THE WORLD BANK

POLICY PLANNING AND RESEARCH STAFF

Environment Department

Why Do Complex Organizational Systems Fail?

Jens Rasmussen
and
Roger Batstone

October 1989

Environment Working Paper No. 20

ACKNOWLEDGMENTS

This paper was prepared by Jens Rasmussen (consultant) and Roger Batstone of the Environment Department to disseminate the results of a workshop on organizational failures from the perspective of safety control and risk management held at the World Bank from October 18-20, 1988. The authors gratefully acknowledge the very responsive cooperation of all the contributors and discussants of the workshop in the preparation for the workshop and these proceedings. All contributors made material and position papers available for distribution ahead of the meeting and have updated their papers in response to the interactions in the workshop. Furthermore, we have received many comments and proposals during the planning and editing periods which have been extremely helpful. The valuable assistance of the chairmen and rapporteurs of the sessions in planning and controlling the individual session is thankfully appreciated. A special thanks is due to the general chairman Peter Benton who very diligently kept the main thread running through the sessions and secured the very responsive atmosphere of the workshop.

ABSTRACT

High reliability organizations have evolved which have adapted to operate most efficiently and effectively, as well as safely close to the boundary of the safety domain. In contrast the management and organization of many industrial, commercial and other complex modern operations and the regulation of them in different cultural settings have not kept pace with the increasing sophistication of technology and its complexity. As a result the frequency and magnitude of organizational failures and the subsequent economic and environmental impacts are increasing at an alarming rate. A multi-disciplinary workshop was held at the World Bank during October 1989 with a focus on safety and risk management to determine what needs to be done to reverse this trend and to propose an agenda for future action. This paper presents the summary results of these discussions and shows that substantial progress can be made even in the short to medium term in guiding managements of organizations and government policy makers in different cultural settings towards more efficient and reliable management and organizational systems. High priority areas of future research are also identified.

FOREWORD

The World Bank co-sponsored this workshop jointly with the Danish, Swedish and Dutch Governments as the first in a series of three to be held over a period of three years. The objective is to develop guidelines, codes of good practices, and recommendations to government and organization decision makers to promote safe, reliable and efficient organizations operating complex technologies in different cultural and regulatory settings, as well as to identify future research priorities. This workshop represents the first attempt to address Risk Management in its full organizational and systems context. The purpose of this approach is to provide a true perspective for evaluating current status of developments in the field, and limitations of existing methodologies, as well as to identify areas of commonality between the various disciplines for future collaboration.

As a result of a too narrow perspective by risk practitioners and decision makers, management of safety and risk is currently viewed as the down-side of the business of an organization to produce benefit(s), and is commonly considered as the poor second cousin to the management of benefit. However, from an organizational systems perspective, the result of the workshop indicated that risk and benefit are two sides of the same coin and can mutually reinforce management's objective to improve system performance, efficiency, reliability, etc. It was also concluded that the safety and risk practitioners are increasingly alienating their profession from the decision and policy makers in enterprises and governments by developing more and more sophisticated "black box" methodologies for analyzing risk with results presented in unfamiliar terms and with undefined boundaries of validity. In an attempt to redress some of the fundamental flaws in these approaches, a group of incidental side issues have also evolved such as: "risk perception," "acceptable risk," "voluntary and involuntary risk," etc., which further diverts attention away from the central concern of decision and policy makers in organizations to manage and control risk.

In general, decision and policy makers are often poorly informed in relation to the risk side of the coin or do not trust the results presented to them. In contrast, the benefit side is usually well presented, in a timely manner and is clearly understood. In most cases decision makers simply do not even realize now poorly informed they really are in relation to risk. As indicated in the discussions as the workshop, what is presented as safety and risk assessments in most organizations represents only a small fraction of the risk profile of the organization.

The risk professionals, therefore, are challenged to make a fundamental reappraisal of their future role in assessing and communicating risk to decision and policy makers in the organization that they serve. This would involve in part: making explicit the underlying assumptions and conditions under which their methods and results are valid, making explicit the boundaries of their system, and presenting the results in a format which is useful for support of actual management decision making.

Likewise the human factors specialists are challenged to expand their vision beyond the confines of human error and reliability analysis and to explore ways in which they could link with the cognitive, decision, systems and organizational specialists in developing risk profiles of organizational and

management systems in different regulatory and cultural environments. An important finding of the workshop is that these groups of specialists are converging in their approaches to, and understanding of, organizational systems and a "conceptual market place" had been established which would enable active trading of ideas concepts, methodologies, etc., among the various disciplines. Significant advances in developing organizational system risk profiles therefore could be expected even in the short to medium term. The risk professionals would also play a role in linking their future developments into this program to give a complete up-to-date picture of risk in organizational systems so that the two sides of the risk/benefit coin are presented to decision and policy makers in a timely manner to optimize system performance.

The conclusions of the workshop strongly support the hypothesis that the present industrial management and organizational structure and practice have not kept pace with technological development and that useful insights can be gained from the experience of high reliability organizations in other fields and special cultural settings.

WHY DO COMPLEX ORGANIZATIONAL SYSTEMS FAIL?

TABLE OF CONTENTS

1. LIST OF PAPERS PRESENTED

1.1 INTRODUCTION

1.1.1 **Rasmussen:** Workshop Outline Background Paper

1.1.2 **Rasmussen:** Some Concepts: A Note for Clarification

1.2 Industrial Safety Viewed as a Control Problem

1.2.1 **Sheridan:** Introduction: Industrial Safety Viewed as a Control Problem
1.2.2 **Rasmussen:** Industrial Safety Viewed as a Control Problem
1.2.3 **Volta:** Safety Control and New Paradigms in System Science
1.2.4 **LaPorte:** Discussion Paper
1.2.5 **Shikiar:** Discussion Points on Industrial Safety Viewed as a Control Problem
1.2.6 **Kugler:** Self-Organization and the Evolution of Instability: The Awakening of Sleeping Nonlinearities

1.3 Risk Management, Current Problems and Practices

1.3.1 **Reason:** Resident Pathogens and Risk Management
1.3.2 **Westrum:** Organizational and Inter-Organizational Thought
1.3 3 **Cramer:** A Programmatic Approach to Risk Management
1.3 4 **Ward:** Will the LOCA mind-Set be Overcome?
1.3 5 **Van Kuijen:** Prevention of Industrial Accidents in the Netherlands
1.3.6 **Cross:** Bank Failures
1.3.7 **Barreto-Vianna:** Risk Management, Current Problems and Practices in Brazil
1.3.8 **Thero:** Position Paper of the Quality Technology Company

1.4 Design of Reliable Organizations

1.4.1 **La Porte:** Safety Control and Risk Management:Views from a Social Scientist at the Operational Level
1.4.2 **Rochlin:** Technology, Hierarchy, and Organizational Self-Design. U.S. Naval Flight Operations as a Case Study
1.4.3 **Lanir:** Accidents and Catastrophes: The Safety Management of Contradictions
1.4.4 **Dynes:** Organizational Adaptations to Crisis: Mechanisms of Coordination and Structural Change (Including introductory note)
1.4.5 **Meshkati:** An Integrative Model for Designing Reliable Technological Organizations: The Role of Cultural Variables
1.4.6 **Fischhoff:** Simple Behavioral Principles in Complex System Design

1.5 Organizational Decision Making

1.5.1 **Brehmer:** Changing Decisions about Safety in Organizations
1.5.2 **Kunreuther and Bowman:** Post Bhopal Behavior of a Chemical Company
1.5.3 **Ostberg:** On the Dilemma of High-level Decision-Makers in Their Handling of Risks in Political Contexts
1.5.4 **Baram:** The Influence of Law on the Industrial Risk Management Function
1.5.5 **Zimmerman:** The Government's Role as Stakeholder in Industrial Crisis

1.6 Adapting Risk Analysis to the Needs of Risk Management

1.6.1 **Brown and Reeves:** The Requirements in Risk Analysis for Risk Management
1.6.2 **Andow:** Discussion Paper
1.6.3 **Swain:** Some Major Problems in Human Reliability Analysis of Complex Systems
1.6.4 **Heising:** Discussion Statement, Two Pages
1.6.5 **Nertney:** Root Cause Analysis of Performance Indicators
Nertney: Adapting Risk Analysis to Needs of Risk Management, A Discussion Statement
1.6.6 **Wreathall:** Risk Assessment and its Use in Feedforward Control
1.6.7 **Embling:** The Risk Management System Approach
1.6.8 **Rowe:** Risk Analysis: A Tool for Policy Decisions
1.6.9 **Perdue:** A Decision-Analytic Perspective for Corporate Environmental Risk Management

1.7 Decision Support for Safety Control

1.7.1 **Rouse:** Designing for Human Decision Making in Large-Scale Systems
1.7.2 **Pew:** Human Factors Issues in Expert Systems
1.7.3 **Fussel:** PRISM: A Computer Program that Enhances Operational Safety
1.7.4 **Sheridan:** Trust and Industrial Safety
1.7.5 **Moray:** Can Decision Aids Help to Reduce Human Error?
1.7.6 **Woods:** Cognitive Error, Cognitive Simulation, and Risk Management

1.8 A Cross Disciplinary Discipline?

1.8.1 **Livingstone:** A Cross Disciplinary Discipline?

2. INTRODUCTION

From the perspective of Project Risk Analysis for World Bank financed projects in developing countries, two major issues were identified by the participants at this first workshop on risk management namely:

(a) The limitation of current approaches to risk analysis.
(b) The application of risk analysis to risk management.

2.1 Limitations of Currently Used Techniques

1. Risk analysis has been a rapidly developing field of expertise in various professional disciplines with little interaction between them up to the present time. Thus, in relation to project risk analysis where we are dealing with the success or failure of a project in its organizational context, we find that each of the various disciplines is only dealing with a small part of the total risk picture. The economist is concerned with the risk of project failure in relation to the variable macro and/or micro economic conditions prevailing during the life of the project. The technologist is concerned about the risk of failure of the technological components of the system, while the financial analyst provides an assessment of the financial risk, etc. Even taking all these components of the risk matrix into account, there is still a large gap which needs to be addressed, namely the risk of failure in the management/organizational components of the system.

2. In the case of bank failures that occurred in the USA during the 1980's, a recent US Treasury report indicates that 80-90% of these failures could be attributed to organizational and management system failures, which are typically not addressed by conventional risk analysis techniques. The report found that a downturn in economic conditions during this period was only a minimal causal factor in regard to these system failures. An analysis of major technological disasters such as: Bhopal, Chernobyl, Exxon Alaska oil spill, Kings Cross Underground fire, etc. indicates a similar pattern; 80-90% of the failures are in the hierarchy of the management and organizational system and only 10-20% can be attributed to the operator and equipment failures, that are so often the focus of blame. The sophisticated risk analysis techniques developed to-date by the engineering, human factors, and scientific disciplines only address 10-20% of problem, since they have not focussed on the management and organizational aspects of system failures.

3. Another factor which the economic and financial community have not grasped to the same extent as the engineering disciplines is the effect of "common mode failures" of numbers of small subsystems or components which can lead to major system failures. A striking example of this is the current crisis in large numbers of S&L Institutions in the USA, with a major financial impact to the country estimated in excess of $100 billion. This case also graphically illustrates the importance of deciding where to draw the system boundary, when making decisions regarding risk. It seems that the regulator in this instance is as much a part of the problem as the individual S&L subcomponents of the bigger system, thus compounding the common mode failures.

4. In the view of the technologist, the current practice of sensitivity analysis as applied to the Economic Rates of Return (ERR) and Internal Rate of Return (IRR) estimates for Bank projects is a rather crude surrogate for risk analysis. The application of sensitivity analysis to ERR and IRR assessments, therefore, raises questions as to the extent of the validity of such a technique for risk decision making purposes, and the manner in which it is being used in Bank projects. For instance, technological risk analysis (as currently developed) is only valid as a tool for assisting decision makers to select between technological options.

2.2 Application of Risk Analysis to Risk Management

5. A "one-off" evaluation of risk at the appraisal stage, no matter how comprehensive, has limited value in promoting the success (or avoiding the failure) of Bank financed projects. Risk analysis should be treated as an integral part of the decision making process throughout the operating life of the project. Those organizations which have adopted such an approach have demonstrated that system efficiency, reliability and performance is markedly increased over the short as well as the long term. Much work is required to raise awareness of this issue and to operationalize risk analysis techniques.

6. Limitations of current risk analysis tools is part of the problem, but lack of appreciation of complex management and organizational risks by decision makers in organizations - both in developed as well as developing countries - is a major barrier. Risk analysis is still viewed by management in many organizations as a "negative factor", as an unnecessary "add on" activity, and there has been insufficient realization that it can play an important role in system efficiency and performance.

> Mr. Peter Benton, Director General of the British Institute of Management, chairman of the Bank workshop on Risk Management, illustrated this with the example of a good sailor (manager) with a detailed chart (risk analysis) showing the shoals and reefs (risks), who was able to safely negotiate these hazards with little margin (saving money) and was able to win the race (maximize profits).

The second Risk Management workshop in Sweden in November 1989 will start to draw up "charts" for guidance of managers attempting to incorporate risk analysis into the organizational decision making process. A proposed set of their guidelines is discussed further in Section 5.

3. SUMMARY OVERVIEW OF THE WORKSHOP PROCEEDINGS

3.1 Introduction

7. In order to set the stage for a cross-disciplinary discussion of safety control and risk management going beyond the present discussion within the involved disciplines, a 'background paper' (Section 1.1.1) was prepared and circulated to all contributors. The selection of topics to include in this note was made by the organizers according to the key problems met during analysis of major accidents and attempts to develop predictive risk analysis.

8. The paper is followed by a note (Section 1.1.2) responding to the discussions during the workshop. **Rasmussen** concludes in this note that a convergence is emerging in the modelling efforts within disciplines such as systems and control engineering, decision theory, and management and organization science which can lead to fruitful cross disciplinary research and development in system safety, if an integrated system point of view is taken.

3.2 Industrial Safety Viewed as a Control Problem

9. Modern technology implies rapid development and large-scale systems. In design for safety, direct empirical evidence must be supplemented by analytical prediction. The focal topic of the first session of the workshop was a discussion of the implications of this present technological trend and its implications for design of the socio-technical systems involved in systems operation and risk management. Can a control and systems oriented analysis of the entire safety control loop contribute to design and evaluation of reliable management strategies?

10. In this introductory note, **Sheridan** reviews the basic concepts of control system analysis. He discusses safety in a larger context and defines the concepts of control from the mathematical point of view of automatic control theory. He concludes that the automatic control perspective does not provide automatic safety, but it imposes a discipline in which safety related variables and their relationships can be defined in a better perspective.

11. To further set the stage for a systems point of view in the discussions, **Rasmussen** contributes a position paper in which he elaborates on the control perspective introduced in the background paper of the workshop. He discusses safety control in a wider context than Sheridan's automatic control perspective and takes a control system point of view on the socio-technical system involved in design and operation of large-scale technical installations. Like Sheridan, he concludes that a control system point of view will facilitate the identification of critical safety issues and guide selection of research priorities. To this end, he discusses the concepts of feedforward (pro-active) and feedback (re-active) measures for control of safety and the role of predictive risk analysis in such control. He emphasizes in particular the conflict between safety and operational goals and the potentially systematic degradation of system safety caused by learning and self-organizing features of the behavior of individuals and organizations. The question is raised whether modern approaches to system science such as catastrophe and chaos theories can

contribute to the analysis of the potential for systematic break-down of self-organizing socio-technical systems.

12. In order for 'general system science' to be useful to the kind of analysis of the potential for systematic break-down of large scale socio-technical systems with adaptive features, the classical cybernetic modelling approach needs to be modified to include semantic and intentional aspects of human systems. The position paper of **Volta** goes further in this line of argument in his discussion of the contributions of new system science paradigms. The basic view of this approach is that in the highly integrated modern society, systems cannot be nicely isolated for analysis. Any part of a system, being it a technical object or a human, will be involved in many systems at the same time. The basic view is, consequently, that for analysis, socio-technical systems should be considered "networks of communication or, in a human perspective, networks of commitments." This, Volta argues, implies the need for new system paradigms. He reviews four paradigms for analysis of non-reducible, systemic properties: (i) the classical, cybernetic paradigms in which systems are considered as the structure of a set; or (ii) as a process involving time and flow of information with focus on linear systems in equilibrium; and (iii) the new system paradigms viewing systems as irreversible, self-organizing entities far from equilibrium; or, (iv) in the latest development, as self-referential entities evolving by 'autopoesis.'

13. The implications drawn from this point of view relate very well with the aspects of risk management raised in the background paper of the workshop, which (a) emphasizes the system and its environment interacting in a reciprocally constructive sense (which is very noticeable for e.g., nuclear power industry in modern society), (b) introduces the notion that communication is not only information, but involves commitment and understanding which is analogous to the problems of communication of intentions and values and of casual arguments, mentioned in the background paper, and (c) the need to consider evolution and self-organizing system which is also in focus of Rasmussen's (Section 1.2.2) and Rochlin's (Section 1.4.2) position papers.

14. In the invited discussion statements, **La Porte** drew parallels from the discussion of self-organizing features to the results of the study of highly reliable organizations as found in air traffic control and aircraft carriers. The extremely high reliability found in dynamic environments such as flight deck operations on carriers depends on cognitive redundancy, a self-designing, flexible organization, and staff commitment. What are the implications when technical systems are posing irreversible boundaries to safe operation? "What do we, as a society, wish to see to make sure that well engineered systems are operated as designed?" La Porte's statements are elaborated further in the discussion of his paper in Section 3.4.

15. In his invited discussion statement, **Shikiar** elaborates on the communication problem raised by Rasmussen and Volta stating that communication is more than transfer of information, and he asks for more effort to overcome the problem of 'multiplicity of inputs to representation when several different professions are cooperating. He also points to the problem of different 'metrics of qualitative and quantitative analysis and warns that two errors in risk analysis are likely--premature and unreasonable attempts to quantify; and

ignoring variables not amenable to quantification. Finally, he raises the important question of `sociology of risk analysis' as a research priority.

16. **Kugler's** research is concerned with the evolution of order in patterns of movements in biological systems and his contribution demonstrates how the interaction between a model at the micro-level of the individual actor and the macro-level of an organization can serve to explain the evolution of structure of behavior in an organization. He uses for illustration the evolution from basic micro-macro properties of orderly nest building behavior by a colony of termites. This example supports the hypothesis, that formal models of self-organizing systems may be useful tools for exploration of organizational evolution. Furthermore, Kugler demonstrates by physical examples how operation approaching boundaries of an operating regime (`sleeping non-linearities') will induce changes of behavior which may serve to detect the boundaries and identify the type of non-linearity while the changes are still reversible. Whether similar techniques can be used to detect and identify boundaries of safe operation of a complex socio-technical system is an open question. However, the examples support the claim, that modern, formal paradigms from system science should be considered carefully for analysis of risk, which can be considered "sleeping non-linearities".

3.3 Risk Management, Current Problems and Practices

17. In Section 3.2 the stage has been set for a system oriented discussion of safety control and risk management from a general, theoretic point of view. This section should serve to put meat on the bones thus prepared. Reason and Westrum review the current problems in the light of recent major accidents, and the current practice within the chemical and nuclear industries is discussed by Cramer and Ward, whereas the problems in banking systems are dealt with in a paper by Cross.

18. **Reason** introduces the discussion of the key problems of industrial safety by an emphasis on the sensitivity of the `defence-in-depth' design philosophy to combinations of human failures. In a discussion of the nature and classification of human errors, he underlines the important distinction between errors, such as slips and mistakes which are defined with reference to the actors goals and intentions, and violations, which can only be described with regard to a social context of operating procedures, codes of practice and regulations. Violations are important because they include a large category which have "some degree of intentionality but which do not involve the goal of system damage" on part of the actor. Reason's discussion of violations under circumstances of taking paths of least effort or of double-bind conditions, therefore, relates closely to the discussion of system breakdown due to self-organizing features as presented in Section 3.2.

19. Reason reviews a number of recent major accidents, Bhopal, Chernobyl, Challenger , and Zeebrugee, and he concludes that in major accidents "rather than being the main instigators of an accident, operators tend to be the inheritors of system defects created by poor design, incorrect installation, faulty maintenance, and bad management decision." Two important conclusions emerge from Reason's review: First, disasters are rarely caused by any one factor, either mechanical or human; second, most of the significant root causes

are present within the system long before an accident sequence is identified. In short, violations very likely turn into `resident pathogens' to use Reason's very illustrative medical metaphor. Accidents thus involve a number of resident pathogens together with local triggers, and from this formulation, Reason derives a number of general principles for improving system safety which can, in fact, be mapped onto the control point of view discussed in the previous chapter. One of Reason's key conclusion is, for instance, the introduction of "pathogen audits" which, in effect, corresponds to introduction of a corrective feedback path serving to monitor the safety preconditions as identified during system design. Reasons concludes his paper by a discussion of the organizational attitude to safety in the situation when managerial decision making is "a delicate and complex balancing act in two feedback loops serving safety and production goals." In this way, Reason's paper gives a very important link between the human error mechanisms as viewed from a cognitive psychology point of view, and system safety viewed from an managerial control point of view.

20. While Reason illustrates from analysis of major accidents how cognitive error mechanisms in decision making can prepare socio-technical systems for disaster, Westrum focuses on the organizational culture and its influence on managerial decision making. How do organizations think? He analyzes three factors: Cognitive adequacy in organizations, management culture, and leadership.

21. He describes the degree of cognitive adequacy in terms of the different reactions to hazards by the organization: Denial actions, which include suppression (individuals are punished or dismissed) and encapsulation (observers are retained, but observation denied); repair actions, which include public relations (observations emerge but significance denied - sugar coating) and local repair (problem admitted and fixed, but wider implications denied); and finally reform actions including dissemination (global actions taken) and reorganization (reformation of operational system). Such responses can be used to define organizations along a scale of cognitive adequacy.

22. In addition, he characterize three levels of cognitive functioning of organizations: Pathological, e.g., when organizations actively circumvent regulations and laws under economic pressure; calculative, i.e., trying to do a good job according to the rules doing the best they can) and, finally, generative organizations exhibiting a high degree of leadership and creativity.

23. These distinctions are illustrated by a discussion of the attempts to cope with the ozone hole and the Michigan PBB contamination in 1972, and Westrum formulates a hypothesis concerning the ecology of thought: Will a creative ability to act enhance the ability to think? When organizations, for whatever reason, are restricted from acting on an observation of hazard, they will become less able to think about these hazards. A consequence of this hypothesis might be that highly regulated organizations are likely to develop Reason's `resident pathogens' because they will not observe them, while dynamic organizations moulding their structure according to the immediate requirements such as Rochlin et al's self-designing organizations will be better able to observe emerging pathogens. A similar argument is brought forward by Dynes with respect to emergency management organizations in Section 3.4: Following recent major accidents, politization due to public opinion has resulted in greater

standardization of emergency organizations, rooted in regulation. Planning efforts are, therefore, moved towards greater rigidity and bureaucratization, toward strong centers of authority and are based on command and control models. The result is that rigidity is emphasized where adaptability is needed. In adaptive organizations, structure bends or disappears when it gets in the way of solving problems. Westrum concludes this discussion with a broad argument: Major constraints on organizational and inter-organizational thought are shaped by organizational 'vested interests'. Cognition which takes place under strong economic and social pressure, is naturally shaped by them.

24. Finally, Westrum discusses the role of organizational culture in shaping organizational thought. The organization's culture provides traditions which orient it to expected problems and point it toward potential solutions. Organizational culture is a learned response to external forces, and gradually accumulates over time. It provides an internal constraint on what can be thought about and how situations are to be handled. Leaders can shape and change this culture through their own decisions and example. By providing channels for dissent and encouraging information flow, for instance, leaders can act to aid thought; they can provide important buffers against external constraints. Again, emphasis is placed on the evolutionary features of organizations, as it is for the discussions in Section 3.2 and 3.5.

25. In the remainder of the section, the emphasis is on current practice for industrial risk management. Cramer first reviews structures of risk management programs in the chemical process industry. Focus of risk management in this industry has moved from worker's safety, to environmental impacts on society. At the same time the context of risk management has been changing. The economic climate has become increasingly unstable: raw material suppliers develop their own production capacity and aging plants are shut down rather than modernized. A number of factors are driving the industry--public attention which may tempt industry to place plants in less regulated countries, increasing cost or unavailability of insurance and the tendency to go to court; together with a common desire to avoid accidents. In consequence, a number of movements in industry can be identified such as a cooperative efforts; and the use of probablistic risk analysis and corporate risk management programs, which are partly due to regulatory pressure and partly a need to reduce business risk.

26. Cramer discusses the autocatalytic effect of increasing public awareness from the rapidly increasing international media coverage of major disasters. The increasing coverage leads to a perception of a rapidly worsening situation which, in turn leads to increasing regulation. Cramer here, in fact, points to the effects of the feedback loop involving public pressure, regulation efforts, managerial decision making, and likelihood of hazards, which calls for an advanced system analysis to support policy making. There is a feel in the chemical industry that regulation may be beneficial but only if applied in the spirit of cooperation rather than in an adversarial manner. The ultimate intelligence and fairness of the media will be influential in shaping public opinion and government response. Process industry must learn to deal effectively with the media, which will require a mixture of honesty, patience and education. To this one could add the need to solve the problem of communicating an understanding of risk and causal explanations.

27. Cramer then reviews the government initiatives in US. He points to the slow development, which he partly attributes to the complexity and economic difficulties of the chemical industry, partly to a real lack of understanding of what to do and how to do it. Federal measures have centered on community right-to-know and emergency preparedness legislation to help public to prepare for accidents.

28. Based on this instruction, Cramer reviews the structure and content of an effective risk management program and concludes, stressing the need for industrial and institutional cooperation based on real and substantial consensus.

29. In an appendix suggesting discussion topics, Cramer points to the "regrettable, but true fact that the outcome of a successful risk management programs is that nothing seems to happen. When working properly, one tends to forget the need for such programs because the risk seems so low. In a highly competitive business that often comes under intense global economic pressure, programs that produce few clear returns on investment are usually the first targets of budget cutting." By these words Cramer echoes the discussion of the influence of organizational adaptation, discussed by Reason and Rasmussen in the previous chapters. He also points to the possible drawbacks of strictly enforced laws in a situation which basically calls for innovation and change. In this way, a voice from industry supports the observations made from the research quarters.

30. For the nuclear industry, the public pressure has had particularly visible impact, and the nuclear schemes for risk management have developed over a considerable time. Ward's discussion of the state of affairs in this industry with respect to human factors problems, therefore, is of particular interest in the present context.

31. The basic message of Ward is the too-nearly total preoccupation of the reactor safety community with the circumstances related to the Loss-Of-Coolant-Accident, in short the LOCA; a preoccupation "created by a billion dollars of LOCA research and now extending itself into the micro-consideration of severe accident phenomena." In his paper he discusses the possible contributions to safety from human factors (HF) research. He then expresses very limited confidence that this contribution will be made, and he mentions the barriers against the application of HF-research.

32. His basic position is that technology can be developed to ever increasing levels of perfection while the level of perfection of human performance to be reached by improved training and instruction has very distinct limits given by nature. He argues that the level of functional perfection of the technology now is acceptable and that focus should be on development of systems that are error tolerant: "We have today machines that are better than ever. And really--good enough. But our machines are operated and maintained by humans who are not, and inherently not, good enough. "--we need to place the human operator, technician, or mechanic in a physical and institutional context in which error, at reasonable rates, on his of her part will not matter." He then points to the fact that plants are not run by individuals, nor by a collection of such, but are so complex that they are run by sophisticated teams.

Consequently "we are not interested in error rates of individuals. Rather we should be interested in those of team" which should be designed to optimize performance. Again, we have here an argument for the flexible, adaptive organizations.

33. Basically, he finds that the human factors knowledge required is available and he therefore asks that question: "what are the barriers against adequate application." Here he finds the key barrier to be the above mentioned LOCA mind-set. He sees a modest new beginning in the present US Nuclear Regulatory Commission (NRC) programs for considering HF, but: "we don't need a modest new beginning, we need something more like a revolution." He is, however, "rather pessimistic about seeing other than glacial progress because the moguls remain suspicious of the technology that needs to be applied. They regard it as rather lightweight. They regard questions of organizational design and behavioral optimization as best answered by "seat of the pants" approaches. They recognize and respect the art of the piping design engineer, but not of the organizational psychologist. They refuse to see that the piping design engineer has done all he can, he has succeeded. But, the organizational psychologist has not had his turn at bat."

34. In this way Ward points to the problem of the global institutional systems design, including the communication between regulation, design and operation communities. In addition, the problem he raises relates to the question of managerial cultures opened by Westrum; thinking about problems is biased by the potential for acting by that decision maker.

35. In the next paper, Van Kuijen reviews the Dutch practice of accident prevention. He raises the criteria problem--what is acceptable risk; and to what extent should accepted risk levels be further reduced? He discusses the nuclear approach based on probablistic risk analysis together with a criterion "As Low As Reasonably Achievable; ALARA." The Dutch approach is interesting in the present context because of the high population exposure and sensitivity to risk led to an early attempt to introduce a legal request for risk management based on quantitative probablistic risk assessments. In the policy adopted, three domains of risk are defined separated by two boundaries: the upper one specifying the maximum acceptable level defined irrespective of the economic and social benefit that could result and a lower one defining the level below which is not sensible to try to reduce further the resulting risk. Between the levels, the ALARA criterion has to be applied.

36. Van Kuijen goes on to discuss the elements of decision making in risk management--hazard identification; quantification; decision on acceptability; and finally, what links risk assessment to risk management in the sense of the workshop, maintaining the situation of accepted risk. Van Kuijen reviews the Dutch practice for these decision elements and gives some actual case examples. He concludes with an illuminating account of the opinions of the Dutch industry and the need for further development. Initially, industry was skeptical towards the use of probablistic analysis as a decision tool because of the supposed degree of uncertainty of the models and the lack of data. In the Dutch case, however, the present conclusion is that the approach can be used reliably even if some improvement is needed. The improvement needed include topics such as

development of support systems, better management structures, and improved risk communication, topics which all supports the aim of these World Bank workshops.

37. The contribution to the workshop discussion given by **Cross** demonstrated the generality of management problems across branches and activities. In the analysis performed under the US Office of the Comptroller of the Currency (OCC), the conclusion is that a major contribution to bank failures is the policies and procedures of a bank's management and board of directors: "poor management and other internal problems are the common denominator of failed and problem banks. Management-driven weaknesses played a significant role in the decline of 90% of the failed and problem banks the OCC evaluated."

38. A number of observations of the analysis fit into the general picture of the present context: Nearly 60% of bank failures had directorates that had either lacked the necessary banking knowledge or were uninformed or passive in their supervision of the bank's affairs. This, in our context, is directly related to the potential for error recovery, making an organization vulnerable when the environment changes. Another observation was the role of overly aggressive, growth-minded policies contributing to eight out of ten cases. In this we recognize the lack of balance between production and risk in managerial control discussed in the previous sections.

39. The contribution of **Baretto Vianna** presents the problems met in a country with a particularly rapid technological development, such as Brazil. In such cases, risk management is not a current industrial practice and the fast development has resulted in many cases of serious damage. Vianna reviews the activities in Brazil, and concludes with a number of research recommendations pointing to the significance of cultural differences, not only between developed and rapidly developing countries, but also between ethical groups and professions.

40. Finally, **Thero** presents the views of a quality control expert. His basic thesis is that risk assessment and risk control cannot be determined separately, but must be examined in the context of the total integrated management system. Thero presents an inside view from his career of the effects of an increasing monetary and profitability pressure at the expense of quality, honesty and integrity of an otherwise concerned organization.

3.4 Design of Reliable Organizations

41. The problems presented to the contributors of this section in advance of the workshop where--what are the implications for organizational reliability of the `defence-in-depth' design practice; how can `requisite variety in organizational behavior necessary to cope with serious disturbances be maintained through long stable periods; if organizational `self-design' is an attribute of reliability, how then to cope with rare events?

42. The topic of this section is the influence of organizational structures on the safety of large scale industrial installations. In Section 3.1 Rasmussen draws attention to the role of individual and organizational learning and adaptation and he suggests that adaptation to economic and functional requirements can systematically endanger a system designed according

to the defence-in-depth principle, because the limits of acceptable adaptation defined by safety requirements are obscure to decision makers. A basic question for the discussion in the present chapter, therefore, is the relationship between adaptation and organizational reliability; what constitutes a high reliability organization?

43. The chapter is introduced by **La Porte**, a representative of the 'High Reliability Organization Project' of University of California, Berkeley which is concerned with field studies in 'high hazard-low risk' large scale organizations.

44. From his social organizational point of view, La Porte finds two important 'cross points' between risk management engineering as presented in section 3.1, and the organizational dynamic research in social science--the problems of 'latent error' and of 'emergency response.' He concludes that the continued improvement of safety now depends more on the social relations of operators, managers, and attentive external parties than on technological fixes and he emphasizes two important research topics--(i) organizational patterns that result in superior social reliability and operation capacity; (ii) the demands on organizations attempting to combine high tempo and peak-demand satisfying capabilities with emergency response capabilities. In his social scientist response he rephrases these questions--to what degree are we deploying systems that demand such organizational complexity that they push the limits of what can be managed beyond the level of safety and reliability the public demands? He notes that this is a question almost never addressed straight forwardly, and, if put at all, it is in the context of the individual behavior in the face of complex machines. He mentions the frequently quoted hypothesis that organizational scale and tight-coupling has grown to a level where human capacity to operate them declines (Perrow). It also points to the fact that some highly complex, hazardous systems are operated with remarkable levels of safety and asks whether the characteristic of these examples can be, that they require reliable ultra-safe operation as a condition of providing benefit. This proposition in a way mirrors the point made by Rasmussen, that the risk presented by defence-in-depth systems is related to the separation of the visible criteria of functional adaptation and (invisible) boundary of safe operation.

45. From this discussion, La Porte turns to an important expansion of the engineering understanding of the concept of technology to the view of technology as a system of social and organizational relationships which, in a social sense, define technology: people working together, are absolutely necessary for the possibilities of new or improved technologies becoming available in a society. Therefore, it is crucial to understand interactions between organizations, communities, and societal institutions within which technologies-as-organizations operate. In sort, La Porte argues for research to understand the global socio-technical system involved in safety and he highlights an important hypothesis in the present context: Advanced technologies depend intrinsically on very sophisticated conceptual and organizational requirements and are, therefore, highly resistant to modifications promoted by variations in local or national culture. In consequence, differences in local or regional effects of a particular advanced technology are more a function of variations in local or regional conditions than of the design of the technology. From this discussion,

La Porte concludes the logical necessity of technology, he expands to the social science view of at least five pairs of knowledge/behavioral conditions of nearly failure-free operation; conditions which add up to the requirement of adequate knowledge for early detection of approaching hazards together with error absorbing capabilities of the organization. This conclusion from a social science point of view supports the issues based on control theoretic considerations proposed in Section 3.1.

46. In a discussion of the findings of the Berkeley group in the reliable organization project, Rochlin supports La Porte's general conclusions by an analysis of the high reliability of the performance of an aircraft-carrier crew.

47. Rochlin introduces the presentation with a discussion of the difference between control and management. The substance of this distinction appears to be more of a terminological nature, and is elaborated on in more detail in the discussion presented in Section 3.1. The presentation by Rochlin appears to be very closely compatible with a control theoretic point of view. One of the key findings of the workshop is, in fact, the present convergence of the formulations appearing from contemporary research in social science, decision theory, and control and systems engineering; a convergence which makes the attempt to formulate cross-disciplinary research cooperation very timely and promising.

48. One distinction made by Rochlin is that between reactive and anticipatory control and management. He assumes that control depends on perfect knowledge, whereas management can be based on imperfect knowledge and he presents the computers' chess game based on pre-calculation in contrast to the expert's chess game based on intuitive anticipation. However, in both cases, the anticipation is based on a model of game performance, the expert's anticipation on intuition from empirical evolution of a large repertoire of game patterns, the computer's anticipation on a formal model of the constraints embedded in the rules of the game. This is not a difference between control and management but between two ways of establishing the basis for anticipatory control and unfortunately, the basic problem in safety of large scale systems is the lack of opportunity for management to acquire empirically the necessary intuition for the accidental patterns of events. The basic control problem is to combine the highly intuitive, empirical operational management skill with analytical understanding of the causality of accidents. The problem of defence-in-depth systems is that the mechanisms of the ultimate accidents are not activated during normal conditions and that, consequently, no opportunity is left the staff to gain intuition, whereas the risk in aircraft carrier flight operations are related to the boundary to loss of control in the dynamic system performance of everyday operation.

49. In his paper, Rochlin characterizes the relationships between technology and organizations with respect to complexity, error, and risk against the background of the influential studies of the Berkeley group of the evolution of the high-reliability organization of an American aircraft carrier. Even if the context is that of a social science study, the notions used to analyze the organization in evolutionary and 'self-designing' terms often mirror concepts of cybernetic theories of self-organization (e.g., Ashby's requisite variety). The Berkeley studies and Rochlin's contribution to the present discussion will prove

influential in clarifying by empirical studies how an organization is shaped by its 'technological core' and by the degree of predictability and variance of the organizational context. The military case study clearly demonstrates how this shaping leads to the evolution of different organizational structures for coping with different problem situations even in a military organization with a strict, formal hierarchy. The important lesson to learn from the study appears to be that an organization can have very high reliability, if it is given the opportunity to evolve into a complex, dynamic overlay of several management modes and networks matching closely the requirement of the different critical task situations. Given that high reliability depends on this dynamic adaptation to the requirements of the task environment, an essential organizational problem in operating safely a plant (like a nuclear power plant or a chemical process plant) is the long periods of normal operation and low variability punctuated with rare moments of complex, dangerous disturbances. How can it be avoided that the organizational adaptation to the normal, stable condition of economic and functional pressure shapes an organization blind for the potential of high variance? Another important feature of the aircraft carrier case is the extensive redundancy implicit in the informal, operational networking, in which any individual is a member of several other overlapping structures and 'has an eye on' his neighbor's performance. In most business organizations, such redundancy signals inefficiency and, probably, would be allowed to deteriorate through the adaptive pressure of normal business, such as that described by Cramer in Section 3.2. However, the "safety circle" approach of some highly efficient Japanese businesses actually recognized the benefits and promote such overlap.

50. Given that organizational structure is shaped bottom-up by the technical core as well as top-down by management culture and values, what will be a solution to the above mentioned dilemma? Would it let the organization adapt to potential variability bottom-up by exercising variability in a proper way; or to develop new management cultures and organizational structures creating variability in normal work such as diversification and continuous change in the roles of the involved people; or a combination of both these approaches.

51. The dilemma between the stability of normal operation and the call for rapid change during emergencies is analyzed in more detail in Lanir's paper on accidents and catastrophes. Lanir sets the stage with a discussion advocating that research should "cease casting for questions and explanations in the river, bu start looking for them in the open sea" and a review of the present problems with the defence-in-depth principle and he points to the fact that failed, 'chaotic' situations in hyper-complex systems "produce not only inconceivable 'negative' surprises, but also inconceivable 'positive' surprising opportunities. These inconceivable opportunities can be explored and used to prevent catastrophe, only if the people on the spot are alert and trained for self-control activation of their initiatives, talents, expertise, and boldness," a requirement the defence-in-depth design is not supporting. He concludes in the introductory discussion that the lesson to be learned "is not about the defence-in-depth design per se, but rather more about the basic characteristics of the type of organization for which the defence-in-depth concept was intended to provide its safety mechanism--the hypercomplex organization.

52. In this context, Lanir suggests a distinction between the meanings of accident, i.e., an unfortunate event causing loss or injury resulting from fail-

ure, and of catastrophe, i.e., a case where an accident releases a chain of events that reveals inadequate model, latent organizational pathogens and improper crisis management which irreversibly multiplies the effect of accident. He warns that we "cannot reconcile ourselves to the popular notion that catastrophes are merely 'bigger' accidents." We have to accept that the ordinary way of managing people to perform safety measures are insufficient for the hypercomplex organization's safety needs. Lanir approaches the problem with long periods of normal operation punctuated with rare, hazardous situations: "Maintaining of the known and coping with the unknown are contradictory in nature. Hypercomplex organization's safety management requires coupling of the contradictions of high quality maintenance with a high quality of managing in chaos." To the question whether this is feasible, he has a basically positive answer, because he finds that organizational behavior is not only the core mechanism of latent failure and resident pathogens but also of latent repair and resident immunity. As a result of this discussion he suggests "an 'unstable system' model of safety management" in which he, in a way, elaborates and develops further the evolutionary model suggested by the study of the Berkeley group and presented in Rochlin's paper. Organizations are seen as having a 'natural' sophisticated richness of form and mechanisms of stabilization by contradictions. Even the most highly 'organized organizations tend to be only 'organized anarchies'. It is recognized that the inherent contradictions have a basic function for the organization's survivability; the contradictions are necessary to keep the organization alive and to maintain the proper mix of the modes of 'coordination by plan' and by 'feedback," mentioned in the next section by Dynes. Lanir suggests to organize safety by contradictions. This type of organization, "while seemingly unnecessary and even destructive for routine operations controlled by a well articulated central model, do have the important function of providing immunity against some of the organization's resident pathogens, and of enabling flexible shifts from situations where safety means strictly following the central control model rules, to situations when safety means confronting accidents in an environment to which the formal organizational model fails to provide a satisfying interpretation. With hypercomplex organizations, we may have reached the point where we better cease regarding safety as identical with a 'stable system,' where contradictions are supposed to be controlled and the paradoxes to be resolved, but rather an 'unstable system' where the interplay between contradictions should not only be tolerated, but encouraged."

53. From here, Lanir goes on describing his choreography of contradictions" which he finds to be able to reduce the rate of accidents as well as preventing them from developing into catastrophes. He draws on military experience including the findings of the Berkeley group and lists the following characteristics: It is rich in forms, has a basic clear pyramid of ranks, regulations, and codes of conduct. However, as Rochlin has found, the reliability of the unstable system is achieved by a dynamic flow of complex behaviors of different people and units, in different positions with different experience, seeing and judging the situation from their subjective standpoint, a system of disciplined improvisations has evolved. He quotes Weick: whenever you have what appears to be successful decentralization, if you look more closely, you will find it was always preceded by a period of intense centralization" and the right to decentralization and self-control is limited to special situations; strict standards of discipline are the indispensable other side of the safety by

self-control coin. In contrast to the strict top-down control of the industrial defence-in-depth organization, the safety concept of military organizations depends on a complex, simultaneous top-down and bottom-up network in which every order and its implementation is communicated, negotiated and cross checked. The organization is continuously evolving and learning, a state that is actually helped by the rapid turnover of military staff. In other words, Lanir suggests an extension of the evolving, high reliability organization analyzed by Rochlin et al. to also cope with rare catastrophes by finding ways to continuously exercise its capability by creating balance of suitable contradictions. More research is necessary to implement this in civilian high hazard environments.

54. The dilemma between the requirements of the normal situations and the infrequent catastrophes is also the topic of Dynes' paper on organizational adaptation to crisis. He sets out by noting that most of the time, social life is structured by habitual behavior and standardized procedures. Crises, however, require the reworking of established procedures and the creation of new means as well as organizations for carrying them out. The direction of response of groups and organizations is for certain aspects of emergent behavior to be combined with elements of routinized organizational behavior. Dynes' discussion is based on the view that the predominant type of coordination in an organization is determined by its diversity and its internal distribution of power and status (related to the bottom-up influence of technology and the top-down shaping by management attitudes, respectively). For coordination, Dynes distinguishes between, on one hand, coordination by plan (feed-forward) based on pre-established schedules and programs and, therefore depending on external control. On the other hand, coordination can take place by feedback,' depending on transmission of new information and mutual adjustment and, consequently, depending on internal control. He concludes that diversity of organizational structure and uncertainty of environment emphasize feedback coordination, while difference in power and status emphasizes coordination by plan. Dynes presents a typology of emergent behavior in a four-fold scheme characterized by regular and nonregular tasks versus old and new organizational structure. This typology has been used to analyze the patterns of variations occurring in the adaptation of bureaucratic structures to organizational stress. In general, he notes, crisis conditions cause organizational structure to move in the direction of feedback coordination, away from coordination by plan which, in turn, imply increased rate of communication and the proportion of horizontal task communication. He points to the important finding that organizational adaptation to crisis which has been traditionally described as emergent, now can be accounted for by rather standard sociological variables as being conditioned by those factors which affect coordination; structural conditions of an emergency period make for uncertainty, diversity and decreased formalization together with decentralization. This change increases communication, complexity of organization, and dependence on feedback coordination.

55. This discussion leads Dynes to his concluding paradox: Contrary to the basic requirements of organizations faced with emergency, the response to recent industrial accidents has been an increased effort by government agencies and regulatory institutions to centralize authority and formalize emergency procedures: coordination by plan is becoming normative, probably because a military model of organizational functioning in crisis is assumed to be most efficient by the planners who often have a military background. In writing,

Dynes presents his conclusion mildly--during emergency "coordination by plan is, at best, questionable."

56. The focus of the discussion so far has been the adaptation of the organizational structure taking care of work coordination to the characteristics of the task environment: In the shorter perspective, technology shapes organizational structures bottom-up. In other words, the coordination of activities in terms of structure and content of information exchange is shaped by the technology while the social organization in terms of the conventions of communication, the form of messages, is dependent on human values. On the other hand, in a longer perspective, technology is shaped to match cultural perceptions of needs and preferred modes of cooperation and social interaction. This complex interaction between technology, organization and culturally based values is likely to create conflicts when technical systems and/or management policies are transferred from one to another cultural context. This topic is discussed in the next section.

57. In this contribution, **Meshkati** advocates the development of an Integrative Model for the design of reliable technological systems. The premises of his conceptual framework match closely the adaptive organizational features discussed in the previous sections such as the response to task uncertainty and tightly coupled technology.

58. Meshkati suggests the use of an integrated model for analysis of industrial accidents as well as for design of socio-technical systems. The particular importance of Meshkati's contribution is the emphasis on the influence of the 'intended technology' and its dependence on the sociocultural setting. The core of Meshkati's contributions is his discussion of the effects of cultural variables on technological organizations and technology utilization.

59. Meshkati adopts Hofstede's operational definition of culture being "the collective mental programming of peoples' minds and reviews the recent concern for the important role of the cultural context of organizational and managerial factors in the success of technology." Cultural variables' reaction to technology is complex and is reflected through processes such as attitudes toward work, technology, organization, work habits, group dynamics, and achievement motivation. In consequence, surveys of administrative theory and practice in developing countries conclude that administrative theory developed for Western settings does not apply because it assumes contingencies that may not be valid for developing countries.

60. Management effectiveness is influenced by several factors: Management philosophy which refers to the attitude of management toward people within and outside the organization, management practices, i.e., leadership, organization building, planning, etc. and environmental conditions including socioeconomic, legal, political and general cultural factors. Hofstede has found that national cultures differ in at least four basic dimensions in the influence on operational and managerial effectiveness: power distance--the extent to which the fact is accepted that power is unequally distributed; uncertainty avoidance--the extent to which uncertainty are met by stricter rules and deviating ideas by intolerance; individualism-collectivism--which refer to the degree to which individuals are in a tight social relationship with relatives, clan, or

organization; and finally, masculinity-femininity, i.e., whether dominant values are acquisition of things and money or related to caring for people and quality of life. A determining factor or organizational success clearly will be the compatibility of the country culture and the culture within the organization along such dimensions. Great differences are found between countries. United States are individual-competitive, Japan is collateral and group cooperative, while some Latin and Middle East countries are considered to emphasize hierarchy and tradition in management. Such factors will have fundamental influence on the organization which is evolving for coping with normal operation and maintaining of complex plants which, in turn will have implications for the education of staff and the design of the interface between people and machinery as well as on the relationship between operating companies and safety authorities and society.

61. In Meshkati's paper, as it is the case in the literature in general, the cultural difference between western countries and developing countries is in focus. This is, however, not the only cultural difference of significance for safety. Also the 'cultural difference' between the technical engineering design culture and the economic, industrial operational culture is becoming to be recognized of increasing importance. When acceptability of the hazard involved in industrial activities depends on the ability to cope with rare, high-risk situations, (an ability which will not evolve during normal work but depends on a fundamental understanding of the causality of accidents as the basis of a continuous performance monitoring). The cultural difference between professions and their perception of management and organization may be as important as the difference between nations for the safety of large-scale industrial operations.

62. So far, the topic of this section has been the structure of organizations and its evolution under the influence of technology, task environment and cultural conditions, i.e., the behavior of the socio-technical system viewed from the perspective top down in the following Fishhoff as an experimental psychologist, takes a look at different approaches to integrating knowledge about the behavior and decision-making strategies of the individual into a comprehensive view of socio-technical systems; an interesting exercise in the present context aiming at the identification of promising research avenues in system safety. He identifies recent contributions to four different points of view--(a) explicit modelling of how people behave in organizational settings, in particular their limitations with respect to efficient, optimal decision making; (b) analysis of a particular organizational settings and its implications for the individual forced to make decisions within it, such as the influence of modern telecommunications on the distribution of decision-making responsibility; (c) analysis of how the interaction between the people in an organization enhances or undercuts the decision-making abilities people have when functioning alone, i.e., a reversal of the usual social science perspective; and finally, (d) he explores in more detail the fourth alternative, i.e., to extract from the research literature on individual judgements and decision-making a variety of "stylized facts" whose basic accuracy would be accepted by most investigators. He then explores what suggestions they can provide for design of more reliable socio-technical systems in terms of better interfaces and training programs, education of politicians and regulators, formulation of regulations, design of incentive systems to motivate better trade-offs between safety and productivity and, finally, for disciplining judgment in probabilistic risk analysis. In

other words, Fischhoff lists a number of basic behavioral principles to have in mind when suggesting improvements to the overall system. The discussion is given under two main headings, (i) behavioral "problems" including--hindsight bias; overconfidence; and social cognition; and (ii) behavioral realities including--semantic differences; and public perceptions of risk. Careful attention to such basic principles can serve to avoid overconfidence in rational normative models when planning improvements in organizational reliability.

3.5 Organizational Decision Making

63. The central topic of this section is how management decision making can be influenced by legal measures, and how it is affected by major accidents.

64. **Brehmer** takes examples from traffic safety to discuss the kind of decisions that should be made to promote safety. His main argument is that safety can be increased only by reinforcing safe conditions, not by penalizing accidents. He starts his argument by pointing to the fact that organizations are pursuing several different goals, of which safety is not the primary reason for the existence of an organization and he notes that no direct studies are found of decision making involving safety issues and indirect inferences must be drawn from available case studies, as for instance the evidence from Perrow's well-known analyses. An immediate observation is the fact, that safety devices are frequently used to increase productivity rather than safety. An often cited example is the effect of radar on maritime transport. Another important observation is the difference in the safety and the productivity aspects of decisions. The effect of decisions on productivity is direct and visible, whereas the effect on safety is conditional, depending on some additional unfortunate circumstances, are caused by decisions or failures of other people. In consequence, the decisions taken when weight is put on productivity will seem both rational and defendable in the situation. Correspondingly, according to recent studies decision makers who had been involved in accidents, did not see themselves to take any risks. Brehmer's conclusion is that it is futile to argue for less risk taking at any level in an organization. No level sees itself as placing anybody in any danger. Not only will management not realize that it may be creating risks, but here may not be very much pressure from below on management to change either. Consequently, one can hardly expect an organization to change behavior on its own and to weigh productivity and safety issues differently. He argues that this requires a change in the environment in which it operates, i.e., in the legal system.

65. A major problem is that it is difficult to specify what the safe conditions are, and unfortunately, the legal attention will be turned to penalizing accidents. This increases the cost of accidents to organizations, but it will not necessarily influence the basic nature of decision making concerning safety. Brehmer uses speed limits as an example to illustrate the point and concludes that to change decision making in organizations towards greater safety, we need to specify and reinforce safe conditions which, in turn, requires that safe conditions can be ascertained and communicated. In other words, the conclusions based on traffic safety support the proposal derived from control theoretic arguments in the background paper (Section 3.1).

66. Based on this discussion, Brehmer turns to a discussion of research needs. He points to three phases of most safety research with a first focus on the agent, the second on the environments of the agent, and a third, more mature phase, focusing on the interaction and he concludes: there is nothing unusual about the behaviors that lead to accidents, they are just ordinary and adaptive behaviors that meet with unusual circumstances. In research, therefore, rather than be looking for the unusual, we should understand the adaptive organizational behaviors that create risk.

67. This again puts the focus on self-organizing control and its response to variability of the environment and gives emphasis to the convergence of the conceptual framework within decision research, social science and control and systems analysis.

68. With the background of Brehmer's arguments, it is interesting to study Bowman and Kunreuther's analysis of the effect of the pressures on chemical industry following the Bhopal accident based on organizational and behavioral decision theory. The stated aim of their analysis is to find whether the heuristics and biases of individual decision makers are also affecting strategical decisions of an organization. The paper is based on a series of interviews of managers in a major chemical company and illustrates clearly how legal measures often are initiated by major accidents. This, in turn, illustrates the discussion in previous sections that feedback from accidents change the structure of a system by resetting the initial conditions of the continuing adaptation to economic and functional pressure. It also illustrates how industry acts under the device: if industry in general does not regulate, government will do it. The reset of initial condition in the particular company included a drastic decrease of the inventory of hazardous substances to avoid future worstcase scenarios together with improved inspection.

69. **Kunreuther** and **Bowman** in their analysis focus on the relation between the decision process in an organization and the firm's actual choices and they relate their findings to the work of Cyert, March and Simon, in particular to the distinction between procedural and substantial rationality. The analysis results in a number of propositions: (a) following a catastrophe, there is a tendency to ignore objective data, and to focus on the prevention of a similar accident; (b) there is a linkage of activities undertaken prior to a catastrophe with solutions following it (like Cyert and March's solutions looking for problems); (c) crisis enable organizations to exert tighter hierarchical control and to take rapid action; (d) confounding between chronic and catastrophic risk; (e) tendency to ignore costs when crisis situations appear; and (f) there is a form of organizational learning which turn tacit knowledge into organizational policy, e.g., principles for safe operation are formulated and institutionalized.

70. In this way, the paper brings an important example of an analysis of the restructuring of organizations in response to feedback from catastrophic events. It is particularly important because it relates organizational structure and response to recent organizational decision theories in a way that appears to be compatible with an overall control theoretic approach to systems analysis.

71. The topics discussed by Ostberg are focussed around the problem of high level decision makers' use of expert advice, in particular the problem of interpreting the factual information supplied by experts in a soft and ambiguous political context. His prime interest is the decision making on societal risk at the level just below government ministers and the fact that decision-making research has been taking place within several academic paradigms, none of which in separation catches the actual, complex problem which involves decision makers left with a conglomerate of incompatible arguments in the dynamic turbulence of public opinion and political issues. He finds that the decision makers' present dilemma cannot be solved merely by more information, but that, in particular, trust and confidence are key factors. In this line of reasoning, Ostberg supports the importance of communication between professional cultures, of the need of decision makers to understand the expert support they have available. In consequence, several disciplines should join in the effort to make decision support useful. Ostberg starts with the warning not to misinterpret management in terms of manipulation but to accept a neutral interpretation as it being a control function in a system including physical as well as biological and social factors. Ostberg points to the conflict between management by rules and management by objectives and gives some examples relating this difference to the distinction between normative and evolving organizations. Ostberg emphasizes the basic importance of concern and care of the individuals involved in a system under management by objectives. This is crucial for producing the drive without which no evolutionary system can thrive. Again, self organizing principles are underlying the conceptual point of view.

72. A central theme in Ostberg's paper is the relationship between the technical understanding of experts and the formal rule system of bureaucracies. A case is prepared for decision makers by civil servants. The matching of factual evidence to the rule system and criteria for decision depend on the judgment and formulation by civil servants whose responsibility and power are strictly formalized. In this matching process, decision makers, civil servants and experts are cooperating in a complex way, loose cooperation can lead to unreliable foundation for decision, tight cooperation to ambiguous responsibility relations. A number of the well known biases in decision making are then brought into relationship with this matching process, and it is concluded that more cross disciplinary understanding is needed for the integration of expertise knowledge and decision making in the public domain.

73. The trace of Ostberg is taken up from an other perspective in the next section by Baram, an attorney involved in risk management. In the paper the interaction is discussed between legal doctrines, economic factors, management systems and technical expertise. The legal frameworks are discussed in terms of national and local regulations and private law and insurance practices. He points to the fact that national laws traditionally have not intruded into the internal aspects of plant operation and management, and even when local laws include such conditions, the actual enforcement has been influenced by economic and employment problems of local governments. However, the recent development following several major accidents has made these distinctions less clear. Next, Baram takes up the discussion of risk management in this legal framework. Risk management has two objectives: to comply with regulations and to prevent losses. The target of risk management for legal compliance is explicit and, by definition, sets the upper limit for the risk that is accepted by risk

management. Loss prevention then will identify a lower level of accepted risk at the discretion of the manager, and at a cost higher than legally required. This target is determined by an evaluation of the loss potential and of the willingness to spend financial resources. The new US and EEC laws are now forcing industry to go beyond the regulatory compliance and to consider also the potential losses. Baram has analyzed the industry response to this change and found that it can be organized along two dimensions: societal views of industrial management; and traditional organizational goals. These two dimensions define a matrix which gives a good overview of the industrial responses to the recent legal pressure. Based on this structure, Baram brings some considerations of the problems of technology transfer to developing countries.

74. In the final paper of this section, **Zimmerman** completes the picture of organizational decision making by her analysis of government's role as stakeholder in industrial crisis, decision mechanisms and strategies in crisis management.

75. Zimmerman summarizes a number of factors contributing to the rise in the number of industrial crises related to managerial decision making, such as deficiencies in financial policies in both private and public sectors, inadequate administrative frameworks, and insufficient knowledge human factors. Following this, a discussion is structured along the dimensions of financial resources, administration and organization, and human resource management.

76. The ability to use financial resources hinges on three factors: the uncertainty of cost estimates in crisis management, the existing patterns for government expenditure, and strategies for financing. Discussion of these factors in light of historical evidence and rule systems contributes to the understanding of the mechanisms constraining their adaptation to the requirements of crisis.

3.6 Adapting Risk Analysis to the Needs of Risk Management

77. The questions posed to the contributors of this section were--how should current practice for risk analysis be developed in order to make the preconditions and models sufficiently explicit to be effective in risk management, and how should the analysis be documented to serve operations management?

78. The discussion in the previous section reflects a fundamental interest in understanding the mechanisms involved in safe operation of complex socio-technical systems and the origin of accidents. In this section, the concern of the contributions have shifted towards that of methodological development and design. The research on methods for predictive risk analysis is very much focused on improvement of the quality of models involved in analysis and in extending the boundary around the scope of the models. The implicit precondition of present probabilistic risk analysis appears to be that once a model has included features of the system, it is up to the system to match that particular representation. Not much interest is vested in research to see how that assumption can be realized in the actual ultimate use; i.e., the trend is to make the models as detailed and complete as presently possible with no basic discussion whether this degree of completeness and detail is the most suitable for managing the ultimate objective of namely plant safety.

79. This section is introduced by an excellent and open minded overview of the problems presently found in probabilistic risk analysis by Brown and Reeves. While the term risk management in the previous sections of the book implicitly has been related to safe management of the technical systems-as-designed through their operational life time, Brown and Reeves includes in risk management the control of safety through proper design, and, as they correctly point out, quantified risk assessment lends itself to this aspect of risk management in two important areas such as improvement of hardware and plant siting.

80. In addition to such functions during design, the authors mention that risk management must also be concerned with "practical decisions made from day to day. The most important of these decisions frequently concern the organization, preparation and deployment of personnel whether they be senior management, maintenance staff, or plant operators." For this part of risk management, which is central to the concern of the workshop, they find presently two lines of development of management techniques: (a) one is to work according to general good practice, which is acknowledged to be a 'blanket approach' which cannot point to management problems which are important to a particular plant; (b) a second approach is to engineer out human errors as much as possible. They conclude the introduction by stating the most promising area for development of risk analysis to be the linking to management actions in a way that enables plant management to rank importance of activities by their effects on plant risk. In order to do so, they find it necessary to change current approaches to both risk assessment and management.

81. The authors follow up with a survey of the problems presently found in the methods of quantified risk analysis, but the focus is clearly on the properties of risk assessment methods as a design tool, i.e., the properties for risk management through choice among alternatives in the plant conceptualization phase. The review is important for judgement of the state of the art of risk assessment as a self contained tool for effective risk management during design. This point of view,however, leads the authors to conclude that "risk assessment can be better adapted to the needs of risk management in a relatively straightforward fashion" i.e., to improve the quality of the methods as now conceived. IN conclusion, the authors support the view that improvement is necessary to make risk analysis suited for practical risk management. They focus on the important need to make risk analysis "a living document" and to improve the communication to operations management. They do not, however, consider the need of a revision of the approach to risk analysis to make the method itself more in line with the requirements of the overall control, i.e., by making the boundaries and preconditions explicit as suggested in the background paper (Section 1.1.1).

82. They acknowledge the need for research in the problem of risk management in the social context but find that differences between concepts and languages of the involved disciplines are too great and, therefore, the problem to be unlikely to be tractable to any technical solution and that research is more likely to prove fruitful if it is now focused on quite narrowly defined areas. The basic problem, discussed at the workshop, is, however, whether a more well defined tractable problem can be defined when attention is turned to structural

and relational properties of the entire system than towards isolated improvement of separate tools.

83. **Andow** contributes a second opinion about the problems and need for further development of quantified risk analysis. His discussion echoes many of the problems discussed by Brown and Reeves and together the papers give an indication of the prime research interest of the risk analysis profession to be a further refinement of the methods in terms of complexity and completeness, rather than to spend effort evaluating the weaknesses of the methods with respect to their application in the ultimate control of plant safety. The risk analysis profession appears to be preoccupied with the verification of the internal consistency and completeness of their models, rather than a validation of the ultimate application for safety control through the plant lifetime.

84. In the following short discussion statement **Swain** from his extensive experience in human reliability analysis supplements the discussion of the need to improve the methods for quantified risk analysis with respect to human reliability. In his concluding remarks, he defends the probabilistic risk analysis as if the general attitude of the workshop rejected the benefit of such analysis. This was, however, not the case, but it was argued that it is more important to make the methods useful to practical risk management than it presently is to improve the methods per se.

85. **Heising** approaches this latter problem in her brief discussion statement, advocating the view that for quantified risk analysis to be useful for risk management, we have to "change company management to fully appreciate the benefit of risk analysis, among other statistical tools." Interestingly, she points to the Japanese concept of Total Quality Control and the possible implications for risk management which is a view close to the organizational quality control mechanisms discussed in the background paper. However, she sees no need to modify risk analysis in order to improve risk management and attributes the benefit, she perceives in Japan, to the broad Japanese appreciation of statistical methods for quality control. This may not, however, be the whole secret, since the Japanese group decision making style and the joint concern with quality may facilitate the functional redundancy, Rochlin discussed in Section 3.4.

86. In the next contribution, **Nertney** turns the coin and gives a thorough discussion of the risk management problem, when viewed as a control problem in a conceptual framework very compatible with that proposed in the background paper of Rasmussen. Nertney's account, however, is based on very substantial experience from safety work at EG&G in Idaho Falls from a risk management program, based on the MORT concept-the Management Oversight and Risk Tree. This concept, in turn, was originally developed by the former chairman of the US National Safety Council, William Johnson from his life-time experience from practical safety work.

87. The main body of the contribution describes a system for analysis of events and incidents in order to identify, analyze, and measure performance indicators in such a way that they will improve the capability to predict future performance. The control view of safety requires the following functions: definition of health and safety performance requirements, measurement in terms

of appropriate indicators, comparison with requirements, detection of deviation, analyses of causal factors and, finally, corrective feedback to the system. Nertney warns that this sequence should not be taken only to represent the classical feedback mode of nulling-out undesired outputs, but includes also more advanced control paradigms for proactive (i.e., predictive) control in which feedback is made in terms of change of system structure and characteristics, as it was also discussed in Section 3.1.

88. In this conceptual framework the operations required for risk management are structured in pre planned analysis decision trees according to the MORT format to make the framework operational and to support the analyst in considering the various aspects of risks as well as of management adequately. The combination of the control paradigm and the design of decision trees of analysis based on the collective experience of EG&G and Johnson of NSC makes it a useful source of empirical information to consider in research on the structure of reliable organizations. In addition, the contribution gives good evidence of the complexity of an adequate analysis of performance indicators and its use in risk management. An obvious research topic would be to explore the possibility of integration of the organization needed for normal operation and for MORT-type analysis of operating experiences. It would be interesting to see, whether such an integration could lead to an operational simplification when implemented in a particular system, supported by the analyses and functions already in action for normal operation and planning.

89. In his contribution on risk assessment and its use in feed forward control, **Wreathall** bases his discussion on the observation from recent major accidents that the 'root causes' are found in areas like confusion, diffused and ambiguous responsibilities, etc. and asks "how do the methods of probabilistic risk assessment reflect on these elements? Wreathall concludes that in order to give the methods feed forward risk management capability, the factors needed to be addressed are: organizational factors; influence of emotional factors; and analysis of complexity of equipment and systems without the assumption that independence is the norm. One avenue of research taken in the nuclear area for extension of risk assessment is evaluation of the feasibility of "programmatic performance indicators." The program has two interesting features in the present context: the use of a process-control type of model for describing the interacting elements of an organization, and a method of identifying possible resident pathogens. The first part of this program is focused on the interaction between the maintenance and training functions in a nuclear power plant and the rest of the organization. It immediately uncovers the complexity of the interaction and the difficulty of identifying suitable probing points for the definition of performance indicators. A very interesting feature of this program appears to be its potential for describing organizational dynamics and the feedback information flow loops involved in error recovery and self-correction in a tightly coupled system (cf. Rochlin's paper in Section 3.4) together with the internal competition among different resources. The contribution of Wreathall based on a functional and structural analysis of an organization in a very fruitful way complements the picture painted by Nertney on the background of analysis of accidents and related management features.

90. **Embling** in the next section adds to the picture of risk management a description of an actual risk management system which has evolved over several

years in Australia, based on proven management techniques from military environments, "as most proven management techniques are." A 'systems approach' is taken considering simultaneously cost of preventive measures, benefits gained by involved agencies, legal aspects, procedures and practices and ergonomic factors and finally, insurance against loss and injury.

91. Risk management according to the principles described by Brown and Nertney, based on detailed analysis and quantification are effective only for particular plants and systems. For support of authorities with nationwide responsibilities for emergency management and accident mitigation, more overall methods based on general classification of risks and their potential sources and a correlation with proper countermeasures are necessary.

92. Rowe considers risk to be the downside of a game of matching outcome with possible loss and addresses risk management from a policy making point of view. In his point of view, risk analysis is a subset of decision theory and he stresses the fact that there are several different approaches to risk analysis, depending on the purpose of analysis (see the discussion in Rasmussen's note in Section 3.1).

93. In the final paper on decision analytic perspective of corporate risk management, Perdue follows up the arguments of Rowe on risk management and decision analysis. The focus of this discussion is the properties and problems of risk analysis as a one-shot decision to enter an activity or not. This unfortunately represents current narrow focus of the majority of risk analysis professionals. The continuous management of risk during operation is not considered.

94. In conclusion, it was the general position in this session, that predictive risk analysis is an important tool for the control of safety in large scale systems and it was also generally agreed that improvement of present methods and of the communication of the findings of risk analysis to operations management are important issues. The efforts of the risk analysis community appear, however, to be focused on improvement of methods for use in design of safe systems and for later acceptance of the systems in the community. Important as this may be, this line of development will not automatically lead to better overall safety control and risk management during system life time.

95. Probably, two different lines of development are needed. One for design and acceptance, striving for the best possible coverage, including operators and organizational management; and another for practical risk management, focused on explicit assumptions, reliable system models with clear boundaries not including complex and dynamically changing conditions which can be empirically controlled, when the system is in operation. This latter line of development is, at present, not very visible from the presentations at the workshop. One reason may be that the first mentioned line of development can take place more or less within an established profession, while the latter requires the establishment of new, cross-disciplinary research relations.

3.7 Decision Support for Safety Control.

96. Given that individual and organizational adaptation to changes in the environment is necessary, how can conscious consideration of safety preconditions which are not an explicit part of the 'gestalt' of the present tasks be secured? Some ideas were proposed in the discussion now, namely-- (a) procedural training; (b) basic system understanding; and (c) making boundaries visible by means of advice giving systems.

97. The topic of this session is a discussion of the state of the art of decision support systems and the potential for improved risk management.

98. **Rouse** sets the stage outlining a basic philosophy for design of decision support systems; people are in the systems to make decisions and to cope with ambiguities. Consequently, Rouse argues, the aim is not to make decisions for people, to automate, but to design systems that provide information, tools, and environments that will enable people to make better decisions. He then distinguishes between three kinds of decision situations: familiar and frequent; familiar and infrequent; and, finally, unfamiliar and infrequent and he finds the latter to pose a dilemma for decision makers which is becoming increasingly characteristic of large-scale, integrated systems. Finally, he defines the role of humans in large-scale systems which is to exercise judgement and creativity and to accept responsibility. He underlines the importance of the human ability to accept responsibility and to find innovative ways to fulfill responsibility when things go wrong. He is concerned that the complexity and technology associated with large-scale systems will lead the people involved to loose the feeling of responsibility and to perceive the system as being in charge. From this argument, Rouse derives the basic design philosophy that the purpose of the people in the system is not to staff the system--on the contrary, the purpose of the system is to support people in achieving their objectives. "The purpose of a power plant is to assist the people involved in supplying power to the community." This philosophy leads to three primary design goals for decision support systems: To help people to overcome their limitations, to enhance their abilities, and to foster user acceptance. Finally, Rouse reviews design concepts for intelligent interfaces, information systems, and integrated support systems. He concludes that society at present seems to be reacting to crisis rather than anticipating problems. It has difficulty in investing early and, therefore, usually has to pay much more later and, finally, it is not prone to long term investment but seeks quick fixes. If we, in the present context, want a quantum leap of improvement, we need planning, prudence, and persistence.

99. **Pew** continues this discussion of the design of decision support systems, by pointing to the usefulness of models of human decision making for identifying features of decision making scenarios. The approach taken is based on a description of decision scenarios not only by scripts but also by sets of goals and subgoals until a level of detail is reached where timing and work load conflicts can be identified and analyzed experimentally. Interestingly, Pew points to the possibility of using expert system techniques to prompt decision makers to seek proper information and, finally, he points to the value of the experimental approach to evaluate problems in transfer of technology to developing countries.

100. The following paper by Fussell presents a particular decision support system which is of particular interest to the workshop, in being an attempt to use a formal quantified risk analysis as the basis of a risk management tool for plant operation in nuclear power. The introduction to Fussell's paper touches on several basic issues of the workshop: "Information from probabilistic risk assessments can be used to make decisions that limit or reduce the risk associated with the operation of nuclear power plants; however, to date there have been few formal attempts to use such analysis for decision making purposes. One reason for this is that PA 1/ reports mix useful results with a great deal of information that is irrelevant to decision makers. Another reason is that these reports are understood only by those who are well versed in PSA methodology."

101. The paper describes a personal computer based system that makes information from risk analysis available to plant managers in a way that matches their immediate needs. The program meets the criteria posed by Rouse; not solving the problem for a manager, but presenting him with useful timely information. The tool is intended to support operations personnel (in control rooms and maintenance as well as managers). The system is based on an on-line fault-tree event tree analysis which makes it possible for the decision maker to ask "what-if" questions. Operators can use it to explore the safety implications of removing specific equipment from service for testing or maintenance at a particular time and managers to identify beneficial changes to procedures or equipment. Based on the plant and risk model, the program calculates the decrement in a safety index in consequence to planned reconfigurations of the plant and makes it immediately possible for a decision maker to see the consequences of intended actions and to examine the effect of hypothetical maintenance schedules.

102. Fussell's contribution is very significant in demonstrating the effort and equipment necessary for creating realistic management support systems to increase the visibility of the boundaries of safe operation.

103. One important problem of application surfaced during the discussion and is the topic of Fussell's appended note. The system was contracted for development by an authority to be used for inspection purposes to judge implication of safety violations on site, but was not approved for operations purposes, because operations management is not supposed to operate with decreased levels of safety. This illustrates well the situation when an improved safety technology comes into conflict with established regulations, which acts to impede progress. A similar situation can be expected when, as it has been proposed, regulatory technical specifications of accepted operation of today are implemented in an on-line interlock computer system shutting down the plant in case of violation. It is very likely that plant availability will decrease considerably, unless the specifications stated in regulation are redesigned for such new implementation.

1/ PSA - Probabilistic Safety Analysis.

104. When designing decision support systems, user acceptance and trust become critical issues, and are the topics discussed by Sheridan and Moray in the following sections.

105. **Sheridan** takes up in a short discussion note the importance for any advice giving systems, and points to the fact that trust also have a negative side--too much trust is as fatal as no trust.

106. **Moray** continues Sheridan's discussion of the human side of computer assisted decision making. He mentions several important conditions for the use of decision support systems. First, he warns, decision makers have to realize that they have a problem in order to consult a support system at all. This is, however, not only a problem of computer based support systems, but even with manuals and guidelines, effective use will require some kind of 'prompting' system. Human factors specialists have for half a century complained that designers do not even use existing HF guidelines. Moreover, in this case, the basic problem is caused by a feature of decision making stressed by Moray, namely--you only seek support when you realize a situation of choice which, very often, only uncovers itself too late. In this way, the suggestion by Rasmussen in Section 3.1--i.e., to run an on-line risk analysis as a background 'spell-checker' during maintenance and operations planning, is supported by Moray's concern.

107. Furthermore, Moray suspects that decision aids are needed precisely during those situations when predictive models are most unreliable. This warning, however, can be countered, considering that decision aids can not only support the decision process itself by predictive models for testing hypotheses, but also the basis of choice providing by a more 'neutral' presentation of available alternatives for action. This helps to avoid the 'I should have known' situation. During normal work situations, there are normally only a small set of alternatives for action in the context given and only little information is needed for resolving the choice. In unusual situations, however, wider alternatives should be considered and can be displayed for hypothesis generation, while the choice or decision is left to the human. This reflects Rouse's plea of leaving responsibility to the human.

108. Next, an analysis is given of the question whether a decision support system can have at all an adequate knowledge about the system, including knowledge about inconceivable events.' Predictive models of system behavior in such cases will be unreliable and should be used with great care. It is, as mentioned, also possible to support decision making by displaying knowledge about alternatives derived from the design basis, such as reasons for the presence of equipment and functions and alternative means of control. Moray in this context warns that knowledge acquisition for expert systems today is a doubtful enterprise. This is very true, if experts in this case are considered expert operators. However, if the task of operators during abnormal conditions is taken to be an extension of the design task, i.e., to redesign control strategies to match unforeseen plant conditions, the expert knowledge required will be the knowledge of designers about the functional design basis, which can be more readily formulated than can expert operators' heuristics. Moray mentions a problem which is important even in this context, namely that advanced systems are not stable; rules and regulations change, equipment is modified and

upgraded. He poses the question--how can up-date of expert systems be guaranteed? This question will be particularly important when the socio-technical systems have the 'self-designing properties discussed in Section 3.4. It is interesting again to note a psychologist citing control theoretic sources such as Ashby.

109. Finally Moray takes up the discussion of advice acceptance. He suggests two axioms about human behavior which are crucial in the present context--(a) most people prefer to make a wrong decision without help rather than a right decision with help; and (b) most people will accept only advice if it agrees with what they have already decided. These features of acceptance again underlines the importance of displaying for the decision maker the alternative choices, prior to the actual decision.

110. Moray gives the crucial problem a very clear formulation--to find the balance between the danger to reject a good advice and the danger of refusing to reject a bad advice. The key to this dilemma is trust, he states and discusses a number of attributes of trust similar to those mentioned by Sheridan. Overall Moray is "not very sanguine about the extent to which decision aids will reduce risk in real time dynamic decision making." He qualifies this statement further: "In general accidents happen because there is neither enough information, nor enough time, nor adequate will. Decision aids cannot guarantee to overcome any, let alone all, of these." In this conclusion, Moray does not seem to consider the use of decision support during normal operation and maintenance in order to avoid violation of the obscure boundaries of safety operation as suggested in Rasmussen background paper, which will help to decrease the likelihood of ending up in a complex decision situation under time pressure, to which Moray is referring All the arguments of Moray seem to stress the importance of such an "on-line" approach in addition to his proposal of using decision aids "at the upper, strategic planning levels."

111. He suggests that we should not be obsessed with the management of error and omit the study of the natural history, psychology and prevention of error and he brings forward a well thought out proposal for research to reach a predictive model of human error mechanisms. It can, however, be questioned whether a program to study behavior fragments defined to be "errors" is the most fruitful path to take, considering that Reason's important discussion of violation and Rasmussen's emphasis on the role of "error" in adaptation, indicate that errors cannot be defined locally, but have 'systemic' roots.

112. What Moray suggests, however, is an ambitious experimental psychological laboratory, a production facility under commercial conditions, for development of predictive models of human behavior which can contribute to our understanding far beyond error situations. He suggests an experimental facility with 'employees' rather than 'subjects' in order to take into account the fact that studies of actual, professional work behavior requires very long training periods to include the facets of expert skill. What he proposes under the name of "Institute for the Study of Error" is, or should, in fact, be an "Institute for Study of Behavior in Work."

113. Another approach to the development of predictive models of human behavior is presented by Woods based on his extensive studies of human problem-

solving behavior during plant emergencies in the nuclear power field. He considers a socio-technical systems under disturbances to be problem-solving systems and he asks two basic questions--what are difficult problems; and how do changes in the machine portion of the system affect performance of the overall system? He suggests a simulation facility based on artificial intelligence tools to translate the problem from the actual work domain language into the language of problem-solving, and into information processing terminology. Such a simulation can support investigation of how changes in an incident, e.g., obscuring evidence, including other failures, affect the difficulty of the problem analysis for a given set of knowledge resources on the part of the problem-solver. He then illustrates from empirical evidence how changes in a man-machine system affects performance. He concludes, as did Moray, that fundamental understanding of the mechanisms of human behavior is crucial and, since models and tools are in an early stage of development, increased effort is necessary for improvement of decision making during accident situations. Again, one could conclude that, at present, the odds for preventing systems getting into accident situation are better than for supporting problem solving during accidents.

3.8 A Cross Disciplinary Discipline?

114. A topic of some concern during the workshop sessions and coffee breaks was the cross disciplinary nature of a system-oriented approach to risk management and safety control. Do we need a new profession to cope with risk management in advanced, large scale systems? In this chapter we bring as a kind of epilogue a paper by **Livingston** discussing the problems and snares embedded in an interdisciplinary field. The basic attitude behind the World Bank series of workshops has been not to argue for the creation of a new discipline but to create a cross-disciplinary marketplace where professionals of various disciplines can meet and create a common currency for exchange of problems, ideas, and methods. We really feel acquaintance with Livingston's pessimism from the past, but we also find that recent developments within approaches to serious study of complex, real life work environments, and the increasing acceptance of analysis of cognitive, i.e., mental processes and phenomena, brings with them a new perspective which has to be explored in a cooperation between professionals from several disciplines. One of the crucial problems we face will be that research in this cross-disciplinary area requires knowledge of real life work domains, attack on the established research paradigms, and funding during an extended period of time before results can be expected, neither of which are promising for a funding body or a young researcher looking for quick brownie-points in a PhD research program.

4. CONCLUSIONS AND RECOMMENDATIONS

115. At the final session, the general chairman of the workshop, Peter Benton, General Director of the British Institute of Management presented his perception of the discussions of the workshop and proposed a communique to convey the conclusion that safety is a management problem and that assistance to managers to operate efficiently and effectively with a visible boundary to the preconditions of safety would enhance their level of control and prevent safety becoming a secondary issue. In contrast, safe operation will in the long run mean efficient operation. The proposed communique was subject to some debate at the final workshop session and has been commented on by several participants after the workshop. The following wording takes into consideration the comments received and is found by the authors to be a fair conclusion of the discussions and the proposals for priority research areas:

- The increasing scale, complexity, and technological sophistication of man-made systems have raised serious concern with regard to the potential for future large-scale accidents.

- There is additional concern that the historical record of safety has little predictive value for empirical control of safety as the complexity, scale, and rate of change of technical systems are steadily increasing and as such systems are introduced into regions or countries with different work traditions, education, infrastructure, and general cultural background.

- The workshop participants agreed that a cross-disciplinary approach to safety research including contributions from such disciplines as--psychology, organization and management, decision theory, control and system theory, and engineering design (including risk analysis) is becoming increasingly realistic and with considerable potential.

- Results from particular industries and specific research projects together with results of recent analysis of major accidents indicate that success and failure in specific situations may be generalizable into a more comprehensive approach to risk management and safety control.

- Avoidance of large-scale accidents is not only a matter of protection of humans and their environment, but also carries with it immediate economic benefits that are frequently undervalued. Top management needs to see and needs to be given the means to see, that these benefits are not sacrificed in the pursuit of short sighted economic or competitive gains.

- The general concern with serious accidents needs to be extended to include such nonlethal systems which are critical for the functioning of modern society, as telecommunications, financial dealing and trading systems, integrated information systems and computing systems.

- The workshop concluded that this first meeting showed considerable promise for a continued exploration of new cross-disciplinary and

interdisciplinary activities. An important fact is, that many of these areas have generally fallen outside of traditional disciplinary lines of research and the concerns of funding bodies.

- o In particular, the following areas of research and study were identified as among those that might provide valuable insights, methods, and techniques:

  (a) The reliability characteristics of organizations evolving in response to requirements and constraints posed by their technological core and the institutional management policy. In particular organizations that expand in scale and tight coupling with technology.

  (b) Conditions in and around the edge of errors and accidents and efforts to make the edges visible to decision makers, including--the interrelationships of latent causalities; long term causal chains (resident pathogens); and the gradual erosion of safety measures.

  (c) Means of supporting decision making and management as systems drive toward the edge of safe performance, including organizational and psychological techniques as well as the use of modern information technology, to make information from design and risk analysis available to decision makers.

  (d) Better understanding, for specific countries of the characteristics of their education, infrastructure, and cultural conditions, and their implications for safe operations of transferred large-scale systems.

- o There is general understanding that early and substantial progress in the management of risk and the modalities of safety is required to avoid future accidents in technological systems whose growth in scale and complexity presents growing threats to life, the environment, and to economic progress. The workshop concluded that, while further meetings were required to continue to explore the prospects and techniques for avoiding future large-scale accidents, the perceived convergence of several disciplines represented, and the potential for transfer of presently effective safety techniques, gave grounds for cautious optimism that such progress is not beyond our means.

116. This general conclusion of the workshop supports the aim of the World Bank to reach the formulation of guidelines for menaging the hazards involved in the exploitation of modern technology. The following workshops will be directed towards such a formulation and an identification of the research and development necessary to pursue this goal. In support of the preparation for the future discussions, some comments on the likely structure of a framework for guidelines can be derived from the present workshop.

5. FRAMEWORK FOR THE DEVELOPMENT OF GUIDELINES

117. First of all, an important issue is that the total system involved in the safe operation of large scale systems should be considered in the design of guidelines. Ideally, the time is past when separate teams and organizations were involved in design, construction and operation of technical installations. Due to the rapid technical development and the very dynamic environment of companies and organizations in terms of changing market conditions as well as regulatory requirements there is an increasingly tight relationship between these bodies. In consequence, guidelines for the various parties should be interrelated and coordinated. From the common threads running through the contributions to the workshop, some preliminary outlines of a system of guidelines can be proposed for consideration. The discussion is by no means intended to be complete, it is only meant as a focus of the formulation of topics to be discussed and refined at the subsequent workshop in Sweden.

118. The parties involved in the management of safety are concerned with the following functions: (a) system design; (b) risk assessment; (c) operations and risk management; (d) regulation; and (e) inspection and audit.

119. First of all, analysis of the overall structure of the entire system from a systems point of view will be necessary to identify weak elements and relations in the control of safety. Such considerations will be important for judging priority of the various topics considered for guideline development.

5.1 System Design

120. For system design, it will be important that guidelines reflect the fact the design task in modern technology is not completed when a system is put into operation. On the contrary, the design task will continue through operation, because system configuration, equipment, and procedures will be updated in response to changes in system environment, to disturbances, and to changes in technology which have not been foreseen in the initial design. Consequently, better guidelines in recording and communication of information about the design basis to the operations management and staff are needed.

121. In particular, when design philosophies such as the defence-in-depth philosophy is applied, guidelines are needed to the effect that boundaries of the safety preconditions are made visible to operations management by adequate system design and communication of design basis.

122. When modern information technology, for instance implemented in the form of expert systems, are used as a means of communicating design information to the operations staff and management, guidelines to ensure system reliability and trustworthiness are needed for high hazard, large-scale systems. Explicit and separate consideration of guidelines are needed for systems intended to communicate neutral information about the design basis, and for those intended to give advice based on the designer's predictions of problem solutions.

123. Finally, when large scale, high hazard systems are based on 'feedforward' control of safety by means of probabilistic risk analysis,

guidelines are needed to constrain design to those system configurations and operation philosophies that are accessible to consistent risk analysis, i.e., guidelines for design according to some criteria of 'analyzability.'

5.2 Risk Analysis

124. Risk analysis is by now a well developed technique and its professional community is primarily involved in application and refinement of the tools. From an overall safety point of view, guidelines for risk analysis are needed to make such analysis useful for operations and risk management, with respect to identification of the boundary of safe operation and establishing terms of reference for monitoring operations and maintenance performance. Similarly, the potential of probabilistic risk analysis to serve as a basis for development of guidelines for inspection and safety audit systems should be systematically exploited.

125. The development of a coordinated set of guidelines for these design and analysis aspects is a very realistic endeavor, given the present state of the art. For the following aspects, however, more research is needed to establish the basis for guidelines.

5.3 Operations and Risk Management

126. At present, it appears to be realistic to formulate guidelines for the application of the results of risk analysis for improved operations management. This will require a coordinated effort for a proper formulation and communication of the results of risk analysis and for developing means to introduce them into operation management practice.

127. In addition, for operations and risk management guidelines are needed for design and maintenance of organizations able to cope satisfactorily with operation of high hazard systems based on feedforward safety control derived from probabilistic risk analysis.

128. From the discussion at the workshop, an interesting juxtaposition can be proposed of the aspects normally related to installations based on the 'defence-in-depth philosophy such as nuclear power plants and to high reliability organizations', such as air traffic control systems discussed in Section 3.4; a comparison of which can identify important topics to consider for guidelines. In nuclear power plant operation, the individual person is generally considered inherently unreliable and, in the usual human reliability analysis, will be assigned error rates in the range of 10^{-1} to 10^{-3} per opportunity. On the other hand, in the context of air traffic control and flight deck operations on air craft carriers, studied by the Berkeley group, the reliability of a group, without the protection of the activity by automatic safety functions, can reach the level of ultimate system failure in the range 10^{-7} per opportunity. This indicates a very effective error recovery in some types of organization, even without the protection from automatic systems. It appears, that very high reliability can be reached in an organization which, during the normal function, operates on the boundary to loss of control, i.e., when people are involved in a dynamic and continuous interaction with the hazard in a reversible mode of control. In defence-in-depth systems, people are not in

contact with the boundaries to loss of control during normal operation and dynamic interaction with the boundaries only takes place during rare situations which cannot be assumed to be reversible. It is probably essential that actors maintain 'contact' with hazards so as to be familiar with the boundary to loss of control and to learn to recover. In 'safe' systems, in which the margins between 'normal operation' and loss of control are made as wide as possible, odds are that actors will still explore the boundaries which then may be more abrupt and irreversible. When radar was introduced to increase safety at sea, the result was not increased safety but more efficient transportation under bad weather conditions. Two basic research questions are--how can boundaries of acceptable performance be established that will give feedback in a reversible way, i.e., absorb violations in a mode of graceful degradation of the opportunity for recovery: and what are the implications for guidelines to organizational design for defence-in-depth systems?

129. It is, however, a research issue to establish the basis for guidelines for organizational design; an issue which will be analyzed further in a forthcoming workshop. However, it appears to be realistic at present to formulate guidelines to apply the results of risk analysis and the preconditions for safe operation

130. Furthermore, in the reliable systems studied by the Berkeley group, activity in hazardous operations depends on an informal, flexible organization which cuts across the formal command structure. The flexibility of this informal organization serves a mode of operational redundancy and mutual monitoring which monitors the likelihood of an upcoming loss of control in a very effective way and supports the recovery from such loss of control. In contrast, in the 'defence-in-depth case, normal operation depend on a very formal, hierarchical organization matching requirements for efficient operation with little 'inefficient' staff redundancy and, consequently, have very limited flexibility. This is also the case for the emergency situations which are highly structured by means of formal instructions and procedures covering predicted hazards. Formal organizations, work instructions, and even the informal 'normal practice' evolving in stable, mature organizations all serve to limit the degrees of freedom of people. In order to respond effectively to the requirements to unpredictable emergencies, perception of the actually available degrees of freedom and skill in using them are crucial for the individual and for the team. A very important question for the development of guidelines for organizational design in high hazard systems is, therefore, whether in the future more concern would be directed toward the exploitation of the properties of flexible, informal organizations also for high hazard industrial defence-in-depth systems. To resolve this question, more research is needed and an important topic to explore at the next workshop will be the directions and opportunities for fruitful research in this area. The conclusions of the workshop strongly support the hypothesis that the present industrial management structure and practice have not kept pace with the technological development and that a focused effort to formulate the necessary change in terms of well founded guidelines is well timed.

5.4 Regulation

131. During the workshop and in the contributed papers focus has been mainly on the organizational level. It should, however, be considered when applying a systems view on safety control, that "control loops" at several levels of the hierarchy of risk management are effective, stretching from an individual worker at the lowest to global regions at the highest level (see figure 4 of the background paper Section 1.1.1). Different mechanisms of control are appropriate at the different levels such as the use of risk assessment, regulations, and international directives (e.g., EEC directives). The critical issues associated with risk management at the national and international level include the political nature of risk in democratic governments--who decides and how are decisions made; governmental organization of risk management; voluntary bodies compliance (e.g., Society for Risk Limitation) vs insurance companies (e.g., Lloyds). International issues would include the influence of cultural differences, feasibility of risk harmonization, impact or risk management on economic growth, and how standards may be implemented consistently.

132. In the past, regulation invariably has reacted to the particular patterns of the latest accident to make sure this will not be repeated. This would probably not be the case anyway. If the adaptive nature of working organizations is considered, it can be difficult to identify the parameters which are sensitive to attempts to change an organization toward safer performance. Changes in terms of reactions to the cause of the latest accident may very well turn out to be changes within the closed loop of organizational adaptation and, consequently, will be cancelled by further adaptation.

133. In consequence, work is necessary to develop guidelines for the analysis of accidents, not only to locate responsibility, but also to identify higher level properties of the system which are actually sensitive to change. This topic will be considered explicitly at the next workshop.

134. Furthermore, the reaction of the regulatory and legal system to accidents in general has been to remove degrees of freedom, i.e., to formalize organizations and to impose certain ways of doing things in high hazard systems. This approach can very well be counter productive in the light of the discussion in the previous section. Concurrently, with the research to identify the properties of reliable organizations and the exploration whether it will be possible to suggest the outline of design guidelines, it will be necessary to analyze the role of regulations and laws in the evolution of the organization operating hazardous systems. Discussion of the present coping systems and law complexes, therefore, will be key topics of the subsequent workshop.

135. An additional topic to consider for planning of regulatory systems has been identified during the discussions and should be briefly mentioned. Regulations tend to focus on normative procedures and technical detail, not on the structural properties of the total system and, therefore, is biased by and tied to the established technological basis of systems and modes of organization and management. An interesting example that came up in the first workshop is the conflict between the implicit intent of regulations and their explicit wording which is uncovered when they are taken literally as implemented in

automatic interlock and decision support systems. An important area of investigation is the question of developing guidelines for ensuring the adaptability of legal systems and authority regulations to a rapidly changing information technology.

136. Concluding, it should be mentioned that practice with respect to normative regulations differ between countries, and the problem mentioned with strict normative rules under technological changes, in some countries (e.g., England) appears to eased by the interpretation that "risk should be kept as low as reasonably practicable, " leaving it to the responsibility of a particular plant management to understand interpret aspects peculiar to the plant in a particular situation. On the whole, the question on regulation and the technological pace of change is a topic worth further consideration.

5.5 Inspection and Audit

137. In order to assure operation complying with the design basis and with regulation, reliable inspection and audit mechanisms are vital at all the levels of the safety control process discussed in the previous paragraph. In addition to laws and regulations, important reference information for inspection and audit are to be found in the preconditions and assumptions underlying predictive risk analysis which can serve to make inspection much more penetrating and focused than inspection based on general good practice and industry standards. Guidelines for the use of risk analysis for planning audit sessions is an important topic of development.

5.6 Conclusion

138. The conclusion of this overview of the volume will be that the rapid trend in the technological development now calls for a fresh view on risk management and safety control in large-scale hazardous systems but, fortunately, several concurrent trends in the relevant areas of research appear to be able to support our understanding of large scale, complex systems and, potentially, to give a basis for guidelines toward improved safety, if properly explored.