwork among the plant functions. One was specifically mentioned as having a significant lack of technical ability within the maintenance organization, and an inability of the maintenance organization to compensate for this weakness by working closely with engineering.

The third area where the DE plants and the high performing case study plants varied was in the ability of the organizations to search the experience of the wider industry to find solutions that could be adapted for the specific problems facing the plant. All of the case study plants had displayed a management philosophy that promoted learning from the environment. This included positive working relationships with INPO, EPRI, vendors, and vendor groups. Staff at these plants were well aware of vendor developed solutions for hardware problems, and the current status of key research and development issues (e.g., advances in predictive maintenance). Management supported participation by plant personnel in conferences and workshops, participated with EPRI in developmental projects, and even appeared to relatively open to input from INPO and the NRC concerning operational deficiencies. On the other hand, plant personnel appeared to be intelligent consumers of industry experience. Rather than accepting particular approaches uncritically, plant management and staff evaluated the applicability of the industry experience to their situation, and evaluated the benefits of the solution relative to the costs.

In contrast, the DE plants typically were not prepared to identify and adapt solutions from the wider industry. For example, one plant was cited for a weak level of attention to vendor notices. Another was cited for failing to adopt improved procedures for the maintenance of motor operated valves. A third was cited for failing to make the improvements resulting from an earlier diagnostic at its sister plant. At the other extreme, one plant was also cited for being too quick to react to external pressure from the NRC or INPO by adopting the solution that they perceived to be the favorite one of the outside party, without thinking through implications and necessary adaptations for the plant's unique situation.

4.3.2 Organizational Constraints

The development and implementation of sound technical solutions must take place within an organizational context that can either facilitate or inhibit the effectiveness of the solutions. Some aspects of this context have already been discussed in the previous section. One of the most important elements of this context, however, concerns budgetary resources. The size of the budget relative to need will determine the ability of technical solutions to be developed and implemented. Among the case studies and the DE plants alike, budgetary issues play a significant role in the effectiveness of solution formulation and implementation.

No plant in the nuclear industry is immune from resource limitations. This is particularly true as deregulation has increased competition among utilities, as Public Utility Commissions have become more aggressive in limiting rate increases, and as increases in operating costs have eroded the cost advantage once held by nuclear over other fuels. Even among the high performing case study plants, the potential exists for having inadequate resources to develop and implement solutions to important operational problems. However, among these plants, several steps were being taken to assure that, to the extent possible, resources were available for important improvements. These included:

- Systematic methods for establishing priorities among competing needs. These methods included risk-based assessments (based on PRA, RCM, etc) of the significance of the operational problem, cost-benefit analyses of alternative solutions, and detailed, forward looking performance goals to organize and direct budgets. These mechanisms helped assure that scarce resources were not being wasted on low priority items.

- Bottom-up budgeting, with resource expenditures planned on the basis of inputs from those individuals and groups with first-hand experience with plant needs. In one case, management was experimenting with a variation on zero-based budgeting.

- Group decision making concerning budget allocations for improvement programs to help establish the plant priorities and to facilitate buy-in on the part of all plant personnel as to the programs that are supported and those that are deferred.

- Widespread educating of plant personnel as to the nature of the budgeting process, and methods for determining the cost/benefit of improvement programs.

Among the DE plants, however, the budgeting process frequently was not as well managed. Several of the DE plants were criticized for having inadequate resources available for solution formulation and implementation. This included inadequate staffing of the engineering function, resulting in high levels of backlog for design change requests, root cause analysis and procedure modifications. This, in turn, resulted in slow or inadequate development of technical solutions. The DE plants also suffered from inadequate resources to implement solutions once they were developed. Nor was this problem simply a matter of funds available.

These plants also suffered from one or more of the following:

- Corporate management being distracted by other projects

- The lack of systematic mechanisms for assessing the importance of competing needs: no risk-based models for prioritization, no plant level goals, poor teamwork among plant functions in developing priorities. As a consequence, plant management frequently was not allocating resources toward the most important problems.

- Excessively large backlogs of unresolved items, making the need for a priority system and for management attention particularly important.

- Lack of involvement of plant staff in the budgeting and resource allocation process.

In addition to resource issues, the effective plants paid particular attention to the organizational issues associated with solution implementation. Plant management typically expended considerable effort to involve organized labor in the planning stages, thus achieving labor buy-in with the solutions. In general, solutions were formulated with the input and review of all affected parties. The DE plants apparently did not engage in similar types of behavior.

One area where both the DE and the case study plants appeared to have problems was when the solution to the performance problem involved a reorganization of the plant. These reorganizations were typically disruptive in the short run at the better plants, and in the long run among some of the other plants. The reorganizations, at minimum, seemed to cause a loss of morale on the part of managers who lost responsibility and authority during the reorganization, and in general caused concern on the part of the workforce about the direction of the plant. Among some of the DE plants, this disruption was severe. This indicates the need for care and skill on the part of upper management when reorganization is considered.

4.4 Assessment and Feedback

Assessment and feedback are also important stages in organizational learning. Once solutions have been identified and implemented, there remains the question of whether the solutions will be effective. To address this issue, organizations must have effective programs to continually monitor key aspects of performance, and outputs of these programs must find their way into decisions about whether new solutions are needed (problem identification). Again, the high performing, case study plants approach the processes of assessment and feedback considerably differently than do the DE plants.

One of the key areas where the case study and the DE plants differ concerns the level of development of the formal systems for tracking performance. In general, the case study plants had developed and were using a wide range of plant performance indicators. In most cases, the indicators exceeded considerably the list recommended by INPO. Of particular importance to learning, however, were the highly developed and effective programs for tracking corrective actions. In general, these programs indicated a very low level of corrective action backlog, indicating that problems that were being identified were also being solved. Technically competent staff with knowledge of the organization as well as the plant were employed to lead the task of tracking corrective actions. In general, it appears that these individuals served as facilitators for improvements, as well as monitors of whether the improvement schedule was being met.

In contrast, the DE plants appeared to have much less well developed assessment systems. This included generally weak QA programs, and lack of corrective action tracking systems. In addition, several of the DE plants were evaluated as having weak management involvement in oversight of the various improvement programs.

Shaping the effectiveness of the formal systems are several organizational factors. First, the nature of vertical communication appears to be very important in assessment and feedback. Where information is not allowed to flow up to management, relevant facts on plant and program performance will not be available for management decision making. Such communication is particularly inhibited when lower ranks and management lack trust of each other.

Another important organizational factor for assessment and feedback is the nature of interdepartmental relations. Where these relations are good, feedback on the effectiveness of new programs or technical solutions can flow freely. Where the relations among departments is bad, or not well developed, this information is not exchanged. In one of the case study plants, and in several of the DE plants, the existence of a large number of independent, non-integrated tracking programs, each the unique possession of a part of the organization, inhibited the effective use of performance information in plant improvement.

5.0 OBSERVATIONS AND CONCLUSIONS

For nuclear power plant organizations to be in a position to learn, they must have in place the technical and analytic skills and the formal information management programs necessary to characterize problems, define solutions, and measure the success of the solutions. However, for these technical skills and information management programs to be successful, the nuclear power plant must provide an organizational context that allows for a focused application of these resources and programs. In determining whether plants can improve from degraded levels of performance, therefore, we must be able to evaluate the organizational context and management strategy present in the plant, in addition to the quantity and quality of technical resources and the sophistication of formal information management programs. To do this, we must be able to assess the following specific items:

- The level and quality of technical resources available relative to the need for these resources
- The ability of the organization to deliver those resources to the other line organizations (operations, maintenance)
- The ability of the organization to direct the technical resources to where they are most needed through a sound process of establishing priorities among competing demands
- The ability to facilitate the flow of information among departments, groups, and ranks in the organization
- The ability to involve all affected personnel in the definition of the problem and the development and implementation of solutions

The exact strategies to be used may be highly plant specific. Certainly, we can anticipate that strategies effective in one country or for one utility may not yield the same high level of results when transplanted to another utility in a substantially different context.

REFERENCES

Haber, S., et al., "An organizational model of a nuclear power plant." Brookhaven National Laboratory, 1988.

NUREG/CR-3215. Osborn, R. et al., Organizational Analysis and Safety for Utilities with Nuclear Power Plants. 1983.

NUREG/CR-3737. Olson, J., et al., An Initial Empirical Analysis of Nuclear Power Plant Organization and its Effect on Safety 1984.

NUREG/CR-5241 Olson, J., et al., Development of Programmatic Performance Indicators 1988.

NUREG/CR-5437 Marcus, A., et al., Organization and Safety in Nuclear Power Plants 1990.

Osborn, R. and Jackson, D., "Leaders, Riverboat Gamblers, or Purposeful Unintended Consequences in the Management of Complex, Dangerous Technologies," Academy of Management Journal. Vol. 31, No.4, December, 1988.

Perrow, C. Normal Accidents: Living with High-Risk Technologies. New York: Basic Books, 1984.

Starbuck, W. and Milliken, F. "Challenger: Fine-tuning the odds until something breaks." Journal of Management Studies. July, 1988.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Conference

MIT International Program on

Enhanced Nuclear Power Plant Safety

Boston, MA June 27-29, 1990

SOCIAL AND CULTURAL LOGICS OF NUCLEAR POWER PLANT OPERATIONS

Constance Perin, PhD
Research Associate
E52-590
617/876-1566

June 28, 1990

SOCIAL AND CULTURAL LOGICS OF NUCLEAR POWER PLANT OPERATIONS

Constance Perin, PhD
Research Associate
MIT International Program on
Enhanced Nuclear Power Plant Safety
June 28, 1990

INTRODUCTION

Insofar as is humanly possible, the technical systems of nuclear power plants are designed to narrow the range of human fallibilities that might interfere with their optimally safe operations. At the same time, however, it is humanly impossible to engineer day-to-day social and cultural dynamics, which include of course timely responses to the unanticipated fallibilities of automated and technical systems. Human intelligence, experience, imagination, and cooperation remain ultimate guarantors of the safe performance of every kind of complex technological system.

Based on field observations and data collection, this study will begin to identify the social and cultural logics of nuclear power plant operations. As the human analogues to plant safety and control logics, these are unique links in the causal chain of safety performance. Ultimately, the understandings we are after should suggest a new class of indicators of conditions conducive to safety performance (Carroll and Cebon 1990: 32-34).

I welcome your ideas about how best to carry out these field studies, which I soon outline, to minimize their impacts on normal operations and maximize the possible benefits of our on-site involvement and comparative perspective.

SOCIAL AND CULTURAL LOGICS

Speaking of organizations in general, their social logics are represented in their basic architecture: How they frame and distribute accountability and responsibility, how they classify and assign the workload between human and technical resources, how they define rewards and sanctions, and how they recruit, train, and socialize their members. Management can only initiate the social logics of hierarchies, functional divisions, resource allocations, and make available the control and coordination mechanisms that tie it all together. How people carry out their tasks day by day brings to life the static social logics of organizational charts. One of our aims is to describe the social logics of nuclear power plants and the dynamics of each plant cycle.

Cultural logics can't easily be charted, partly because they're taken so much for granted that we're unlikely to think twice about them. Cultural logics consist of a linked series of implicit agreements about what matters, what means what, and why. They provide the grounds on which people live in groups of all kinds. They guide both behaviors and expectations in every domain. Until they're made explicit, they can't be renegotiated and are unlikely to change.

For example, we're all born into a basic social contract between ourselves and our family. But once we begin to think about who to invite to a wedding, and how much each relative adds to its cost, we've begun to rethink the implicit agreement about what "family" means. Then when we begin to list the friends we want to include and consider the relatives we might exclude, we're beginning to rethink the grounds of friendship as well as kinship. We may find ourselves assigning degrees of kinship or judging friends on criteria that had never before occurred to us -- or wanted to acknowledge. These are cultural logics having major consequences not only in our personal lives, but in society as well, as courts and legislatures are today renegotiating long standing agreements about the meaning of _family_.

Nuclear power plant safety may depend on equally consequential cultural logics. Studies of aviation accidents show that our unstated agreements about the relationship between politeness and rank affect cockpit behaviors. That is, we expect more politeness going up the chain of command than down. Studies of cockpit conversations after aviation accidents reveal that captains may not hear -- that is, not take in -- what crew members are telling them. _How_ actors comply with procedures and read signals turns out to be as significant as compliance per se.

An Allegheny Airlines flight to Rochester overran the runway by 728 feet, and at landing, the aircraft was going considerably faster than the recommended speed. The crew survived and the National Transportation Safety Board interviewed members about their cockpit actions. "The captain reported that he did not remember being excessively over recommended airspeed and had no explanation either for flying at excess airspeed or for not noticing it. [But] the copilot mentioned in his interview that he 'tried to warn the captain in subtle ways, like mentioning the possibility of a tailwind and the slowness of flap extension.'" The black box recording bore him out. About the flaps, the copilot had said, "Yeah the # flaps are slower than a #," to which the pilot said, "We'll make it, gonna have to add power" (Linde 1988: 379).

The co-pilot's subtle, indirect, and polite compliance with procedures -- reading the signs and giving a warning -- the pilot did not hear. The co-pilot deferred to rank, and so did the captain, who wasn't tuned in to what a subordinate was trying to convey.

Implicit agreements themselves are important, but equally important are the ways in which people interpret, use, and renegotiate them, for we also make agreements about how to do those things. Here are examples of varying degrees of direct and polite speech in the cockpit:

--Direct speech, copilot to captain: "The visibility is dropping."

--Somewhat polite speech, copilot to captain: "Let's take the shortest route to the airport."

--Very polite speech, off-duty captain to captain, when discussing a possible emergency landing: "If I might make a suggestion -- you should put your coats on -- both for your protection and so you'll be noticed so they'll know who you are."

And finally, an example of what linguists call "aggravated speech" and I call rude talk, which Americans agree should only go down the chain of command: Here is captain to flight engineer discussing possible emergency landing: "You just haul ass back there and do whatever needs doing" (Linde 1988: 383).

This study, funded by NASA to investigate "aviation accidents caused wholly or in part by problems in crew communication and coordination," confirms statistically several important hypotheses about the influence of the cultural logics of politeness on communicative success (linguists call it "mitigation"). Communicative failure means that the message was not received as the sender intended it.

> (1) Utterances going up the chain of command are more mitigated than those going down, showing that mitigation is sensitive to social rank. (2) Utterances introducing a new topic are more likely to fail if they are mitigated than if they are direct. (3) Suggestions by a crew member to the captain are more likely to fail if they are mitigated than if they are direct (Linde 1988: 375).

Although it's clear that direct speech in the cockpit is more conducive to communicative success than indirect speech, its link to safe performance is not entirely clear, given a parallel finding that crews designated as being "high in safety performance have a higher rate of mitigation than poor crews" (ibid: 395). We need to look beyond cockpit activities to their wider context. The cultural logics of mitigation and status etiquette also smooth the crew's close, often long-term relationships; they prevent animosities. Crews that maintain higher levels of politeness may therefore also have a higher level of solidarity and cooperation that translates into high safety performance.

Besides training crews in direct expression, then, this study concludes, "it would also be necessary to train in forms of communication that can challenge a superior's assessment of a situation, while indicating respect for the superior's position. At present, we know very little about how subordinates respectfully and successfully challenge superiors" (ibid: 396).

Reading narratives of the TMI-2 accident, I'm struck first by the absence of graphic images to portray the network of actors and their communication. They identify the chief actors categorically, but not interactively or systematically. They designate them by job title alone, which by itself conveys no sense of their rank or their level of expertise. There is no depiction of their communication patterns in both normal and abnormal situations nor of the plant's spatial organization. The actors aren't situated, that is, in terms of their reciprocal, systematic relationships as senders and receivers of information and interpretations.

In general, talking and listening, asking questions and answering them, and understanding and misunderstanding are fundamentally organized by social and cultural logics. For example, women have known for some time what studies of meetings have begun to document: Even with equal rank, what they say is likely to evoke frowns and what men say, smiles and nods of approval. Their ideas are unlikely to get a hearing until a man repeats them. Women are more likely to be interrupted than are men. Such conditions, I suspect, may also hold true for men in junior or subordinate positions and for newcomers to organizations, for example.

On the other hand, ranked relations yield to the imperatives of safe behavior on aircraft carriers, for example. The social distance between order givers and takers narrows "as the tempo of operations increases....[f]ormal rank/status declines as a reason for obedience. Hierarchical rank defers to technical expertise often held by those of lesser formal rank. Chiefs advise Commanders, gently direct Lieutenants, and cow Ensigns. Criticality, hazard, and sophistication of operations prompts a kind of functional discipline, a `professionalization' of the work teams. Feedback and (sometimes conflictual) negotiations increase in importance; feedback about `how goes it' is sought and valued" (La Porte and Consolini 1989: 13).

FIELD STUDIES

The most fertile source of social and cultural logics at work is in to be found in the ways people conceive of and carry out their work. We are interested in describing work systems during each plant cycle and in collecting data on routine problem-finding behaviors during these normal times. Work systems I define as the people and tools involved in carrying out specific tasks, whether confined to a single function or across functions. We are equally interested in administrative and technical work systems.

1) Work Systems Studies

To acquire data with which to describe and systematize the social and cultural logics of nuclear power plants, we need to observe and describe each work system or a sample of work systems during each plant cycle, through all shifts. Making the work system the basic unit of data collection will permit comparison across sites; they will vary of course by the technology. The data needed to describe work systems are both objective and subjective.

<u>Objective Data on Work Systems:</u>

Program: The program of a work system is composed of its mission and tasks, the inputs it requires and the outputs others expect from it.

People: Demographic and organizational information about each work system and its members (i.e., numbers, training, sex, organizational role, pay range, incumbency and turnover).

Performance: Current performance appraisal systems applying to each role and the rewards and sanctions in force.

Tools and Setting: For each task in the work system, how people, tools, and the physical environment are arranged and rearranged for each cycle.

<u>Employees' Perceptions of Work Systems:</u>

Routine and Nonroutine Tasks: How employees describe their day, week, and month dividing between more and less routine activities.

Authority and Responsibility: Employees' understandings of how these are distributed and exercised formally and informally.

Images of Plant Organization: How do they see the organization and interdependencies of work in the plant as a whole? How do their images or theories of the organization map onto actual interdependencies?

Work Communication Networks: Who do they regard as being essential to their work, whether or not they are in their function, in their formal workgroup, within or outside the plant? How often are they in contact, what are the the topics at issue, and how critical are they? Where are they physically located and what channels do they use (telephone, computer, memo, meeting)? What is the character of each communicative event, e.g., getting/giving information or advice, checking or verifying information? Who initiates communication? (We expect these networks to cross not only functional boundaries but also plant boundaries -- peers in other plants, NRC staff, union staff, academics.)

These data will allow us to specify the nature of the social and cultural logics of nuclear power plants. They will also allow comparisons between assumed and actual interdependencies and of the relative importance of formal and informal channels of communication by topic. On the basis of these initial data we will design further detailed studies, which may use survey methods.

2) Problem Recognition Studies

TMI-2 accident narratives dramatize the centrality of problem recognition. Reading various signals, actors found them so far out of pattern and so foreign to expectations, that they dismissed the original events as "not credible." Heard as a "thud," the significance of the hydrogen spike was unappreciated for a day and a half, "written off" as an instrument malfunction. Actors disbelieved the valve signals yet believed the temperature signals.

In being so alien, these signals elicited rejection instead of curiosity -- people are prone to behave this way toward any event or object that doesn't fit what they expect, when the degree of difference is great. They avoid the problem instead of approaching it, as they are likely to do when the difference is smaller. The signals were literally unrecognizeable and unthinkable in the cognitive and interpretive frames that actors habitually used. The question of interest here is whether and to what extent their technical and procedural logics are, as in cockpits, accompanied by social and cultural logics.

To collect data with which to pursue that question, we will ask a sample of employees to provide detailed accounts of situations where they recognized, interpreted, and communicated about unexpected, nonroutine events, whether or not they saw them as being directly related to safety. Who did they talk to? What did they do (e.g., refer to manuals, seek new information)? How did they interpret each event's meaning? These accounts of responses to out of pattern events are likely to provide spontaneous evidence of social and cultural logics not normally displayed and voiced. Studying "simple" cases may help us to understand the nontechnical logics involved in more complex sequences where recognition and interpretation are crucial to safety performance and behaviors. We hope also to observe such events in real time.

How they tell their stories about handling exceptions is also important data about more general interpretive and sensemaking practices. These accounts will also help us learn how employees use feedback loops, how learning occurs, and how they balance initiative, innovation, and creativity with procedural compliance.

We expect therefore to be able to speak to management and training issues as well. Do employees need special training to acknowledge rather than reject out of pattern information and events? Do they need a larger store of schemata or scripts, in order to interpret the significances of unexpected signals? In discussing their inferences and checking their observations with one another, do they reveal tendencies not only toward customary patterns of social deference, but toward closing out alternatives? Do their communicative patterns suggest a knowledge hierarchy that only partially maps onto the authority hierarchy?

CONCLUSION

This research strategy does not propose to codify social and cultural criteria for safety performance, but instead to flag communicative and social conditions under which safety behaviors are likely to flourish. Ultimately we should be able to identify organizational conditions that stand a good chance of reducing misrecognition, miscommunication, misinterpretation, and incorrect inferences.

As engineers, operators, and managers confront warning signals and discuss their interpretations and check their inferences with one another, they may also be relying on cultural logics alongside their technical knowledge. They may be drawing not only on their national culture, but on plant culture, occupational culture, and regional culture as well. Local plant rules and procedures that take into account these many cultures remain essential because clear communication depends on implicit agreements of such depth and density that nontechnical logics may vary even plant to plant, no matter how universalized the technical operations may be. There are hints in the literature, for example, that different regions of the USA work from different agreements about what constitutes politeness -- an experience we've all had, I'm sure. Cross-national comparisons are for this reason also important, not only to test that proposition, but as well to learn how organizational policies and operating procedures adapt to national and regional cultures -- and vice versa.

Finally, in focusing on work systems and communicative networks, this anthropological approach emphasizes the social contexts that influence individuals' behavior. Being appreciated, encouraged, and trained appropriately provides the basic motivation to work responsibly. That support is a social product that individuals transform first into a personal resource and then into feelings of loyalty and involvement. Human factors specialists tend to measure individuals' relationships to tools, without factoring in the constraints and opportunities of their social and physical environments. Organizational psychologists may emphasize personal traits over peer influences. Compensation systems may reward individual performance when management expects superior team performance.

Although we generally agree that ultimately individuals as responsible for their behaviors, we can all cite situations that bring out the best and worst in us, l'm sure. Complex, tightly coupled, and highly consequential technological systems create work situations that can afford only to bring out the best in people, depending as they do on human systems that have no alternative but to operate at the highest levels of cooperation, alertness, and open communication.

Bibliography and References

Carroll, John S. and Peter Cebon. The Organization and Management of Nuclear Power Plants. n.d. Sloan School of Management, MIT. Cambridge, Mass.

Kemeny, J. The Need for a Change: The Legacy of TMI. Report of the President's Commission on the Accident at Three Mile Island. Washington, D.C.

La Porte, Todd R. and Paula M. Consolini. "Working in Practice but Not in Theory": Theoretical Challenges of `High Reliability Organizations.' Department of Political Science, Institute of Governmental Studies, University of California, Berkeley. March 1989.

Linde, Charlotte. The Quantitative Study of Communicative Success: Politeness and Accidents in Aviation Discourse. Language and Society, V. 17, pp. 375-399. 1988.

Marcus, Alfred A., et al. Management, Organization and Safety in Nuclear Power Plants. Draft report, August 1989, prepared for the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.

Three Mile Island: A Report to the Commissioners and to the Public, Volume I. NUREG/CR 1250, U.S. Nuclear Regulatory Commission. M. Rogovin, Director, Nuclear Regulatory Commission Special Inquiry Group. Washington, D.C.

Organisation and Management of WANO

18 March 1991

WANO Coordinating Centre

Ryuichi Nakazono

1. **WANO**
2. **The Mission of WANO**
3. **Organisation**
4. **WANO Members**
5. **Implementing WANO activities**
6. **WANO Programmes**
7. **WANO NUCLEAR NETWORK system**
8. **Funding and Staff of Centres**
9. **Summary**

1. WANO

The benefit of nuclear power can be brought to mankind only if safety is kept at the highest level. The ultimate safety responsibility for nuclear electricity generation rests upon the organisation that operates the nuclear power plant.

Each nuclear utility has an individual responsibility to guarantee safety. The utilities also have a collective responsibility to work together to improve their performance and to upgrade continually the safety of operating plants.

One proven effective way of promoting the safety and reliability of nuclear power is the mutual exchange of information on nuclear power plant operations between utilities. In this way, the utilities can all learn from one another, they can help one another, and they can raise the performance of all to the standards of the best.

For these reasons, the World Association of Nuclear Operators was created.

WANO was incorporated in the UK on 9 May 1989 as a company limited by guarantee under the Companies Act 1985, and was inaugurated at the first meeting of the General Assembly held in Moscow on 15-16 May 1989.

2. The Mission of WANO

The mission of WANO is to maximise the safety and reliability of the operation of nuclear power plants by exchanging information and encouraging communication, comparison and emulation among its members.

In carrying out its mission WANO will strive to:

- Promote bilateral and multilateral exchange and use of operating experience information among members.

- Provide members with early notification and follow-on information on significant events.

- Screen and analyse events that occur at nuclear power plants world-wide in order to identify possible precursors of more serious events and disseminate lessons learned.

- Identify and promote the use of good practices among members.

- Encourage comparisons of operations and emulation of high standards among members through sponsorship of exchange visits. Encourage sharing of methodologies among members through sponsorship of workshops and seminars.

- Collect, maintain and use data on selected performance indicators to improve nuclear plant performance in area such as nuclear plant safety and reliability, plant efficiency, and personnel safety.

- Maintain cooperative relationships with international organisations, such as IAEA, working to promote safety and reliability of nuclear power plants.

- Effectively manage WANO resources.

3. Organisation

3.1 Structure

The structure of WANO consists of a General Assembly, a Governing Board, a Coordinating Centre in London and four Regional Centres located in Atlanta, Moscow, Paris and in Tokyo.

3.2 General Assembly

Each member of WANO is entitled to appoint one official representative to the General Assembly.

The General Assembly ratifies changes to the Charter of WANO and advises on other matters put to it by the Governing Board.

3.3 Governing Board

The Governing Board of WANO manages the activities of WANO and consists of either eight or nine voting members as follows:

- The Chairman of the Governing Board of each Regional Centre
- One member of the Governing Board of each Regional Centre
- A Chairman who may or may not be elected from among the eight Regional Members

3.4 Coordinating Centre

The Coordinating Centre is under the direction of the Governing Board of WANO.

The primary function of the Coordinating Centre is to assist the Regional Centres in coordinating their work and in communicating efficiently to carry out the mission of WANO.

3.5 Regional Centres

Each Regional Centre is under the direction of the Regional Centre Governing Board. Each Regional Centre operates independently.

4. WANO Members

4.1 Membership

A member of WANO may be either:

- an individual operator of nuclear power plants
- an organisation representing a group of operators

An operator or operator organisation cannot be a member of WANO without belonging to a Regional Centre. Each operator or operator organisation is free to join the Regional Centre or Centres most suited to its need.

Recognising that the safety of each individual plant affect the viability and acceptability of nuclear power plants throughout the world, all members accept:

- their individual responsibility for the nuclear power plant they operate

- their collective responsibility to inform, help and emulate other nuclear operators,

by the provision and effective use of operating experience.

To facilitate the free flow of information within WANO each member undertakes to safeguard the information it receives and release information outside WANO only if authorised to do so by the originating WANO member.

4.2 WANO Members

The Regional Centres have the following members.

Atlanta Centre:

- United States NPPs
- Canadian NPPs
- Mexican NPPs
- Yugoslav NPPs

Moscow Centre:

- Soviet Union NPPs
- IVO for Finland
- Bulgarian NPPs
- Hungarian NPPs
- Czechoslovak NPPs
- Polish NPPs
- Cuban NPPs
- German(East) NPPs

Paris Centre:

- French NPPs
- Belgian NPPs
- TVO for Finland
- Spanish NPPs
- Swiss NPPs
- Brazilian NPPs
- Argentinean NPPs
- South African NPPs
- Italian NPPs
- Dutch NPPs
- German(West) NPPs
- British NPPs
- Swedish NPPs

Tokyo Centre:

- Japanese NPPs
- South Korean NPPs
- Taiwanese NPPs
- Indian NPPs
- Pakistani NPPs
- Chinese utilities are observers

5. Implementing WANO activities

Each Regional Centre operates independently. The members of each Regional Centre decide how their centre is organised and operated.

The Coordinating Centre is to assist the Regional Centres in coordinating their work and in communicating efficiently to carry out the WANO mission.

In order to have consistency of the implementation of WANO activities, the WANO Charter and the Policy Guidelines define the WANO programme.

Whereas the Charter and the Policy Guidelines specify the basic WANO programmes, the WANO planning process begins with the Long Term Plan. From this broad statement of overall goals of the organisation, two year goals are developed. Annually, specific, measurable objectives are established to meet the two year goals. Regional and Coordinating Centres develop their own objectives and work plans that are in harmony with, and support, the achievement of the WANO goals and objectives.

6. WANO Programmes

The following four major programmes are being developed.

- Operating Experience Information Exchange Programme
- Operator to Operator Exchange Programme
- Good Practice Programme
- Performance Indicator Programme

6.1 Operating Experience Information Exchange Programme

The Operating Experience Exchange Programme is an event reporting system through WANO NUCLEAR NETWORK. There are two types of reporting.

- To provide early notification of significant events
- To provide follow-up analysis reports including cause analysis and actions to be taken

The criteria for issuing reports are specified in the relevant Policy Guideline.

6.2 Operator to Operator Exchange Programme

To exchange information about plant operation, management organisation, maintenance, chemistry, radiological protection, emergency preparedness, technical support, public acceptance, good practice and so on through following activities:

- technical exchange visits
- seminars
- workshops
- direct information exchange through NUCLEAR NETWORK

6.3 Good Practice Programme

In order to share the good performances of plant operation, good practices are collected through exchange visits, workshops, seminars and documentation reviews, and disseminated among the members of WANO.

6.4 Performance Indicator Programme

Ten WANO Performance Indicators have been adopted to provide a quantitative indication of nuclear plant performance in the areas of nuclear plant safety and reliability, plant efficiency, and personnel safety.

These indicators are intended for use by nuclear operating organisations to monitor performance and progress, to set challenging goals for improvement, to gain additional perspective on performance relative to that of other plants, and to provide for the indication of a possible need to adjust priorities and resources to achieve improved overall performance.

WANO performance Indicators are intended to support the exchange of operating experience information and to allow consistent comparisons of nuclear plant performance.

It is expected that the WANO performance indicators will encourage emulation of the best industry performance and further motivate the identification and exchange of good practices in nuclear plant operation.

7. WANO NUCLEAR NETWORK system

In order to help WANO members to share information relative to the safe and reliable operation of nuclear power plants, WANO uses an electronic mail system which is the WANO NUCLEAR NETWORK.

The information is classified in the following Topics permitting different communication channels between members and Regional Centres and including data base.

WANO Topics

- Communication among Regional Centre and Coordinating Centre
- Coordination within each Regional Centre
- Coordination within WANO
- WANO Event Reports
- Miscellaneous Event Reports

8. Funding and Centres' Staff

WANO is a non-profit making organisation. The costs of WANO are fully funded by its members.

The Coordinating Centre and each Regional Centre operate with the minimal staff necessary including seconded engineers to the Centre from its members. Most of the information exchange is ensured by the electronic mail system or by direct contacts between operators during technical exchange visits, workshops or seminars.

9. Summary

WANO is now well established as an organisation.

WANO was created by operators, for operators and has their full support.

WANO operates with the minimal staff necessary.

The WANO NUCLEAR NETWORK has been established.

Operator to Operator direct communication system has been established.

INTERNATIONAL ATOMIC ENERGY AGENCY

THE

A S S E T

(Assessment Of Safety Significant Events Team)

S E R V I C E S

PREVENTION OF INCIDENTS

THE PATH TO EXCELLENCE IN

OPERATIONAL SAFETY

B.A. Thomas

February 1991

-Content-

* * *

I. THE IAEA SAFETY ACTIVITIES

The International Atomic Energy Agency was assigned two main roles at its creation in 1957:

- Prevent diversion of nuclear materials for military purposes
- Promote development of peaceful applications of nuclear energy in areas such as biology, medicine, agriculture, etc... and generation of electricity.

During the three-past decades, safe use of nuclear energy for electricity generation became an increasing concern of the public (accident of Chernobyl, Windscale, Three Miles Island, Goiana, etc..). This led to the development of a still growing work force within the IAEA under the supervision of the Division of Nuclear Safety.

The safety activities of the IAEA are threefold:

- Produce safety guides for regulatory and operating organizations

  Recently, these efforts were concluded by the basic safety principles, Safety Series No. 75 INSAG-3 1988 followed by Safety Series No. 75-INSAG-4 1991, a document dealing with safety culture. The next step should advise on techniques of assessment of operational safety at NPPs.

- Promote exchange of experience on the numerous aspects of plant safety.

  This continuous effort is made through organization of meetings by the IAEA or participation in meetings organized within the nuclear community. It is, however,recognized that this process does not involve high participation of NPPs operators.

- Provide services to nuclear power plant in order to assess and recommend enhancement of operational safety.

The Services offered by the IAEA are meant to exchange first hand technical experience on the field where operators are dealing with the daily safety issues during plant operation.

II. THE IAEA SERVICES TO NUCLEAR POWER PLANTS

The IAEA offers three types of services to address plant safety in the following areas:

- Design
- Operation (OSART)
- Management of the plant programme for prevention of incident (ASSET)

Since 1991, in the frame of the project devoted to older reactors, reviews of design identify weak points, assess their significance to safety and recommend hardware modifications.

Since 1983, reviews of operational practices by Operational Safety Review Teams (OSART) identify shortcomings, assess their importance to safety and recommend improvements of procedures and working practices.

Since 1986, review of operating experience by Assessment of Safety Significant Events Teams (ASSET) identify operational issues relevant to safety, rate their significance, conduct root cause analyses and recommend corrective actions to improve management of operational safety by enhancing prevention of incidents.

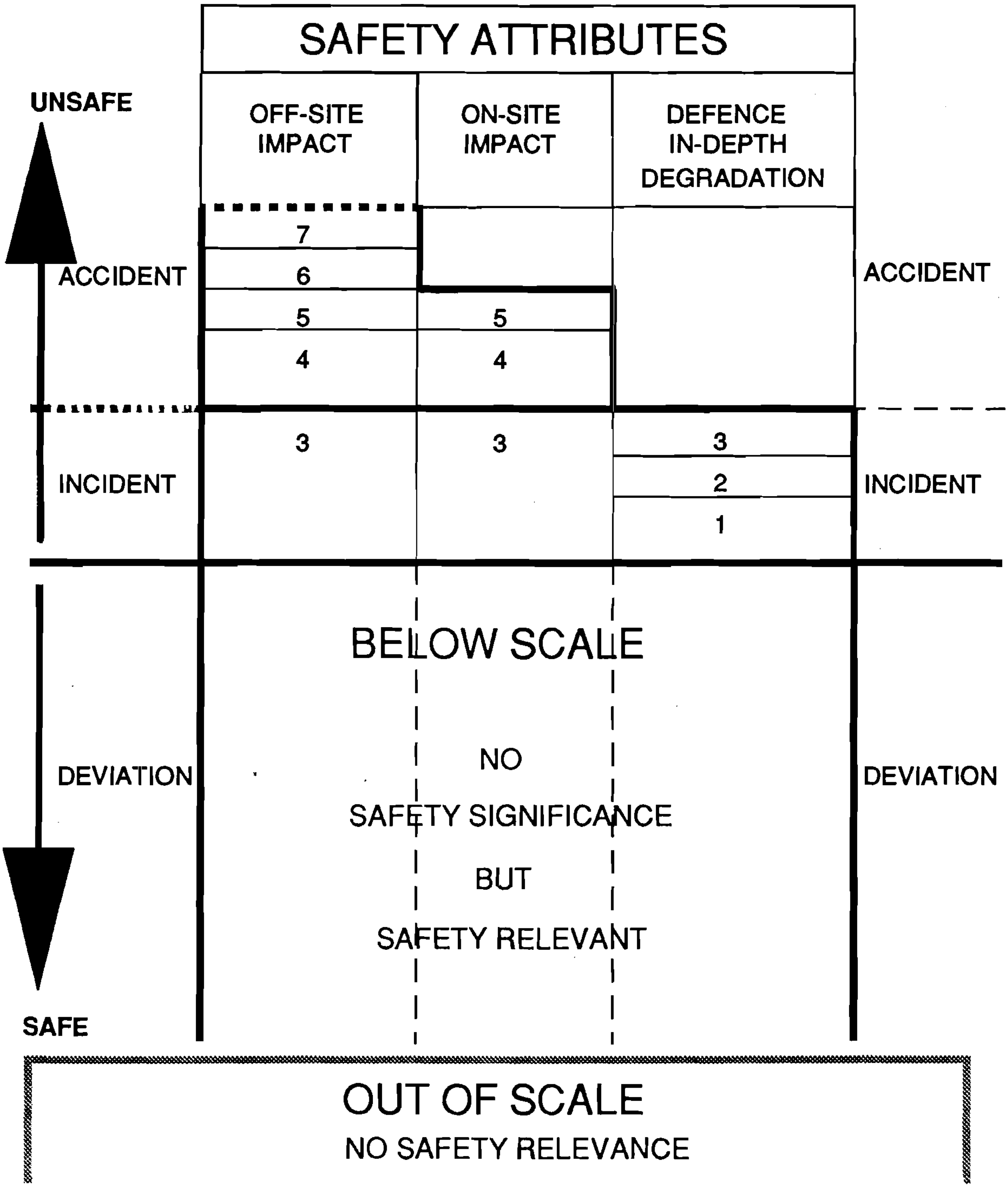
The growing popularity of the systematic ASSET investigation methodology among IAEA Member States has led to numerous requests for the ASSET services (missions and training session). Since 1990, the IAEA is being requested to train staff of operating and regulatory organizations on the use of the ASSET tools: INES rating of significance to safety and ASSET root causes analysis.

Appropriate management of the plant programme for prevention of incidents, operation and design, are the most important aspects addressed by the ASSET services while reviewing plant operating experience.

The optimum achieved through operational provisions made at plants to compensate for the weak points of the design is the challenge addressed by the ASSET approach.

THE INTERNATIONAL NUCLEAR EVENT SCALE

SAFETY CONCEPT



III. THE INTERNATIONAL NUCLEAR EVENT SCALE (INES)

On 28 March 1990 as a result of a general consensus, the International Nuclear Event Scale was accepted for a trial implementation period at the end of which the INES leaflet and the User's Manual might be amended to include experience gained.

As of 30 December 1990, 25 countries had already informed the IAEA that the Scale is officially implemented to rate the safety significance and accepted to report to the IAEA within 24 hours delay all the nuclear events of level 2 and above, for worldwide dissemination.

Beyond the initial public information purpose, the safety concept conveyed by the scale represents a major step forwards to redirect managerial attention to enhancement of plant programmes for prevention of incidents, the major cornerstone for long term operational safety.

The Scale is not an analytical tool. The Scale is a rating tool based on seven levels and three safety attributes: off-site impact, on-site impact and degradation of defence-in-depth. The levels, their descriptors and detailed criteria are shown together in the INES leaflet with examples of classified nuclear events which have occurred at nuclear power plants. The lower levels (1-3) are termed incidents, and the upper levels (4-7) accidents. Events which have no safety significance are classified as Below Scale/Level Zero. Industrial accidents or other events which are not related to nuclear plant operations are not classified on the scale; these are termed Out of Scale.

The matrix of the INES leaflet explains the underlying logic of the Scale. Key words indicate generally the safety significance and are not intended to be precise or definitive.

The first safety attribute applies to events resulting in releases of radioactivity off-site. Understandably, the public is most concerned with such external releases. Level 7, the highest in this column, corresponds to a major nuclear accident with widespread health and environmental consequences.

Level 3, the lowest point in this column, represents a very small release that would result in a radiation dose to the most exposed members of the public equivalent to a fraction of the prescribed annual dose limit for the public. Such a dose is typically about a tenth of the average annual dose from exposure to natural background radiation.

The second safety attribute considers the on-site impact of the event. The range is from Level 5, typically representing a situation of severe damage to the nuclear reactor core, down to Level 3 at which there is major contamination and/or over-exposure of workers.

The third safety attribute applies to events involving the degradation of plant's defence-in-depth. All plants are designed such that a succession of safety systems act to prevent major on-site and off-site impacts. The defence-in-depth considerations classify event as Levels 3 through 1.

An event which has characteristics represented by more than one safety attribute is always classified at the highest level according to any one criterion.

The International Nuclear Event Scale provides finally a common understanding on the definition of accidents, incidents, deviations and on the definition of a threshold of significance for each of the three safety attributes.

THE INTERNATIONAL NUCLEAR EVENT SCALE (INES)

EVENT RATING FORM (ERF)

to be sent to: IAEA, WAGRAMERSTRASSE 5, P.O.BOX 100, A-1400 VIENNA, AUSTRIA
TELEX: 1-12645, CABLE: INATOM VIENNA, FACSIMILE: 43 1 234564, TELEPHONE: 43 1 2360 2685

EVENT TITLE											EVENT DATE	
RATING INES	LEVEL	0	1	2	3	4	5	6	7	CRITERION	DEGR. DEFENCE IN-DEPTH	
											ON-SITE IMPACT	
											OFF-SITE IMPACT	
COUNTRY		PLANT NAME								REACTOR TYPE POWER		

SHORT DESCRIPTION OF THE EVENT : *

BASIS FOR RATING OF THE EVENT : *

DIFFICULTIES ENCOUNTERED IN EVENT RATING : *

CONTACT PERSON FOR FURTHER INFORMATION	NAME	
	ADDRESS	
	PHONE	
	FAX	

* PLEASE, ATTACH ADDITIONAL INFORMATION IF NEEDED

IV. THE ASSET BASIC PRINCIPLES: Prevention of incidents, the path to excellence in operational safety.

The public demands safe generation of electricity by nuclear power plants. Probabilistic considerations that imply possible occurrence of accidents, even at low likelihood, are met with reservation by the public. Accidents are unacceptable. Incidents must be prevented.

According to the safety concept conveyed by the International Nuclear Event Scale (INES), a plant is operated in a fully safe manner when each of the three safety attributes; off-site impact, on-site impact, degradation of defence-in-depth, are kept below the specific thresholds of significance that define the lower boundary of the Scale.

Any exceedance of one of the three thresholds is significant to safety and considered as an incident or an accident that is classified from level one to seven on the basis of the event consequences off-site, on-site or on plant defence-in-depth.

Below Scale events are not significant to safety and are considered to be deviations. However, deviations relevant to the three safety attributes remain the main concern of plant managements that are dedicated to prevention of incidents. Deviations are precursors that provide potential for future occurrence of incidents if remedies are not systematically implemented to eliminate root causes.

Sound design and adequate operation are prerequisites for electricity generation without incident but not sufficient.

Effective management of a comprehensive plant programme for prevention of incidents is the key factor for long term safe operation as demonstrated by numerous nuclear power plants worldwide that did not and will not experience any accident and incident classified on the Scale. The plant programme for prevention of incidents ensures that the three basic elements that currently interact in any industrial process are at the optimum level of quality in order to perform as expected: Man (personnel proficiency), Machine (equipment operability), Man-Machine Interface (procedures adequacy).

Three successive barriers under close control of plant management enable timely elimination of all latent weaknesses that may lead to incident or accident under adverse circumstances:

- A systematic quality control programme to ensure that the level of quality required for personnel, equipment procedures, is achieved prior to be used in plant operation.

- An effective preventive maintenance programme to ensure that the level of quality required is maintained during operation.

- A comprehensive plant surveillance programme to ensure that any fortuitous degradation of the level of quality required is timely detected and promptly restored.

Enhancement of tightness of these three successive barriers is the aim of plant striving for excellence in operational safety.

Prevention of incidents is a dynamic process that can only be successful through systematic in-depth analysis of all deviations below INES followed by implementation of the necessary improvements to close the operating experience feedback loop.

The ASSET (Assessment of Safety Significant Events Team) root cause analysis method provides the powerful tool needed by plant management to build up safer operation.

The ASSET approach offers a systematic way to handle safety issues in order to address both, the technical and the managerial aspects of nuclear power plant.

The ASSET approach promotes an adequate response to the definition of Safety Culture given by the Safety Series No. 75-INSAG-4 1991:

❖ SAFETY CULTURE ❖

IS THAT ASSEMBLY OF CHARACTERISTICS AND ATTITUDES IN ORGANIZATIONS AND INDIVIDUALS WHICH ESTABLISH THAT, AS AN OVERRIDING PRIORITY, NUCLEAR POWER PLANT SAFETY ISSUES RECEIVE THE ATTENTION WARRANTED BY THEIR SIGNIFICANCE.

SAFETY SERIES NO. 75 INSAG-4-1991

THE ASSET RESPONSE

- ❑ SAFETY ISSUES ARE IDENTIFIED THROUGH A COMPREHENSIVE PLANT SURVEILLANCE PROGRAMME CAPABLE OF TIMELY DETECTING ANY LATENT WEAKNESS AMONG PERSONNEL, EQUIPMENT, AND PROCEDURES.
- ❑ SIGNIFICANCE TO SAFETY IS ASSESSED ON THE BASIS OF THE INTERNATIONAL NUCLEAR EVENT SCALE (INES).
- ❑ ATTENTION IS PAID THROUGH SYSTEMATIC ROOT CAUSE ANALYSIS OF ALL DEVIATIONS BELOW SCALE TO ENHANCE PREVENTION OF INCIDENTS.

V. THE ASSET APPROACH

The ASSET approach is based on the following:

EVENTS (DEVIATIONS, INCIDENTS or ACCIDENTS) occur always because of a

FAILURE (OCCURRENCE) to perform as expected due to a

LATENT WEAKNESS (DIRECT CAUSE) [poor preparation prior to operation or degradation during operation] which was not promptly eliminated owing to a deficiency in the plant programme of

SURVEILLANCE (ROOT CAUSE) [detection or restoration] of equipment, personnel or procedures.

The main concern in the ASSET approach is therefore with the effectiveness of the policy for the prevention of incidents at nuclear power plants, which is the cornerstone of long term operational safety.

Provisions made at plants for mitigation of accidents are meant to palliate for unreliable prevention and are therefore out of the scope of the ASSET approach.

The ASSET approach is based on commonly shared principles, as outlined, for example, in IAEA Safety Series No. 75-INSAG-3, the International Nuclear Safety Advisory Group's Basic Safety Principles for Nuclear Power Plants (1988). and No 75-INSAG-4 1991: Safety Culture (1991). Safe operation and good performance at nuclear power plants require a reliable interaction of the three basic elements: proficient personnel, operable equipment, and adequate procedural guidance.

In the ASSET programme, it is recognized that personnel, equipment or procedures should not necessarily be held responsible for failure to performing as expected during on-line operation. Incidents may demonstrate only that these basic elements were not well enough prepared, maintained or restored to ensure safe and reliable operation. Plant management control is decisive and human performance is crucial in carrying out activity related to safety.

An occurrence or failure to perform as expected results always from the existence of a latent weakness (direct cause) that was not timely eliminated due to a deficiency of the plant surveillance programme (root cause).

A latent weakness results always either from poor control of quality of the final products prior to be used in operation or from degradation due to poor preventive maintenance during operation.

Deficiency of plant surveillance programme, due to either poor detection capabilities or poor restoration process when a latent weakness is detected, results always from either inadequate surveillance policy or inappropriate implementation of the surveillance programme.

Inadequate plant surveillance policy results from a lack of a clear safety objective in management of plant operational safety performance.

Incidents classified on the INES result therefore from a failure of the plant management process in the area of prevention of incidents.

Management of the plant programme for prevention of incidents concentrates therefore on improvement of the tightness of the three successive barriers:

- "Quality control" prior to operation and "preventive maintenance" during operation to prevent latent weaknesses.

- "Surveillance" to timely eliminate latent weaknesses resulting from untightness of the two first barriers.

The plant surveillance programme:

- is the ultimate barrier for prevention incidents,

- is expected to provide plant managers with early signals for timely corrective actions.

- is comprehensive and updated systematically on the basis of operating experience and new studies.

- includes two types of monitoring:

  (1) periodic testing of the level of quality of the three basic elements involved in plant operational safety.

    * testing of personnel proficiency
    * testing of equipment operability
    * testing of procedures adequacy

  (2) trending of safety indicators to assess results of plant managerial practices under the three safety attributes:

    * off-site impact
    * on-site impact
    * degradation of defence-in-depth

- includes low thresholds acceptance criteria in order to identify deviations.

- requires systematic root cause analysis of all deviations even the most benign.

- requires systematic implementation of corrective actions to restore the level of quality required and improve, if needed, the capability of the plant surveillance programme.

VI. THE ASSET INVESTIGATION METHODOLOGY

The primary objective is to address the plant managerial practices regarding prevention of incidents. This is achieved through a detailed review of past operating experience intended to provide conclusions on appropriateness and completeness of corrective actions implemented.

The review of plant operating experience is carried out according to the ASSET investigation methodology as follows:

- Identification of events relevant to safety
- Rating of significance of the events relevant to safety
- Selection of safety issues significant or recurrent
- Root cause analysis of selected safety issues

6.1 Identification of events relevant to safety

The review concentrates on the operational events reported according to the Regulatory Body reporting criteria.

Firstly, the Regulatory Body reporting criteria are reviewed to verify if they are at least covering all aspects connected with the three safety attributes off-site impact, on-site impact and degradation of defence-in-depth.

Secondly, reporting thresholds are reviewed in order to make sure that not only accidents and incidents but also deviations below scale are reportables.

Thirdly, plant compliance with the Regulatory Body reporting criteria is verified through a few examples.

If conclusions of one of the three previous verifications are negative, there is a need to complement the list of operational events to be reviewed.

If conclusions of the previous verifications are all three positive, the operational events reported are reviewed individually to identify those that had consequences off-site, on-site or on the defence-in-depth according to definitions provided by the User's Manual of the International Nuclear Event Scale:

- Off-site impact: * Radioactive releases (gaz, liquid, solid)
- On-site impact: * Radioactive doses to workers (irradiation, external and internal contamination).
  * Contamination of plant (surfaces, atmospheric)

- Degradation of defence-in-depth:

  * Degradation of tightness of the safety function "BARRIERS" (fuel cladding, primary boundary, containment).

  * Degradation of operability of the safety function "PROTECTION" (control of reactivity, cooling fuel, confinement of radioactive products).

  * Degradation of operability of safety functions "SUPPLY" (electrical power off-site, electrical power on-site, service water, control and instrument air).

  * Degradation of proficiency of personnel (violations of operational limits and conditions, violations of maintenance and operating procedures).

  * Degradation of adequacy of procedures.

  * Degradation of effectiveness of plant surveillance (more fortuitous events than deviations detected by surveillance).

This review is expected to identify two groups of events among the population of operational events reported; the events that are safety relevant and the events that are out of Scale.

Additional conclusions are provided on the safety relevant events regarding nature of occurrences (equipment or personnel or procedure failure), direct causes, root causes, corrective actions implemented, generic lessons and suggested areas for improvement.

6.2. Rating of significance of events relevant to safety

The International Nuclear Event Scale is used as rating tool to categorized the events relevant to safety in two groups: the events below scale that are not safety significant and the events significant to safety that are classified on the Scale.

The lower boundary of the Scale that defines the border between safety significant and non-safety significant events corresponds mostly to the limits of the authorized functional domain (operational limits and conditions that include technical specifications).

The rating procedure requires to consider first the off-site impact of the event, then the on-site impact, then the impact on the plant defence-in-depth and to take the higher rating as final classification.

Most of the events relevant to safety are however categorized under the safety attribute "degradation of defence-in-depth". The significant ones are classified at levels 1, 2, or 3.

The rating procedure is based on the combination of two concepts: the initiator frequency (expected, possible, likely) and the availability of the safety functions (full, within operational limits and conditions, adequate, inadequate).

This approach enables to assign a weight to the degradation of defence-in-depth which corresponds to levels 1, 2 or 3 on the Scale.

It should be noted that the rating procedure assumes that the safety functions are appropriately designed to cope with the initiators taken into account in the plant studies and that the operational limits and conditions are adjusted accordingly.

A wide variety of systems are usually provided to ensure the safety function "PROTECTION" (control of reactivity, cooling of fuel, confinement of radioactive products) and the safety function "SUPPLY" (electrical power off-site, electrical power on-site, service water, control and instrument air). The list and frequency of initiators considered for designing safety function vary also from one plant to another according to the specific environmental conditions and plant design features.

The rating procedure of events related to degradation of defence-in-depth does not include therefore any critical review of the completeness of the list and frequency of initiators considered and of the appropriateness of the design of the safety functions (redundancies, etc.).

6.3 Selection of safety issues for root cause analysis

The objective of the third stage of the ASSET investigation methodology is to select safety issues that provide an accurate picture of the main safety concerns at the plant.

This selection is made from the population of events relevant to safety. The events most significant to safety are not necessarily selected particularly if corrective actions implemented are appropriate and complete.

The basic idea is to select safety issues that are still pending because corrective actions are either inappropriate or incomplete. Useful recommendations based on international operating experience can therefore be offered to cope with the problem.

As an ASSET is always limited in time, the selection is often restricted to three pending safety issues of crucial interest. Selection of safety issues is mostly based on a combination of two criteria: recurrence and significance.

Non-compliance with procedures, insufficient detection capabilities of the plant surveillance programme are examples of safety issues selected on the basis of the criterion recurrence.

Insufficient prevention of fires that may affect safety systems, risk of damage within the pressure boundary as a result of local surpression due to explosive recombination of radiolytic hydrogen are examples of safety issues selected on the basis of the criterion significance.

Safety issues selected for root cause analysis are usually related to the three following areas:

I. Management of the plant programme for prevention of incidents.

such as insufficient detection capabilities of the plant surveillance programme

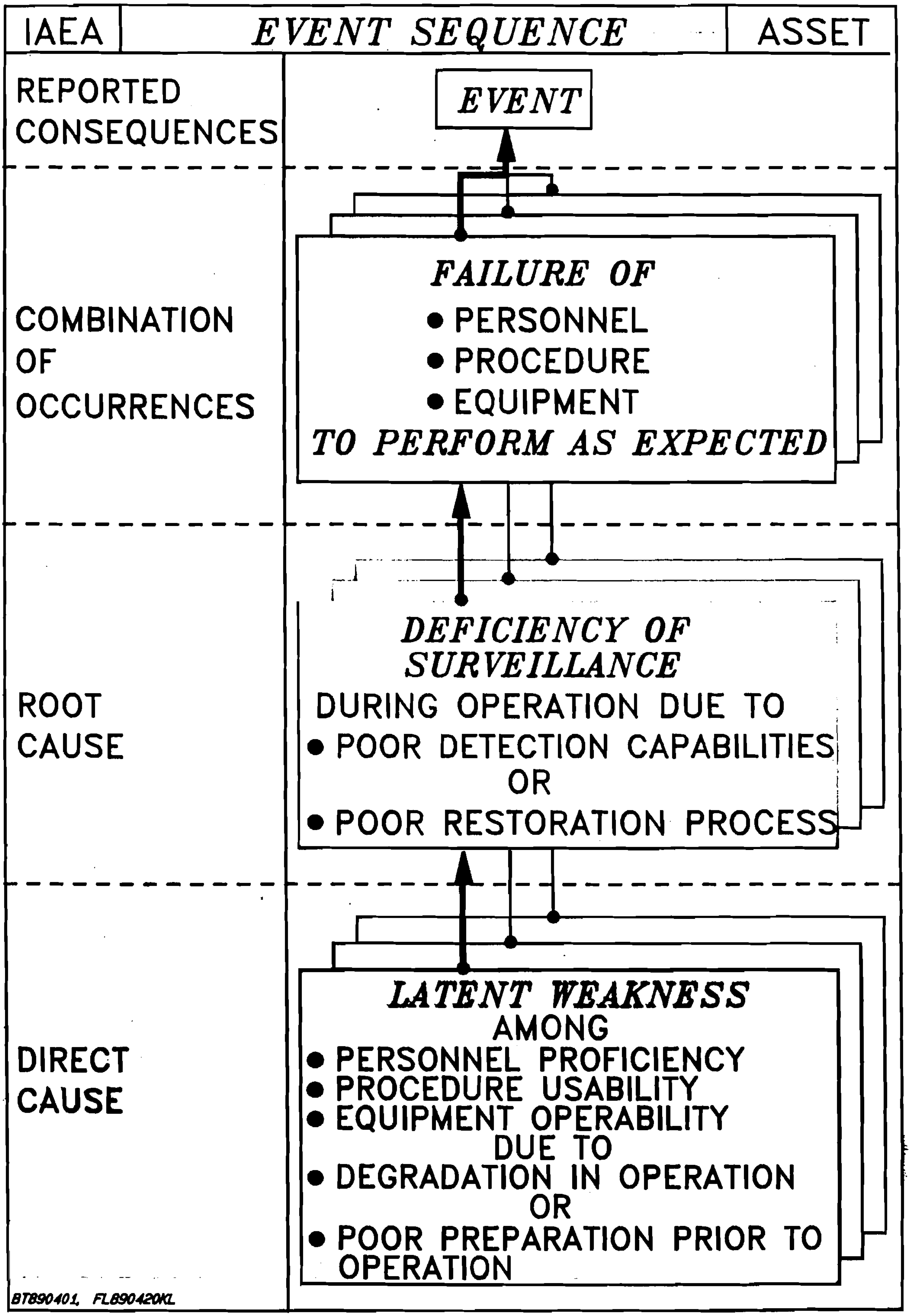
II. Design

such as risk of damage within the pressure boundary as a result of local surpression due to explosive recombination of hydrogen.

III. Operation

such as non-compliance with procedures

A specific event illustrating each of the safety issues selected is chosen for in depth root cause analysis.


IAEA
EVENT SEQUENCE
ASSET
REPORTED CONSEQUENCES
EVENT
COMBINATION OF OCCURRENCES
FAILURE OF
• PERSONNEL
• PROCEDURE
• EQUIPMENT
TO PERFORM AS EXPECTED
ROOT CAUSE
DEFICIENCY OF SURVEILLANCE
DURING OPERATION DUE TO
• POOR DETECTION CAPABILITIES
OR
• POOR RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS
AMONG
• PERSONNEL PROFICIENCY
• PROCEDURE USABILITY
• EQUIPMENT OPERABILITY
DUE TO
• DEGRADATION IN OPERATION
OR
• POOR PREPARATION PRIOR TO OPERATION
BT890401, FLB890420KL

6.4 The ASSET root cause analysis method

The events selected are analysed according to the ASSET guidelines and ASSET operating instructions, which provide both practical guidance for determining the mechanisms of events and a consistent basis for conclusive assessment.

The ASSET root cause analysis is made according to the following seven steps:

6.4.1. Description and statement of the significance of the event

How was the event detected? What were its consequences and what actions were taken? What is the actual and potential significance of the event?

Conclusions are provided on the following aspects:

* Initial status of the plant.
* How the event was detected?
* Brief description of the chronological sequence.
* Final status of the plant.
* Actual consequences of the event off-site, on-site and on defence-in-depth.
* Immediate actions taken to interrupt the event sequence and to restore safety.
* Assessment of the severity of the event on the basis of the International Nuclear Event Scale.

6.4.2 Selection of the occurrences to be analysed

What is the occurrence or the combination of occurrences most significant to safety in the sequence of the event?

This selection is made through the following process:

* Establishment of the chronological sequence of occurrences (failure of personnel, equipment, procedure to perform as expected)
* Establishment of the logic tree of occurrences
* Assessment of the safety significance of each occurrence
* Selection of the most significant occurrences for root cause analysis

6.4.3 Identification of the direct cause of each occurrence selected

What latent weakness was affecting the element (personnel, equipment or procedure) that failed to perform as expected?

This identification is carried out as follows:

* Nature of the occurrence (personnel, equipment or procedure failure)
* Identification of the latent weakness of the element that failed to perform as expected (reliability in operation, fitness to working conditions, qualification for the task)
* Identification of the contributors to existence of this latent weakness (inadequate preparation of the element prior to be used in operation or degradation during operation)
* Conclusions on effectiveness of both the plant programme for control of quality prior to operation and the plant programme for preventive maintenance during operation

6.4.4. Identification of the root cause of each occurrence selected

Why was the latent weakness (of the element that failed to perform as expected) not detected earlier by the plant surveillance (detection or restoration) programme and eliminated?

This identification is carried out as follows:

* Identification of the deficiency of the plant surveillance programme that did not eliminate the latent weakness before the event (inadequate detection programme or inadequate restoration process following detection of weakness)
* Identification of the contributors to the deficiency of the plant surveillance programme (inappropriate surveillance policy or inadequate implementation of the plant surveillance programme)
* Conclusions on effectiveness of the plant surveillance programme (detection and restoration), on plant surveillance policy and implementation of plant surveillance programme.

6.4.5 Determination of corrective actions for each occurrence selected

In what areas are improvements needed and what corrective actions are needed to enhance both the quality and the surveillance of quality for the element that failed to perform expected?

Corrective actions should address all the items involved in both the direct cause and the root cause of each occurrence as follows:

* Elimination of the actual consequences of the event
* Repair: Elimination of the latent weakness (direct cause) of the elements that failed to perform as expected

  - by restoring the level of quality of the elements that failed
  - by mitigating the contributors to the existence of the latent weakness

* Remedy: Elimination of the deficiency of the plant surveillance programme (root cause) that did not eliminate the latent weakness

  - by enhancement of the plant detection programme
  - by enhancement of the plant restoration programme
  - by mitigation of the contributors to the deficiency of the plant surveillance programme (policy and management)

* Conclusions on the appropriateness and completeness of the corrective actions implemented by the operating organization for each occurrence.

6.4.6. Generic lessons on prevention of incidents at the plant

What are the generic lessons learned for more reliable prevention of incidents?

* Conclusions are provided on the plant programme for prevention of incidents while addressing the three successive barriers (plant subprogrammes) as follows:

* Conclusions on plant quality control programme to qualify equipment, personnel and procedure prior to be used in operation.

* Conclusions on plant preventive maintenance programme to prevent degradation of quality of equipment, personnel and procedure during operation.

* Conclusions on plant surveillance programme to detect and restore any degradation of equipment operability, of personnel proficiency and of procedures adequacy during operation.

6.4.7. Suggested action plan to enhance prevention of incidents at the plant

What specific actions are suggested to enhance safe operation? What are the alternatives and what is the schedule for implementation?

This section is expected to offer a realistic action plan based on short term actions addressing the direct cause of the event (removal of latent weaknesses), medium term actions addressing the root cause of the event (improvement of the plant programme for prevention of incidents) and long term actions addressing international co-operation (improvement of operating experience feedback).

Short term actions are covering the following aspects when applicable:

* Improvement of equipment operability

  - design, manufacturing, installation
  - qualification tests prior to be used in operation
  - periodic testing during operation

* Improvement of personnel proficiency

  - recruiting criteria
  - training, retraining, licensing prior to be used in operation
  - periodic testing during operation

* Improvement of procedures adequacy

  - content and format
  - validation prior to be used in operation
  - periodic review during operation

Medium term actions are covering the following aspects when applicable:

Improvement of management of the plant programme for prevention of incidents.

* Quality control programme of the final products of plant activities directed to the achievement of the required level of the quality for equipment, personnel, procedures

* Preventive maintenance programme to keep at the level required equipment operability, personnel proficiency and procedures adequacy.

* Surveillance programme to timely detect and promptly restore any degradation of the level of quality of equipment, personnel, and procedures

* Systematic root cause analysis of all deviatons

Long term actions are covering the following aspects when applicable:

* Relationships with the nuclear community for operating experience feedback.

* Use of the IAEA services

  - Training on use of the International Nuclear Event Scale.

  - Training on root cause analysis.

Conclusions of the root cause analysis of an event can be summarized on the following form:

IAEA	EVENT ROOT CAUSE ANALYSIS FORM				ASSET
I. EVENT TITLE:					
II. OCCURRENCES SELECTED FOR ANALYSIS NATURE OF THE FAILURE	**III. DIRECT CAUSE**		**IV. ROOT CAUSE**		**V. CORRECTIVE ACTIONS**
	LATENT WEAKNESS	**CONTRIBUTOR**	**SURVEILLANCE DEFICIENCY**	**CONTRIBUTOR**	
1.	**1.**				**1.**
		2.			**2.**
			3.		**3.**
				4.	**4.**
2.	**1.**				**1.**
		2.			**2.**
			3.		**3.**
				4.	**4.**

IV. GENERIC LESSONS			
V. ACTION PLAN	**IMMEDIATE ACTIONS** **1.** **2.** **3.** **4.**	**SHORT TERM ACTIONS** **1.** **2.** **3.** **4.**	**LONG TERM ACTIONS** **1.** **2.** **3.** **4.**

ASETFORM1/90-09-24,FL/LP

VII. THE ASSET SERVICES

Since 1986 the IAEA ASSET Services have been providing operators with the opportunity to exchange on the field very valuable experience on policies for prevention of incidents at nuclear power plants, the major cornerstone for long term safe operation.

Three main options are offered to regulatory and operating organizations:

(1) Seminars on the systematic ASSET investigation methodology (5 days maximum, 3 ASSET lecturers) to familiarize staff involved with a rating tool to assess significance to safety (INES) and with a powerful analytical tool enabling an easy identification of the underlying root causes of safety issues.

Such ASSET training sessions are appropriate for recent nuclear power plants in the course of setting up an effective programme for prevention of incidents. No specific preparatory work is required from participants.

2) Review of a single safety significant incident (5 days maximum, Team of 7 experts) to prepare, on the basis of the lessons learned, recommendations to the nuclear community applicable to management of any nuclear power plants.

Such ASSET workshops are generally requested by regulatory and operating organizations of countries that consider important to share their own experience with a view to contributing to enhancement of prevention of incidents worldwide. The preparatory work required from plant operators for an ASSET workshop is restricted to providing a summary of the root cause analysis report in English.

3) Review of plant operational safety experience (10 days maximum, Team of 7 experts) to identify pending safety issues, to rate significance to safety, to identify underlying causes and to provide conclusions on adequacy of corrective actions implemented at plants in the software and hardware areas to prevent incidents in the future.

Such ASSET missions are particularly appropriate for older plants that consider important to carry out a thorough check up of plant management policy for prevention of incidents after some years of operation. The preparatory work required from plant operators for an ASSET mission is restricted to providing a list of operational issues reported since commercial operation and a copy of the regulatory body reporting criteria in English.

The IAEA does not require any fee for the experts involved in the Safety Services provided by the ASSET. The expenses related to travel and subsistence allowance of the ASSET members in connection with the work carried out are either borne by the IAEA Technical Co-operation Department in the case of developing countries or invoiced to the operation organization in the case of developed countries.

In addition to these three options, the ASSET service is also requested to carry out Implementation and Follow-Up missions.

ASSET Implementation Missions are requested to assist the operating organization in implementing the ASSET recommendations.

ASSET Follow-Up Missions are requested to assess both, progress made by plant management in implementation of the ASSET recommendations and resulting effectiveness of the plant programme for prevention of incidents.

The activities of the ASSET requested by Member States as of 15 February 1991 are shown on the attached Table.

<u>IAEA Reference Documents</u>

- ASSET Guidelines
- ASSET Practical Guidance
- The ASSET Services
- The Activities of ASSET Service
- ASSET Training Session Syllabus
- INES Leaflet
- INES User's Manual
- Event Rating Form
- Event Root Cause Analysis Form

ACTIVITIES OF THE ASSET SERVICE
1986 - 1992
REQUESTED BY MEMBER STATES
(as of 15 February 1991)

ASSET MISSIONS (M), WORKSHOPS (W), IMPLEMENTATION MISSIONS (I), FOLLOW-UP MISSIONS (F)				TRAINING SESSION ON THE ASSET INVESTIGATION METHODOLOGY	
TYPE	NPP	COUNTRY	YEAR	COUNTRY	YEAR
M	KRSKO	YUGOSLAVIA	1986		
M	ANGRA	BRAZIL	1988		
M	KARACHI	PAKISTAN	MAY 1989		
M	KARACHI	PAKISTAN	SEPT 1989		
M	IGNALINA	USSR	NOV 1989		
M	GREIFSWALD	GDR	JAN 1990		
I	GREIFSWALD	GDR	JUNE 1990	GDR	JULY. 1990
W	GRAVELINES	FRANCE	JULY 1990	HUNGARY	SEPT. 1990
M	BOHUNICE	CZECHOSLOVAKIA	OCT 1990		
M	KOZLODUY	BULGARIA	NOV 1990		
W	VANDELLOS	SPAIN	DEC 1990		
I	KARACHI	PAKISTAN (Rec. No. 3)	6-10 JAN. 1991	BELGIUM	28 JAN.-1 FEB. 1991
I	KARACHI	PAKISTAN (Rec. No. 6)	13-17 FEB. 1991	SPAIN	11-15 FEB. 1991
I	KARACHI	PAKISTAN (Rec. No. 5)	17-28 FEB. 1991	KOREA, REP. OF	25-29 MAR. 1991
M	LAGUNA VERDE	MEXICO	24 FEB. 1991	NETHERLANDS	8-11 APR. 1991
M	KOLA	USSR	APR. 1991	ARGENTINA	22-26 JULY 1991
M	NOVOVORONEZH	USSR	MAY. 1991	BULGARIA	16-20 SEPT. 1991
F	ANGRA	BRAZIL	OCT. 1991	ITALY	7-11 OCT. 1991
M	KOZLODUY	BULGARIA	4-15 NOV. 1991	SWEDEN	21-25 SEPT. 1991
M	PAKS	HUNGARY	1992	USSR	1992
				CSFR	1992
				CHINA	1992

IAEA contact point:
Mr. B. Thomas
P.O. Box 100
A-1400 Vienna, Austria
Tel: 1-2360 2685
Fax: 1-234564

INFLUENCE OF ORGANIZATION AND MANAGEMENT ON INDUSTRIAL SAFETY

B. Wahlström[1], E. Swaton[2]

Abstract. An analysis of accidents and performance of industrial plants demonstrates the importance of adequate management. Management sciences have provided many insights in the management of business corporations. Less attention has been given to the influence of organization and management on the safety of potentially hazardous industrial installations. The paper is discussing safety oriented organizations and their requirements on management practices. It is argued that organizational deficiencies can provide major safety threats by making human errors more likely. A continued safety and good performance of a plant will rely on an early detection and correction of such deficiencies. Organizational safety reviews are proposed as an approach for detecting and correcting organizational deficiencies. Present frameworks of organizational reliability are however still based more on intuition and common sense than on theoretical models. The paper concludes by arguing for more research in how organizational factors influence industrial safety.

INTRODUCTION

The interest in organization and management as providing preventive insights to industrial safety is relatively recent.[1 2 3 4] The connection has certainly been recognized earlier, [5 6] but comparatively little has been written in the field before the late eighties. The TMI, Bhopal, Challenger and Chernobyl accidents revealed however that human errors together with deficiencies in organization and management can provide major threats to the safety of technological systems.[7]

The importance of organization and management has manifested itself not only in the accidents but also in the operational performance of the plants. Comparative studies on nuclear power plant performance have conclusively shown that their performance is depending on how they are managed. These findings are actually not surprising, but it is perhaps more astonishing that to date only a few systematic attempts have addressed these issues.

Human factors research in the nuclear power field took off as a major activity in the aftermath of TMI and has been oriented towards control room design, operational procedures and operator training. The Chernobyl accident brought violations as a third category to earlier discussed human error categories of slips and mistakes.[8] There is an emerging consensus that organization and management can make human errors more likely. Proper responses to issues of organization and management is one of the remaining challenges in the human factors research.

The management sciences could provide guidance also in how safety oriented organizations should be managed, but they have mainly been oriented towards problems in the business world. The management of potentially hazardous industrial installations is today relying more on managerial intuition than on a theory of organizational reliability. A careful housekeeping is certainly one of the components behind a safe plant, but the question is to what extent such prescriptions can be generalized and made more concrete. The management has control over some of the factors behind a good performance, but others are determined by plant design and the industrial environment.

[1] International Institute for Applied Systems Analysis, A-2361 Laxenburg, Austria.

[2] International Atomic Energy Agency, P.O.Box 100, A-1400 Vienna, Austria.

MANAGING A POTENTIALLY HAZARDOUS PLANT

Managing any large installation involves a multitude of different roles and tasks. Managers are defining tasks and responsibilities for subordinates, they are supervising how the tasks are executed, they are maintaining contacts to other organizations, they are formulating strategies as a part of the planning procedures, etc. The influence of good management can be seen as a smooth operation at all levels. Managing a potentially hazardous plant is a typical managerial task, but the requirements of the technology gives it a distinct flavor.

A modern chemical or nuclear plant can have large amounts of toxic and highly reactive substances confined in the processes presenting potential threats to human health and the environment. A large plant is a very complex piece of equipment, which requires experts skill in many different fields. Day-to-day operation requires accuracy and good quality control. Disturbed operation can require delicate judgment and is usually extremely stressful for the organization.[9]

The initial design of a plant sets the baseline of its safety. The way it is operated will however influence its safety. Wear in components and systems is depending on operational strategies and have to be compensated by preventive maintenance. Selection and training of personnel is like the maintaining of plant documentation- a continuing effort. A large plant will also typically require modifications, because actual demands are seen only when the plant is in operation. The management of changes becomes therefore an important task with safety implications.

The performance of a potentially hazardous plant is a combination of safety and economy. Safety is however hard to quantify, which means that operational performance can be difficult to define and measure. There can also be different interpretations of good performance even within the same organization. It is not likely that a single measure describing performance can be found. Instead it is necessary to assemble some suitable set of performance indicators.

Industries with a potential for hazards are regulated with the intent of ensuring an acceptable safety for the society. The regulation is typically written as a set of licensing requirements to which the industry has to comply before permits to plan, construct and operate the plant are granted. The regulation is also requiring regular inspections and different analyses to be performed when the operational permits are renewed. Managing the safety of a potentially hazardous plant can be seen as a control system with several feedback loops and participating organizations.[10] There are many similarities but also differences between regulations in different countries. Reasons for the differences are contained in the legal system, in social values and in traditions rather than technical.[11]

The management of safety within the industry is not restricted to the plants only. It is necessary also to consider the environment in which a plant is operating. This means a consideration of the company structure and the framework of national legislation. The interactions with plant or system vendors can also prove crucial in unexpected situations. The societal infra-structures such as communication systems and institutions for education and training are also important for a continuing safety at the plants. In the safety considerations it is necessary to understand that each of the interacting organizations have their own goals and accountability.

LESSONS FROM ACCIDENTS

An accident will seldom be the cause of some single event. Instead there are many events interacting in a complex web of contributing technical, human and organizational causes. An analysis of the causes for an accident has therefore to follow a multiple path, where the underlying causes are searched for on each level. The accidents should actually be analyzed in a multiple framework of technical, organizational and personnel perspectives.[12] [13] Sometimes it is actually necessary to expand this analysis beyond the plant and the company operating it, to the regulatory system and the governmental decision-making processes.

Five particular management problems have been identified as contributors to human errors.[14] These are

(1) time pressures, (2) observation of warnings of deterioration and signals of malfunction, (3) design of an incentive system to handle the tradeoffs between safety and productivity, (4) learning in a changing environment and (5) communication and processing of uncertainties.

Any thorough analysis of accidents reveals several layers of problems relating to design, manufacturing, construction, maintenance, quality control, safety management, communication, training, etc. The work routines can be identified as a generic cause for these problems, because the necessary quality of work has at times not been achieved. The management is naturally responsible for such slips in performance, but simply laying the blame on management is not constructive, because it will not give suggestions for improvements. A more productive approach is to identify generic problems, propose how they could be solved and outline good management practices in principle.

Analysis of accidents point generic categories of organizational deficiencies. An incomplete identification of goals and priorities can cause problems both in the design and in the operation. An unsatisfactory definition and distribution of tasks within the organization can introduce many opportunities for later problems. An impaired feedback of experience can leave even serious deficiencies uncorrected. Inefficient safety management can render risk assessments and procedures for quality assurance practically useless.

COMPARATIVE STUDIES OF NPP PERFORMANCE

The performance of nuclear power plants in the world varies. Some plants regularly achieve a power availability in the region of 85% and other plants have difficulties even to reach the world average of about 70%. A careful housekeeping of a large number of different ingredients seems to be one of the components contributing to good performance. Some of those ingredients can be influenced by management and others cannot.[15]

A set of studies have tried to identify how organizational characteristics are related to different performance measures.[16] [17] The finding indicates different correlations between organizational design parameters and safety indicators. A more recent report[18] stresses that efficiency, compliance and innovation should be the outcome of a better understanding between safety and organizational factors.

A comparison of nuclear power plant performance is usually based on annual load factors. A study comparing performance in France, Germany, Japan, Sweden, Switzerland and USA concluded that a strong focus on on-site operations, planning, and maintenance is important for achieving high performance.[19] A systematic effort at training and learning from the past is also needed. Their data illustrate that it is possible to create industry-wide programs that can lead to substantial improvements. The report speculates also on reasons for the inadequate performance of nuclear power in the United States and claims that the industry has not succeeded in learning from experience.

Another comparative study of eight well-performing nuclear power stations with a total of 22 operating units shows that similar patterns emerge.[20] The following factors are identified as important:

- Goals are well defined and communicated to the staff. Progress in achieving goals is monitored. Improvements are identified, prioritized, and implemented.

- The organization is well defined. Responsibilities, levels of authority, and individual accountability are defined. Teamwork is supported.

- Managers and supervisors interact with staff members and are involved in plant activities. Relevant experience is sought and used to improve performance.

- Quality assurance principles are applied. Operations and maintenance work are controlled and executed in a disciplined manner.

- Staff proficiency is established and maintained. Effective working relationships with outside organizations are established.

CONCEPTS FROM MANAGEMENT SCIENCES

The management sciences have been oriented towards the needs in the business world. Different schools of thinking have been emerging and the theories have been anchored in many diverse fields such as operations research, psychology, sociology and political sciences. The theories have created typologies and models aiming at providing a better understanding of the complex interactions which can be observed in real organizations.[21] The goals for business organizations are different from those of a safety oriented organization, but it can still be expected that the concepts developed are applicable in general.[22]

Designing an organization for a specific purpose involves several different tasks such as (1) deciding on an organizational structure, (2) defining positions, (3) building the executive systems, and (4) specifying the information systems. Organizational design involves many different parameters such as the span of control for the managers, the size of the organizational units, the number of hierarchical levels, the degree of formalization of the tasks, etc. The control of an organization is exercised at each hierarchical level through the tasks of (1) objective setting, (2) strategy formulation, (3) generation of predictions (feedforward control), (4) providing feedback (5) coordination, and (6) allocation of resources.[23]

The performance of an organization is usually assessed as a continuing effort to make it possible for the organization to improve and to adapt to changes in its environment. This function is often implemented as a part of the strategic planning process, in which strengths and weaknesses of the organization are identified to provide the basis for setting a target state and define the strategy of getting there. The performance is immediately measurable for some organizations, but has often to be assessed using qualitative indicators.

Organizational effectiveness is a concept closely related to performance, but is in addition also considering the available resources. Effectiveness has attracted a good deal of attention within the management sciences, and popular books, which have become bestsellers, have been written on the subject.[24] In spite of a considerable amount of work in the area of organizational effectiveness there is still no generally accepted theory available.[25] There is however an agreement that the management can make a difference and that good management and effective organizations are correlated. It appears however that effective organizations are able to handle seemingly contradicting attributes (cf. Table 1).[26]

If the effectiveness of an organization is declining as compared to its competitors it will ultimately die. A large interest in the reasons for such decline arose in the early eighties when the business failures in USA increased rather significantly.[27] In this context it would be interesting to know what is causing organizational decline and what kind of responses should be initiated. A rough division of the causes for organizational decline separates between internal and external causes, where the external causes often are connected to changes in the environment of the organization.[28]

Leadership involvement is a critical element in ensuring safe and reliable operational performance for safety oriented organizations.[29] Still it is not clear to what extent visions and charisma will be needed in the same way as in a rapidly changing business organization. Authority and a recognized

Loose - Tight coupling.

High specialization - Generality of roles.

Continuity of leadership - Infusion of new leaders.

Deviation amplified - Reduction processes.

Expanded search of information - Avoidance of information overload.

Disengagement and disidentification with past strategies - Reintegration and reinforcement of roots.

Table 1. Contradictory attributes of an efficient organization.

technical background seems to be more important in providing the necessary stability of high reliability organizations. The incentive systems of business organizations have been receiving a considerable attention. To what extent different kinds of incentives can be used in high reliability organizations is still to be investigated.

An organizational theory has to approach the relationships and the interactions between the formal and the informal organizations. The formal part of the organization is defined in organizational schemes, internal procedures and job descriptions. The informal part, which reflects on how things are handled in reality, has also to be addressed systematically. There are many dangers in allowing the informal organization to depart too far from the formal organization, but there is also a danger in requiring a strict adherence to inflexible routines.

PRESCRIPTIONS FOR SAFETY ORIENTED ORGANIZATIONS

The design of safety oriented organizations has not been addressed explicitly from a theoretical point of view. Practical guidance for a country entering a nuclear power program can however be found.[30] Similar guidance for maintaining the qualification and competence of the operations personnel at a nuclear power plant is also available.[31] The general safety principles for the whole nuclear industry in general have also been addressed.[32] There is an indication that the number of organizational levels correlates negatively with common safety indicators.[33] A comparison of actual practices in different countries reveals considerable differences both in the span of control for a plant manager and for the depth of the organization.

An important part of the organizational design is the allocation of tasks into specified positions. In the operation of an industrial plant certain well defined functions have to be maintained and they will also be reflected in the organizational structure. The corresponding positions will usually be implemented in a relatively straightforward way, based on more or less formal job and task analyses. The more implicit tasks of planning, quality control, feedback of experience, etc. are not equally well defined. There might also be areas in the borderlines between different positions and different organizational units causing confusions. A special requirement is the provision of organizational redundancies for the case of emergencies.

Efficient organizations are highly adaptive, but in high reliability organizations a certain stability has to be ensured. The stability is needed both for the planning and the execution of tasks, because a good predictability is mandatory for assessing implications on safety. A certain compensatory behavior over organizational borderlines can be observed, where a less satisfactory performance in one unit can be compensated by a higher performance in another. The allocation of tasks between positions and organizational units would ideally proceed in a top-down manner, but this will seldom occur in practice. Multiple iterative cycles, which are combining top-down planning with bottom-up implementation are more common and actually more useful. The actual division of responsibilities in an organization is therefore the outcome of partly systematic planning and partly a historical development process.

Operational performance of an industrial plant is relatively easy to assess, but an assessment of its safety is far more difficult. In pursuing plant effectiveness it is also relatively easy to forget long term goals in the pursue of short and intermediate term goals. Well-defined performance indicators can supply valuable information and can also be helpful in directing the attention to proper control. Performance indicators can provide a framework for comparing plants and organizational structures to support the exchange of operational experience and managerial practices. Ideal characteristics of a set of performance indicators have been developed (Table 2).[34] The performance indicators should, in addition to the straightforward performance related measures, also reflect more subtle factors such as resource management, employee satisfaction, and public relations, which can only be expressed in qualitative terms.

Planning and analysis are two important components in the execution of any task within a safety oriented organization. In the planning a proper balance between general lines and small details has to be found. Strategic planning can in this context be seen as an important component, although not directed explicitly towards management of change. By carrying out the strategic planning as an exercise involving several organizational levels and units, it can in addition to its primary output also provide an important training function in rehearsing the relationships between means and ends in the organization. The strategic planning provides also a suitable forum for a comparison of actual performance with the targets set and with other similar organizations.

A balanced level of safety over the whole operational life of a plant needs to be achieved in spite of personnel turn over, new regulatory requirements, aging of the plant, etc. Maintaining the operational quality of the organization over the complete life cycle of the plant implies also one or more turns of generations in personnel. Regularly executed organizational reviews can provide means for maintaining vigilance both of individuals and the organization as a whole.

The management can in a way be seen as the control system for the organization reacting on feedback signals and providing the control actions. With this metaphor it is easy to understand why an impaired feedback of actual performance and experienced problems can be dangerous for safety. The planning and analyzing can in this context be seen as providing feed-forward control, where a prediction of future performance is used to select present control actions. The pursue of a higher effectiveness operates like an adaptation mechanism, where control parameters continuously are adjusted for a better performance. A problem with safety oriented organizations is that a very high performance tends to leave little for that adaptation mechanism to work on, which may lead to an adaption to unacceptable goals due to a low signal to noise ratio.

Close relationships to risks and/or safety,

Data readily available,

Quantitative (show range of performance),

Unambiguous,

Unlikely to cause undesirable actions,

Significance should be understood (objective and fair),

Industry wide applicability,

Not susceptible to manipulation,

Physical results,

Independent indicators essential,

Manageable set,

Worthy goal.

Table 2. Ideal characteristics of a set of performance indicators.

The large amount of stability and routine poses the problem of maintaining vigilance over time for all tasks. When a routine becomes boring it is likely that shortcuts will be taken. A continuing safety relies on alertness, where deficiencies are actively sought and corrected. Sometimes it can be necessary to react quickly, which means that procedures for obtaining authorization for specific actions should be simple. This could be reached by a proper delegation of authority and keeping organizational lines of authorization short.

The need to coordinate all activities on the plants have led to the adoption of a formalized work order system, where each activity should be approved by specific persons before they are allowed to proceed to the next planning step or to be executed. This system is sometimes considered to be a burden at the plants. However one of the main tasks of management is to make staff aware of the importance of certain administrative requirements.

The feedback of operational experience is one of the most important functions in improving and maintaining safety. Incidents from the own plant and from other similar plants should be thoroughly analyzed for collecting the lessons to be learned. The results of the analysis should then be innovatively used in order to detect possible safety threats of similar kinds. One scheme of analysis taking into account the multiple perspective of the technical, the human and the organizational systems is suggested in Appendix 1.

A good baseline of performance gives an opportunity to fine-tune the routines and therefore make an improved safety possible. It can therefore be argued that earlier success should make future success more likely. On the other hand there is also the possibility that earlier success makes the organization overconfident with a resulting degradation of future performance.[35] Failures can also make additional failures to appear more probable, when they are indicating that over-optimistic safety estimates have been used. An organizational reliability curve of Figure 1 can actually by hypothesized, where two different mechanisms of errors are interacting.

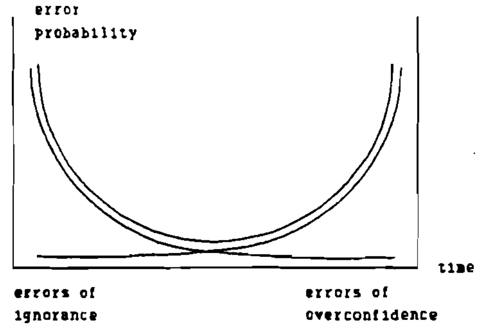


Figure 1. Errors of ignorance can be substituted by errors of overconfidence resulting in a bathtub curve of organizational reliability.

In approaching the intersection between safety and organization a common prescription is to support a safety culture.[36] There are however many views on the content of such a concept. Even the use of the word culture contains the inherent assumption that the concept cannot be defined accurately. One part of the concept implies that people should care and take responsibility. Everybody should thus react on and report unsafe practices. There is, however, a cultural bias toward reporting, which could be demonstrated by a reluctance to get involved in another's business or to squeal on a colleague.

A difficult question is connected to honesty in the communication to the outside. Organizational performance relies on team-work with an implicit division into we and they. Here is a danger that the organization is closing itself to the outside, where even cover up actions are carried out for the protection of the establishment. A very open communication is certainly not appropriate for a safety oriented organization, because it could endanger some of the crucial safety precautions and it could also unnecessarily make individuals vulnerable to unfair attacks from the outside. Completely closed channels of communication are also less desirable, because important feedback channels and lines of accountability would in this case be cut. There seems to be a need for a continuous probing and reformulation of means and ends, which cannot be given up if the organization should remain healthy.

ORGANIZATIONAL REVIEWS

Recognizing the importance of organizational and management issues it would be desirable to develop methods that can detect and correct organizational deficiencies before an incident occurs. The use of organizational safety reviews could provide one approach for detecting weak signals of a deteriorated safety. It might be difficult for an organization to improve from the inside, but it is also difficult to initiate the correcting actions from the outside. Here is actually a CATCH-22 situation, because an initiative from the inside of the organization can be considered as a proof of healthiness, whereby an initiative coming from the outside is likely to be rejected by an unhealthy organization. It is evident that all practical means to detect and correct organizational deficiencies require both diplomacy and knowledge.

One procedure for carrying out organizational safety reviews was developed as a part of the Nordic research program in nuclear safety.[37] The procedure was based on a structured interview carried out with a guide providing a model of a successful organization. The procedure was tested on three cases in Sweden, and a follow-up study has been carried out in Finland.[38] Experience indicates that such an exercise could be valuable as an instrument for internal safety reviews.

The OSART review procedure, developed and carried out by the IAEA, is another example of reviews that includes organizational issues in an assessment of safety.[39] Results from the reviews show that not all nuclear power plants have taken the necessary structured approach to safety.[40] Among the comments were that workers do not always follow established guidelines and that managers and supervisors should involve themselves more in plant operation. Each plant practiced some good safety measures, but even the best-performing plants had areas for improvements. In most cases the deficiencies were known, but had not been resolved effectively before the OSART mission. The missions seem in general to have provided a valuable exchange of technical information, concrete recommendations for improvements and many informal occasions to exchange operational experience.

A third framework intended for the review of emergency preparedness has been developed.[41] This review is also touching on several organizational issues.

Identifying and correcting organizational deficiencies can be difficult, because social institutions are not necessarily receptive to outside critique.[42] It is also difficult to create reliable and valid methods for measuring psychological and sociological variables. It is necessary to build confidence in the fairness and intent of the review. One possibility is to carry out organizational reviews as internal exercises. It is, however, easy to be unaware of immediate problems, and it can therefore be valuable to involve outsiders in the review. An outsider may also find it easier to discuss sensitive matters with individuals at different levels in the organization.

An early commitment of management has to be obtained before any review can be effective. Carrying out the study as a training exercise connected either to strategic planning or to the analyzing of an incident can provide the justifications. It is also then possible to collect ideas for responses to the deficiencies. It is also possible to initiate a horizontal exchange of information between adjacent organizational units or to exercise a vertical training effort of transferring and interpreting goals that involves two or more levels in the organization.

A structured interview seems to be suitable in the light of available experience. The review should concentrate more on improvements and exchange of good operational practices than on details of past performance. A general structure for an organizational review is proposed in Appendix 2. It is also proposed that the interview should be carried out as an internal exercise, but with an outside moderator. If the moderator has personal experience from other plants, he could cross-fertilize the discussion by bringing up examples from other plant milieus. By combining the review either to the strategic planning process or to the analyzing of some incident it should be possible to avoid dead-locks caused by a lacking grass-root realism or undiplomatic moves.

CONCLUSIONS AND LESSONS FOR THE FUTURE

There have been problems in bringing the psychological aspects of human factors research into the engineering process of design and construction. The additional need to understand groups of humans does not make this task easier. In the search for quantifiable performance indicators it is not expected that any set of objective measurements of organizational effectiveness can provide the answer. The assessment of organizational performance has therefore to be based on expert judgment. This brings up the question how such experts could be selected and trained. If an organizational theory could be developed for the safety oriented organizations it might be possible to remove some of the arbitrariness from this kind of judgment.

It is not likely that any single optimal solution will be found, because it is always necessary to adapt to cultural norms, available educational systems, technical infrastructures, etc. There seems also to be feedback mechanisms producing dynamics within the social systems, where good performance provides opportunities for further improvements, but bad performance can lead to a downward spiral of decline (cf. Figure 2).

People and organizations need signals to react on. The accidents and incidents can be seen as such signals necessary for detecting safety threats. The accidents of TMI, Bhopal, Challenger and Chernobyl have initiated intense periods of organizational learning. The argument that the accidents have been more expensive than the benefits of the lessons learned [43] is still relevant, because most of the findings from the accidents were actually available before, but not seriously considered.

There is a dilemma of high reliability organizations that continued high performance does not provide the immediate feedback on the safety level achieved. This may give a false impression that it still is possible to squeeze a higher efficiency out of the organization without obstructing safety. The increasing hurry among high-level managers and executives provides one example of stretching of resources, because individual and organizational attention is a scarce resource.[44] The search for an ever increasing effectiveness might be a generic symptom for a structural change in the contemporary society, but for the potentially hazardous industrial installations it can prove dangerous. Only a continuing assessment of how all small components are contributing to safety can provide the necessary signals for increasing dangers.

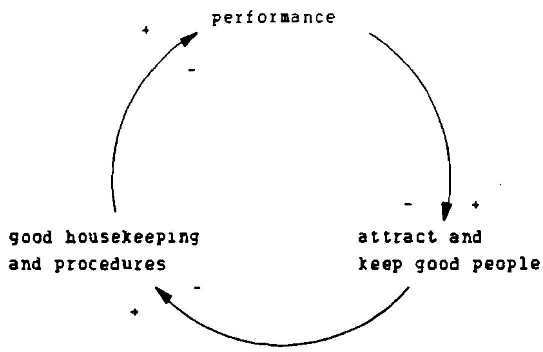


Figure 2. Improved performance can lead to still better performance and vice versa.

In hindsight it is always easy to identify a better decision. It is far more difficult to detect and correct deficiencies before they have been made obvious by an accident. There seems also to be a problem in bringing available knowledge into practice. The research in human errors has been very intensive since the TMI accident[45] and just scanning what is available, it seems that enough guidance has been produced. It seems however difficult to apply the results for the concrete day-to-day routines in the safety oriented organizations. The diffusion of new knowledge will always take time, but one may ask if this diffusion is efficient enough or if additional ideas and resources will be needed for the intake and digestion of new findings.

The discussion has been directed to the safety oriented organizations as a whole, but one specific question is how the managers of these organizations should be selected and trained. How could the feedback of experience be supported by national and international institutions and how should these be managed. What kind of systems could be built to promote the transfer of good operational practices. What kind of regular organizational reviews should be carried out and how should the issues relating to organization and management be regulated. These questions will not have any simple answers, but it can be expected that international organizations such as the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO) in the area of nuclear applications could be instrumental in coordinating research and harmonizing practices.

The safety of any industrial installation is ultimately societal concern. In spite of the diminishing dimensions of the world there are still large differences in the views on an acceptable level of safety. It is also necessary to understand that investments in the safety of one technology may decrease similar investments in another. The balancing of resources has on this level to be treated in the national and international policy making processes. In creating an environment, where it is possible for high reliability organizations to carry out their tasks credibility and confidence in the institutions has to be built. Otherwise societal hostility can influence the long-term effect on safety by feedback mechanisms in the society.

Very basic conceptions of responsibilities, work and people, which are anchored in the culture can also have an important influence on the operation of a safety oriented organization. It may even be hypothesized that high reliability organizations would be easier to operate in certain societies. If this is true it could lead to changed views on international cooperation and development assistance. The concentration of all potentially hazardous installations to only a few areas in the world might however not be possible due to the problems of transporting the products.

There is a need for a better understanding of how organizational factors affect safety. Theories developed should be able to provide a tangible improvement as compared to managerial intuition. It would actually be necessary to take a step beyond anecdotes and personal experience in order to arrive at usable prescriptions for safety oriented organizations. Any research in the intersection between safety and organization has to be multi-disciplinary with close contacts to operational plants. A high level support from the regulators and from the industry seems to be necessary to initiate such work. In applying such theoretical work it is still necessary to rely on the insight and skills of the managers and the workers within the industrial community. Management involvement and workers' commitment will also be important components in achieving the functions necessary for safety [46].

APPENDIX 1.

A SCHEME FOR ANALYZING EVENTS, INCIDENTS AND ACCIDENTS.

There is a common understanding that events, incidents and accidents have to be analyzed in a large degree of detail to provide the lessons to be learned. In the analysis process generic models of cause and consequence relationships have to be combined with an understanding of the situational characteristics to yield the generic lessons. These lessons could then in an effort of synthesis be combined with information in the PRA to propose possible chains of events that could pose threats towards the safety. These threats could be reacted on by specific improvements in the plant construction or in the procedures applied. The analysis is usually understood to proceed towards the identification of a "root cause" ie. a place where it is possible to break the sequence of events by an improvement of the system. In this context it is understood that multiple root causes might be identified. In the identification of root causes it is necessary to take a step beyond the simple explanations behind the primary causes and search for secondary, tertiary, etc. causes. In this search the stopping criterion is rather pragmatic, because the identification of a place where an improvement would make the sequence impossible is not well defined. The synthesis effort where the ultimate consequences of a specific event chain is also governed by a similar pragmatic stopping criterion.

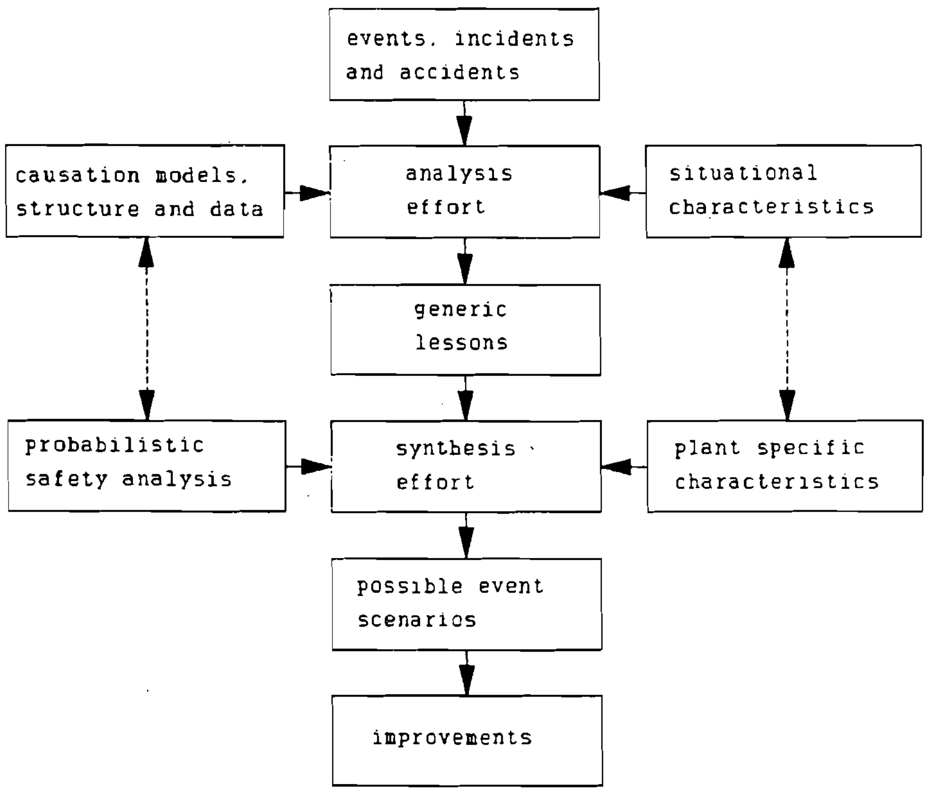


Figure 3. Analyzing events, incidents and accidents in the context of plant improvements.

The causes could on the most general level be divided into technical failures and human errors. A further consideration of different classes of technical failures however often points to human errors as a secondary cause. A consideration of causes for human errors is in the same way proposing organizational deficiencies as tertiary causes to the observed failure. Proceeding with the analysis through the diagram three classes of generic causes for accidents are proposed. If the potential dangers of the sequence in consideration have not been recognized before the incident we may speak about new experience which has been obtained. If the dangers have been identified, but not accounted for then available knowledge has not been utilized properly. If the danger of the sequence has been understood and properly reflected in the risk assessments carried out it may be necessary to attribute the sequence to bad luck in a conscious gambling situation

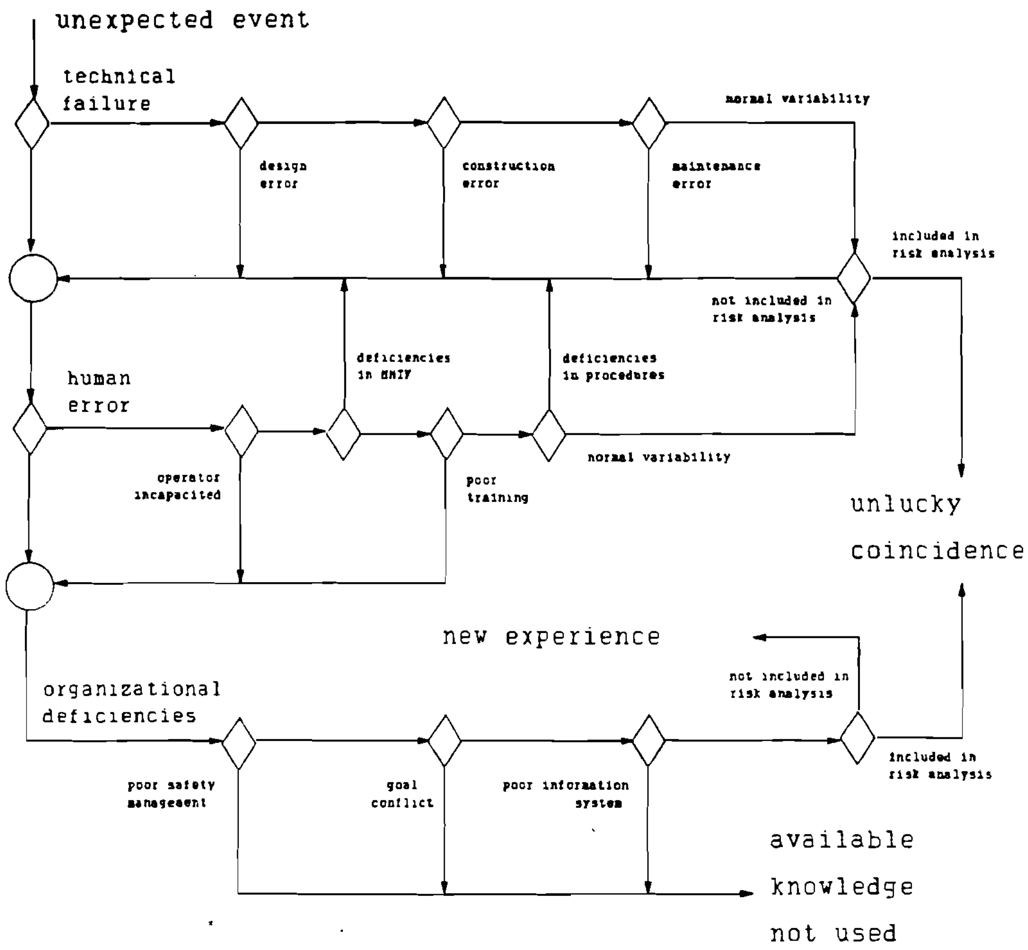


Figure 4. An analyzing scheme for unexpected events which is taking into account the multiple layers of causal factors behind an observed failure or error.

APPENDIX 2.

A TENTATIVE CHECKLIST FOR ORGANIZATIONAL REVIEWS

GOAL FORMULATION.

Performance targets. Organizational policies. Principles of setting performance targets. Performance in comparison with other similar organizations. Systems for monitoring performance. Definition of performance targets for organizational units.

Priorities. Selection of priorities between different goals (eg. safety, economy). The price of safety.

Goal conflicts. Procedures for detecting and settling goal conflicts. Conflicts between members of the organization.

The safe operational envelope. A definition of the safe operational envelope. Safety technical specifications.

TASK DEFINITION.

Task structure. Hierarchical layers in the organization. Rigidity of the hierarchical organization. The division of task between different organizational units. Informal organizational structures.

Responsibilities. The division of responsibilities between different units and different levels in the organization.

Task characteristics. Shift schedules. Task demands and stressfulness. Normal operation compared to refueling operations.

Exchange of information. Procedures for distributing information. Management of information overload.

Operating procedures. Instructions and operational procedures. Verification of the procedures. Updating of the procedures.

Changes in task structure. Examples of, reasons for and experience of organizational changes.

FEEDBACK OF EXPERIENCE.

Reporting. Systems (formal/informal) for reporting of incidents. Cases of unreported events. Responsibility for reporting. Company policy towards reporting.

Analyzing. Principles for analyzing incidents. Identification of root causes.

Improvements. Actions generated from incident reports. Systems for handling the reports.

Utilization of international experience. Procedures for utilizing event reports from other plants. Contacts to staff from other similar plants.

SAFETY ANALYSIS AND QUALITY ASSURANCE.

Safety analysis. Plans for carrying out a probabilistic safety analysis (PSA). The utilization of the results from the PSA. The concept of a living PSA.

Quality control. Internal principles for quality control. Quality control for contracts and sub-deliveries.

Inspection. Inspection of critical components. Contacts with the regulatory body.

Audits. Internal safety audits. External safety reviews.

Informal work practices. Measures for the identification and correction of work practices not in accordance with task definitions.

MAINTAINING KNOWLEDGE AND SUPPORT.

Organizational change. Transfer from the pioneer to the continuous operation. Mechanisms for responding to ambitions in the organization. Principles for promotion.

New staff. Turn over of personnel (too large/too small). Number and level of applicants for new positions. The use of internal recruiting.

Training. Principles of training. Emphasis on understanding in the training. Use of training simulators. Use of training tools. Training for team work. Execution of drills for emergency responses. Follow up on the development of trainees.

Outside support. Maintaining channels to outside support. Contacts to vendors. Plant user organizations.

Fostering a safety culture. Management commitment to safety. Moving around in the plant. A grass-root understanding of the dangers involved in operation.

REFERENCES

1. David A. Ward (1988), Will the LOCA mind-set be overcome? Proceedings of the IEEE Fourth Conference on Human Factors and Power Plants, Monterey, Ca, June 5-9, pp.37-39.

2. HFRG (1988), Proposal to prepare a short guide entitled "Guide to reducing management error which may lead to a major accident, UK Human Factors Reliability Group, Internal discussion document, 7 March.

3. Greenhalgh, G. (1990), Focus shifts to organizational issues, Nuclear Engineering International, March.

4. OECD/NEA/CSNI (1989), Minutes of the Principal Working Group #1 meeting, 25-27 September, Paris SEN/SIN(89)49.

5. William G. Johnson (1975), MORT: The management oversight and risk tree, pp.4-15, Journal of Safety Research, Vol.7, No.1, March.

6. Perrow, C. (1984), Normal accidents. Living with high-risk technologies, Basic Books, New York.

7. Zebroski, E. (1989), Sources of common cause failures in decision making involved in man-made catastrophes, pp.443-453 in "Advances in risk analysis, Plenum Publishing Company.

8. D.A. Norman (1981), Categorization of action slips, Psychological Review, Vol.88, pp.1-15.

9. Mitroff, I., Pauchant, T., Shrivastava, P. (1988), The structure of man made organizational crises: Conceptual and empirical issues in the development of a general theory of crisis management, Technological Forecasting and Social Change, 33, pp.83-107.

10. Wahlström B., Laakso K., Lehtinen E. (1988), Feedback of experience for avoiding the low-probability disaster, IAEA International Symposium on the feedback of operational experience from nuclear power plants, IAEA-SM-302/23, Paris, 16-20.5.

11. Jasanoff, S. (1988), Judicial gatekeeping in the management of hazardous technologies, Journal of Management Studies 25:4 July, pp.353-371.

12. Bowonder, B., Linstone, H.A. (1987), Notes on the Bhopal accident: Risk analysis and multiple perspectives, Technological Forecasting and Social Change 32, pp.183-202.

13. Harold A. Linstone (1990), Multiple perspectives on the Alaska oil spill, Portland State University, Portland, OR, April.

14. M. Elisabeth Pate-Cornell (1990), Organizational aspects of engineering system safety: The case of offshore platforms, Science, Vol.250, 30 November, pp.1210-1217.

15. Palmgren, A. (1986), Experience of plant performance and methods of improving performance including refuelling, ENC'86 Conference Geneva, 1-6.6.1986.

16. Osborn, R.N., Olson, J., Sommers, P.N., McLaughlin, S.D., Jackson, M.S., Scott, W.G., Connor, P.E. (1983), Organizational analysis and safety for utilities with nuclear power plants, NUREG/CR-3215, US Nuclear Regulatory Commission.

17. Olson, J., Osborn, R.N., Thurber, J.A., Sommers, P.E., Jackson, D.H. (1985), An empirical analysis of selected nuclear power plants maintenance factors and plant safety, NUREG/CR-4281, US Nuclear Regulatory Commission.

18. A.A. Marcus, M.I. Nichols, P. Bromiley, J. Olson, R.N. Osborn, W. Scott, P. Pelto, J. Thurber (1990), Organization and safety in nuclear power plants, US Nuclear Regulatory Commission, NUREG/CR-5437.

19. Beckjord, E., Golay, M., Gytopoulos, E., Hansen, K., Lester, R., Winje, D. (1987), International comparison of LWR performance, MIT Energy Laboratory Report, MIT-EL 87-004, Cambridge, MA, February.

20. IAEA (1989), Good practices for improved nuclear power plant performance, International Atomic Energy Agency, IAEA-TECDOC-498, Vienna.

21. Henry Mintzberg (1979), The structuring of organizations, Prentice Hall Inc., Englewood Cliffs, NJ.

22. Sonja B. Haber, John N. O'Brien, Thomas G. Ryan (1988), Model development for the determination of the influence of management on plant risk, pp.349-352 in proceedings from the IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA, June 5-9.

23. M. Joseph Sirgy (1989), Toward a theory of social organization: A systems approach, Behavioral Science, Vol.34, No.4, October, pp.272-285.

24. Peters, T., Waterman, R. (1984), In search of excellence, Harper&Row, New York.

25. Arie Y. Lewin, John W. Minton (1986) , Determining organizational effectiveness: Another look, and an agenda for research, Management Science, Vol.32, No.5, May, pp.514-538.

26. Cameron, K. (1986), Effectiveness paradox: Consensus and conflicts in conception of organizational effectiveness, pp.539-553, Management Science, Vol.32, No.5, May.

27. Kim S. Cameron, Robert I. Sutton, David A. Whetten eds. (1988), Readings in organizational decline, Ballinger Publishing Company, Cambridge, MA.

28. Bill McKelvey (1988), Organizational decline from the population perspective, in Cameron et al (1988).

29. Lando W. Zech, Jr. (1988), Remarks (pp.40-42) at the IEEE Fourth Conference on Human Factors and Power Plants, Monterey, Ca, June 5-9.

30. IAEA (1980), Manpower development for nuclear power: A guidebook, International Atomic Energy Agency, Technical Report Series No. 200, Vienna.

31. IAEA (1989), Guidebook on training to establish and maintain the qualification and competence of nuclear power plant operations personnel, International Atomic Energy Agency, IAEA-TECDOC-525, Vienna.

32. IAEA (1988), Basic safety principles for nuclear power plants, A report by the International Safety Advisory Group, International Atomic Energy Agency, Safety Series No.75-INSAG-3, Vienna.

33. Thurber, J. (1986), The effect of management and organizational structure on nuclear power plant safety, ANS/ENS International Topical Meeting on Advances in Human Factors in Nuclear Power Systems, Knoxville, Tennessee, 21-24 April.

34. IAEA, Status report on the development and use of numerical indicators to enhance nuclear power plant operational safety program, International Atomic Energy Agency, IAEA-TC-679.2, Vienna.

35. Starbuck, W., Milliken, F. (1988), Challenger: Fine-tuning the odds until something breaks, Journal of Management Studies, 25:4 July, pp. 319-340.

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

37. Lindqvist, J., Rydnert, B., Stene B. (1985), Organizational reliability improvement procedure, Projektsammanfattning (project summary), Organisationsbeskrivning (organizational description), Procedur (procedure), in Swedish, Swedish State Power Board, May.

38. Wahlström B., Laakso K., Tamminen A. (1987), Thoughts on how to maintain organizational effectiveness at a nuclear power plant, pp. 203-211 in Nuclear Performance and Safety, IAEA, Vienna 28.9-2.10.

39. IAEA (1988), OSART guidelines, International Atomic Energy Agency, IAEA-TECDOC-449, Vienna.

40. IAEA (1988), OSART results, International Atomic Energy Agency, IAEA-TECDOC-458, Vienna. IAEA (1989), OSART results II, International Atomic Energy Agency, IAEA-TECDOC-497, Vienna.

41. UNEP (1988), APELL, awareness and preparedness for emergencies at local level; a process of responding to technological accidents, United Nations Environment Program, Industry and Environment Office.

42. Dolores S. Morisseau, Isabelle E. Schoenfeld (1988), Organizational environment and operator culture, pp.568-569 in the proceedings of IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA, June 5-9.

43. La Porte, T., Consolini, P. (1991), Working in practice but not in theory: Theoretical challenges of "High-reliability organizations", Journal of Public Administration Research and Theory, J-PART, 1(1991):1:19-47.

44. H. Simon (1982), Models of bounded rationality: Economic analysis and public policy, Vol.1, Behavioral economics and business organizations, The MIT Press, Cambridge, MA.

45. Lösher, E. (1991), Library search using key-words Human Factors and Nuclear Power performed at International Institute for Applied Systems Analysis, January.

46. Reig, J. (1990), Closing remarks in the "Seminar on the use of unusual event reports for improving nuclear power plant safety", IAEA-SR-169, International Atomic Energy Agency, Vienna, 14-18 May.

A. RASTAS

INDUSTRIAL POWER COMPANY LTD.

MANAGEMENT-RELATED PRACTICES IN INDUSTRIAL POWER COMPANY LTD (FINLAND)

Industrial Power Company Ltd (TVO) operates two BWR units of 710 MW each in Olkiluoto, Finland. They have been taken into operation in 1978 and 1980, respectively. During recent years the capacity factors have been about 90 per cent.

The Olkiluoto plant units cover around one fifth of Finland's electricity consumption. Therefore the good performance of the units is essential for the whole country where no fossile fuel resources are found, the climate is cold and the industry is energy-demanding.

TVO is owned mainly by Finnish industry and supplies energy to its shareholders at cost. The strategy of the company is very straightforward, to produce maximum amount of electricity at minimum cost maintaining high safety standard.

TVO was started from scratch. The company organization was created in step with building, commissioning and operating of the plant units. There were no old traditions to hinder the implementation of the most suitable practices being in line with the company strategy.

Foreign principles and practices are seldom followed as such but reviewed critically and adapted to the Finnish conditions. This policy has led to some practices which may not be common elsewhere.

Quality assurance has had a significant role in all the activities. The policy is to achieve high quality by making, not only by controlling.

The organizational responsibilities are clearly defined in a manual always kept up-to-date. Ad hoc groups are established to solve special problems. Constant emphasis is put on the good teamwork and effective reporting mechanism.

The staff's ability to run the plant is maintained and improved by continuous training and education. Attention is also paid to the work motivation as well as to the mental and physical condition.

The staff taking care of the daily operation and maintenance is supported by a staff concisting of high level specialists. The motivation and the competence of this technical support has been maintained and enchanced by many special projects, such as the capacity uprating of the plant units, the construction of an intermediate storage for spent fuel, backfitting of the containments against degraded core accidents, PRA-study and construction of the final repository for reactor waste.

Co-operative relations are maintained with the original vendor and supplier organizations. Prompt access to technical support services is secured by frame contracts.

In utilization of operating experiences the major emphasis is put to the own plant and to the sister plants in Sweden.

A competent, effective and strict supervisory authority is a necessity for the successful operation. In Finland the authorities are highly qualified. An active and open communication is maintained to both directions.

A strict boundary between safety and non-safety matters is not applied. Almost all the matters are interpreted to be safety-related, only some more than some others. The safe operation of the plant and its high availability are seen most often as synonyms. They are seldom in cotradiction.

System Safety and Safety Culture[1]

by

Bernhard Wilpert
Technische Universität Berlin

1. Introduction

Safety and reliability of complex technical systems is usually, from an engineering point of view, treated as a problem of probabilistic risk analysis. A relatively large portfolio of approaches and techniques exists for this problem. Quantitative methods for analysis of the human, social and organizational factors contributing to systems safety rely on the same probabilistic rationale as the technical risk analysis, although it is becoming increasingly clear that this logic is inappropriate for the analysis of human failure propensities. What is required here are causal models of the human, social and organizational conditions and mechanisms leading to systems (un)reliability (Rouse & Rouse, 1983).

In addition, based on empirical evidence of accident and near accident analyses (Munipov, 1990; Reason, 1990; Wilpert & Klumb, 1991), it is safe to claim that safety and reliability must be considered as a performance result - like product quality - of the whole socio-technical system. "Safety culture" has become a fashionable catchword to denote this holistic perspective that encompasses the total socio-technical system. Hence, reflections on organizational and managerial factors contributing to safety performmance must be guided by systemic thinking. A first part of this paper, therefore, discusses the implications of comprehensively taking into account the total system. A second part then, by way of a case analysis, illustrates social, organizational and managerial factors contributing to system (un)reliability. The conceptual bases of safety culture and its potential role in systems safety is treated in the concluding part of this paper.

2. Total System as Point of Reference

The first problem that presents itself here is the question regarding system boundaries, i.e. what are the constituting elements and parts belonging to the "system" in question? A simplified, but nevertheless convincing illustration of the US accident prevention system of civil aviation can be found in a

[1]Paper prepared for the joint IAEA, IIASA meeting on "The Influence of Organization and Management on the Safety of NPPs and other Industrial Systems", Vienna, Austria, 18-20 March 1991

presentation by Miller (1988):

Fig. 1 about here

The picture neatly brings into focus all those factors of the comprehensive system contributing to a given performance task, namely safety. Beginning from collectively shared knowledge of known precedent, leading to specific requirements imposed by the Federal Aviation Agency which constrain certain manufacturer solutions, offering the public choices of purchasing decisions which are implemented on the operator level. Each incident/accident and the ensuing investigation then constitutes the basis for new known perecedents and sets into motion various feedback circles into the whole system.

System safety, a term first entering the literature around 1954, may with Miller (1988:72) then be defined as

> the result of the solution of engineering, operational and managerial tasks to avoid accidents and incidents of a given system.

This is what I meant with the notion of safety as a performance result of all relevant elements of the total socio-technical system. This encompassing conceptual approach has important implications for what we consider "the system". The following case analysis may illustrate this point.

3. An Illustrative Case

In an analysis of an incident that occurred in the reactor block of Biblis A in December 1987, where we utilized a total systems analysis approach, we could show that indeed the incident must be described as an event in which complex technical, organizational, social and individual factors that converged as necessary conditions for the occurrence of the incident (Wilpert & Klumb, 1991). "Human failure of the team of operators", "operator error" (and ensuing culpabilization of ther individuals envolved) played a rather marginal role according to our opinion. This, by the way, corresponds to a result of the Institue of Nuclear Power Operations which analyzed 180 NPO incidents and attributed only 16 % of them to "front line errors" (INPO, 1985). Also in the Biblis A case we found conditions, decisions, design faults and incorrect judgements of management that were far "upstream" of the actual incident, i.e. factors which Reason (1990) calls "latent failures". What then was the matter with Biblis?

A detailed account of the events that, on December 17, 1987, lead to the emission of a small amount of radioactive substance into the environment of reactor block Biblis A has been given elsewhere (Nucleonics Week, December 1988; Wilpert & Klumb, 1991). Suffice it to say here that during the course of an operation reactor restart, an incorrectly open valve caused a sequence of events that 15 hours later were recognized by the then second subsequent shift as potentially harmful. A risky "last minute" maneuver of the shift to close the open valve had the emission consequences. The ensuing public debate was filled with contentious charges ("near catastrophy of Tchernobyl dimensions") and countercharges ("easily controllable incident") concerning safety and trust of the German nuclear power industry.

Our (here reduced) list of the incident producing factors we were able to indentify exclusively on the basis of published reports included:

(1) Faulty design
- The exact position of the open valve was difficult to determine since there existed no additional criteria for the verification of a faulty position: lackof requisite redundancy.
- Technical constraints reduced the exactness of measurement indicators.
- Alarm signals were often ambiguous.
- Software and physical arrangements for error protocols tended to reduce the significance of a given alarm.

(2) Organizational factors
- Work load under certain task conditions (e.g. reactor restart) is such that certain information cannot taken into account. Economic considerations may add to these constraints.
- The original risk analysis evidently failed to take into account "unimaginable" circumstances and, hence, developed no technical defences against them.
- The "siege climate" between public and NPO-management increases proclivities of management to "play down" events.

(3) Contributing social factors
- Processes of "group think" (Janis & Mann, 1977) may have prevented the third shift to recognize the emergent system state - or the competence mix of the shift team was inadequate.
- Previous experience with (sometimes faulty) error messages may produce in the team a tendency to "rationalize away" signals that do not fit the socially shared interpretation of the situation.

(4) Contributing individual factors
- Erroneous generalizations of previous experiences may lead to faulty learning: what has proven in 99% of the cases an adequate action may, und "unimagibale circumstances", turn out to be a fatal misjudgement.
- Research on handling complex problems (Doerner et al., 1987) has shown that people have a hard time to evauate exponential system development states and to think in terms of non-linear causal nets, a factor that seems to have influenced also the events in Biblis A.

. Reason (p. 148)

Reason (1990:148) in his important recent book on human error gives a succinct representation of the relationships described. They require a much larger problem horizon than usually employed. I would even go so far as to expand his model even further by including also the governmental control agencies and the public at large. A case in point is the reaction of the Biblis management to the public debate when it instituted new organizational safety control units and procedures within the plant. Another point in case is what might be called the dysfunctional effects of **regulation overload** often stipulated by over-anxious official regulators: rather than leading to a "Sicherheitskultur" (= safety culture) regulation overload leads to an "Absicherungskultur", a set of mind and behavior in which every person tries to cover their behinds by making sure that he/she has ticked off all required items on a control list in order not to be made liable in case something goes wrong. A behavior thus induced is tantamount to flight from responsibility and may interfere in necessary corrective actions by the operator. This already leads into the next part:

4. Safety Culture

The concept of culture, coming from social and cultural anthropology, has in recent years invaded organization sciences. Organizational culture has become an ubiquitous term probably for two reasons: it caters to the emerging need for more holistic concepts and everyone can easily associate something meaningful with this umbrella term: collective will, invisible force behind organizational phenomena, personality of an organization, shared attitudes, philosophies, assumptions, values etc. In short: the term is in need of conceptual clarification.

Already in cultural anthropology culture found a multitude of definitions. One of the central discussions related to the question whether culture should be defines exclusively on the cognitive, attitudinal and evaluative level ("programming of the mind", Hofstede, 1980) or whether the term ought to cover also behavioral and structural aspects of a social unit.

Concerning the concept of organizational culture a contentious debate concerns the question whether organizational culture is something an organization **has** or something an organization **is.** In the former understanding organizations have certain characteristics that can be added to the organization and the term organizational culture is seen as a kind of managerial technology, comparable to the concept of corporate identity. This is a functionalist notion. In the latter sense, organizational culture is something that grows from the interaction of its members, something that is collectively constructed, which expresses itself not only in norms, attitudes and values, but also in behavior. In this sense organizational culture denotes the essence of the organization.

I favor the notion of organizational culture referring to the essence of an organization, mainly because we know from theoretical reasoning as well as from empirical and everydays evidence that attitudes, norms and values do not necessarily tranylate into corresponding behavior. People deviate from norms, act by trade off judgements among values. But also because the essential notion of organizational culture avoids the erroneous belief that culture can be turned on and off ad libitum. The development of organizational culture is a laborious collective process enveloping the whole of the organization.

Safety culture then should, to my mind, be understood in that latter sense of the term as well.

> **Safety culture is the shared consciousness and corresponding behavior of all systems members that promote safety of the total system.**

Safety culture, if the concept is to make practical sense, must pervade the whole system, i.e. with this understanding concern for safety cannot be delegated to a part or subsystem of the system (safety engineers, management, regulators). It cannot be introduced per ordre de moufti but requires a lenghty process of organizational development of the total system to arrive at collective mental representations of all system members concerning the role and production goal of safety **with their corresponding behaviors**. In that sense safety culture is a notion that attempts to look at the causal social and organizational conditions for safe and unsafe behavior beyond the probabilistic understanding of the occurance of certain human acts.

We can now have a brief look at the most authoritative document on safety culture in NPOs, the Report by the International Nuclear Safety Advisory Group on <u>Safety Culture</u> (Safety Series No. 75-INSAG-4, 1991). I shall address four points that I consider of critical importance for our discussion:

(1) Total systems perspective
(2) Definition of safety culture
(3) Developmental approach
(4) Learning system

In raising some critical points I do not want to denigrate the value of this important and future oriented document, but simply to identify some points that may deserve more attention.

(1) Total systems perspective
The document clearly views safety culture in a total systems perspective, which we postulated above as crucial, covering the whole gamut of parties involved, from regulators to operators, this being a necessary condition for safety culture:

> "...the discussion extends to Safety Culture in all concerned, because the highest level of safety is achieved only when everyone is dedicated to the common goal" (point 3).

(2) Definition of safety culture
The INSAG-definition reads:

> "Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance" (p. 1 and point 6).

The document is a bit amiguous with regard to the central defining elementssa of Safety Culture. In the Summary it emphasiszes that Safety Culture "is attitudinal as well as structural" and that it concerns perceptions and action. But the next sentence elaborates again that Safety Culture relates "to personal attitudes and habits of thought" (p. 1). This ambiguity prevails throughout the document. By linking the definition of safety culture predominantly to attitudes and cognitive, at best motivational, attributes (point 8), it leaves the essential behavioral and structural dimensions elaborated above only implicit. They are, of course, recognized in the whole document as important, but without their integration into the definition. As it was said before, it is an error to assume that behavior necessarily corresponds to attitudes. Behavior is a consequence of cognitive as well as social, structural and organizational, situational conditions.

(3) Developmental perspective
The document advocates an approach of turning a NPO-system into a safe system which starts at the apex of the system and works itself top-down. The operating staff is expected to respond (part 3.3) to the nationally legislated and managerially layd-out policy framework and requisite managerially induced working environments. In other words, the underlying developmental model is what we call in psychology an S-R-model: a stimulus (S) is set and the individual is expected to give the appropriate response (R). Adequate reinforcement will help the individual to learn and stabilize the requisite response.

It seems doubtful that the organizational development required in order to turn NPO-systems into safe systems of excellence can be described by such simple models. If safety culture is conceived as the consequence of the interaction of all system members in the collective construction of safe organizational realities, more emphasis is needed on these dynamic interactive processes. They imply the involvement and participation of all systems levels in such a systems development beyond the mere reflexive response to stimulus conditions.

(4) Learning system
Cybernetics and systems theory teach us that living systems mainly learn from their mistakes. Quite in line with this received insight the INSAG document advocates self-regulatory strategies to facilitate such learning through regular review of safety relevant activities, feedback of operating experience in order to learn and to avoid a punitive search for schortcomings (point 3.1.4).

I wonder whether we might not go one more step beyond by introducing anonymous reporting systems on incidents, potential incident conditions and imaginable technical, social and organizational trigger factors which are systematically documented and anonymously analyzed by independent institutions, similar to the Aviation Safety Reporting System of the USA. Thus the organization develops an organizational memory requisite for systems learning. The anonymity and independence of the proposed analyses seem to be essential conditions in order to overcome what the INSAG-document calls the "siege mentality" in the public debate and the "punitive search for shortcomings" within organizations.

5. Conclusion

Safety, reliability and risk of complex socio-technical systems are traditionally analyzed from an engineering point of view that favors probabilistic risk analysis techniques. Such techniques attempt to include also assumptions about probabilities concerning the occurrence of individual behaviors. Relatively rare are investigations that study human reliability and error behavior in a more holistic and systemic perspective which comprises the technical, individual, social and organizational conditions for the occurrence of particular human activities. This in itself surprises, since safety and reliability cannot be described except in terms of performance characteristics of the total system. A crucial and at the same time difficult problem, therefore, concerns the boundaries of the focal system. In line with present trends of thinking we have argued that these boundaries must not be drawn too restrictively.

At the same time one must note that the development of theoretical concepts and methodological techniques which would facilitate such comprehensive sytemic approaches are still in statu nascendi. The concept of safety culture may, with proper specifications, serve as a model for new ways of thinking about safety in complex industrial systems.

References

Doerner, D., Kreuzig, H.W., Reither, F. & Stäudel, Th. (1983). Lohhausen: Vom Umgang mit Unbestimmtheit und Komplexität. Bern: Huber

Hofstede, G. (1980). Culture's consequences, London: Sage

INPO (1985). An analysis of root causes in 1983 and 1984 significant event reports. INPO 85-027. Atlanta, GA: Institute of Nuclear Power Operations

INSAG (1991). Safety culture. A report by the International Nuclear Safety Advisory Group. Vienna:International Atomic Energy Agency. Safety Series No. 75-INSAG-4

Janis, I-L. & Mann, L. (1977). Decision making: A psychological analysis of conflict, choice, and committment. New York: Free Press

Miller, C.O. (1988). System Safety, in: E.L.Wiener, D.C.Nagel (eds.), Human factors in aviation, San Francisco: Academic Press, pp. 52-80.

Munipov, V.M. (1990). Der menschliche Faktor bei Havarien in den Kernkraftwerken Tschernobyl und Three Miles Island. In Gottlieb Daimler- und Karl Benz- Stiftung (eds.) 3. Internationales Kolloquium Leitwarten. Köln:TÜV-Rheinland

Reason, J. (1990). Human error. New York: Cambridge University Press

Rouse, W.B. & Rouse, S.H. (1983) Analysis and classification of human error. In: IEEE, Transactions on Systems, Man and Cybernetics, 4, pp. 539-549

Wilpert, B. & Klumb, P. (1991). Störfall in Biblis A. Theoretische und pragmatische Überlegungen zu einer systemischen Betrachtung der Ereignisse. In: Zeitschrift für Arbeitswissenschaft.

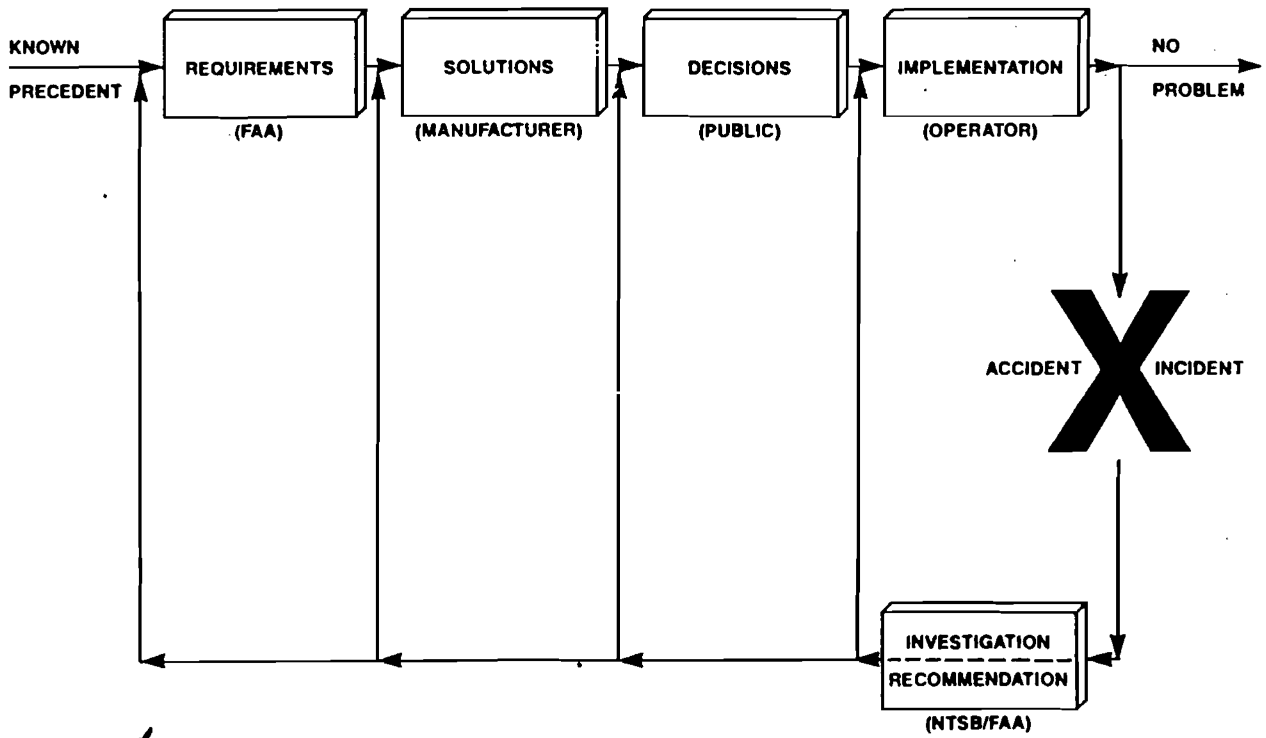


Figure ~~3-1~~ 1. The civil aviation accident prevention system. The principal parties in each are shown in parentheses.

APPENDIX D

Participants

Prof. Dr. B. Wilpert
TU Berlin, Sekr. DO. 303
Institut für Psychologie
Dovestrasse 1-5
D-1000 Berlin 10, Germany
Tel.: 06 030 314-2 2915

Mr. A. Rastas
Industrial Power Company, Ltd.
Fredrikinkatu, 51-53B
SF-00100 Helsinki, Finland
Tel.: +358 38 3811
Fax: +358 38 3813009

Mr. J. Mc Ardle
7 Medlows
Roundwood Park
Harpenden
Hartfordshire AL5 3AY, U.K.
Tel.: +44 582 767058

Mr. R. Nakazono
World Association of Nuclear Operators
Coordinating Centre
262a Fulham Road
London SW10 9EL, U.K.
Tel.: +44 71 3523617
Fax: +44 71 3519678

Prof. J. S. Carroll
Massachusetts Institute of Sloan School of Management
50 Memorial Drive E52-590
Cambridge, MA 02139, U.S.A.
Tel.: +1 617 2532617
Fax: +1 617 2532660

Dr. C. Perin
Massachusetts Institute of Sloan School of Management
50 Memorial Drive E52-590
Cambridge, MA 02139, U.S.A.
Tel.: +1 617 2532617
Fax: +1 617 2532660

Dr. Jon Olson
Battelle Seattle Research Center
4000 NE 41st Street

P.O. Box 5395
Seattle, WA 98105-5428, U.S.A.
Tel.: +1 206 5253130
Fax: +1 206 5283552

Dr. A. H. Protsenko
Central Economic and Mathematical Institute
USSR Academy of Sciences
Krasikova str. 32
SU-117418 Moscow, U.S.S.R.
Fax: +7 95 1292627

Dr. G. Sergeev
Central Economic and Mathematical Institute
USSR Academy of Sciences
Krasikova str. 32
SU-117418 Moscow, U.S.S.R.
Fax: +7 95 1292627

IAEA

Ms. E. Swaton, NENS-SAS (Scientific Secretary)
Mr. B. Thomas, NENS-SAS
Mr. M. Dusic, NENS-SAS
Mr. A. Erwin, NENS-NOSS
Tel.: +43 1 2360
Fax: +43 1 234564

IIASA

Mr. B. Wahlström, SET (Scientific Secretary)
Tel.: +43 2236 715210
Fax: +43 2236 71313