AN ABSTRACT OF THE THESIS OF

Esteban L. Biondi for the degree of Master of Ocean Engineering in Ocean Engineering presented on October 22, 1998. Title: Organizational Factors in the Reliability Assessment of Offshore Systems.

Redacted for privacy

Abstract approved: _____

Solomon C. S. Yim

The reliability of ocean systems is dependent on organizational factors. It has been shown that low probability / high consequence system failures are overwhelmingly induced by organizational factors. However, no methodology is yet widely accepted for the evaluation of this phenomenon or its accurate quantification.

A qualitative complementary approach is proposed based on the CANL (Complex Adaptive Non-Linear) model. In the first part, the understanding of organizational processes that affect reliability is sought. The approach is applied to several case studies based on published information: the "Story of a Platform Audit" (where no failure occurred) and some offshore accidents. A methodology is proposed to complement regular safety audit procedures. The approach is shown useful also to improve post-mortem investigations.

In the second part, quantitative probabilistic formulations are revised, based on the understanding obtained through the previous approach. Some of the limitations of these quantitative methods are pointed out. The Reliability State of an Organization is defined and a ranking for its evaluation is proposed. Preliminary guidelines are presented for the use of this approach as a framework to identify suitable quantitative methods for a given case.

The use of a qualitative approach is demonstrated. A different insight into organizational factors is achieved based on a disciplined approach that relies on experience. Significant conclusions regarding quantitative methods, their limitations and appropriate use, are obtained.

Organizational Factors in the Reliability Assessment of Offshore Systems

by

Esteban L. Biondi

A THESIS

submitted to

Oregon State University

In partial fulfillment of
the requirements for the
degree of

Master of Ocean Engineering

Presented October 22, 1998
Commencement June 1999

Master of Ocean Engineering thesis of Esteban L. Biondi presented on October 22, 1998

APPROVED:

Redacted for privacy

Co-Major Professor, representing Ocean Engineering

Redacted for privacy

Co-Major Professor, representing Ocean Engineering

Redacted for privacy

Chair of Department of Civil, Construction and Environmental Engineering

Redacted for privacy

Dean of Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Redacted for privacy

Esteban L. Biondi, Author

ACKNOWLEDGEMENT

I appreciate the trust and support of my academic advisor Professor Solomon C. S. Yim. He accepted this topic and its non-traditional approach and encouraged me to pursue my ideas.

Professor David A. Bella's research and teaching provided a fundamental disciplined approach that constituted one of the reasons for this research. I appreciate all the time he dedicated to discussions and reflection on this subject and his always-encouraging comments.

I specially thank Professor Robert G. Bea (University of California at Berkeley), for the background material he furnished, his insightful comments and his encouraging remarks. His "Story of a Platform Audit" is an outstanding piece of engineering literature, which provided the other fundamental reason for this research.

Several other professors and fellow students at Oregon State University contributed spending their time in fruitful conversations about my project. Among others, I particularly thank Colin B. Brown (Courtesy Professor, Civil, Construction and Environmental Engineering) for his valuable comments and suggestions in the later stages of this work. Kenneth H. Funk II (Assistant Professor, Industrial and Manufacturing Engineering) and Jonathan King (Associate Professor, Management, Marketing and International Business) contributed with helpful early comments. Students of courses and seminars directed by Prof. D. Bella, J. King, and Thomas Miller (Civil Engineering) listened to presentations on diferent aspects of this research and raised interesting questions. Marcela Brugnach (Ph.D. student, Forest Sciences) borne several discussions about modeling of complex systems.

While this report is the result of research with no specific funding, my program of study at Oregon State University was supported financially by the Fulbright Program, Oregon State University International Cultural Service Program and Oregon Laurel's Supplementary Award. I greatly acknowledge all the people involved in them for the extraordinary educational experience they allowed for me and my family. None of these could have happened without the trust of the Fulbright Commission of Argentina.

Berenice, my wife, and Agustín, our son, shared very close to me all the joy and sacrifices of this process. The rest of our families did so from far away. I hope my actions can tell them all how much I thank them and I love them.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

Page

PART II

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF FIGURES (Continued)

LIST OF TABLES

LIST OF APPENDIX FIGURES

LIST OF ACRONYMS

ALARA	As Low as Reasonably Attainable
ALARP	As Low as Reasonably Practicable
CANL	Complex Adaptive Non-Linear (model, approach)
CPG	Candidate Parameter Group
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
GBS	Gravity Based Structure
GEMS	Generic Error Modeling System
HEP	Human Error Probability
HOF	Human and Organizational Factors
HRA	Human Reliability Assessment
HRO	High Reliability Organization
IAEA	International Atomic Energy Agency
IDA	Influence Diagram Analysis
NRC	U.S. Nuclear Regulatory Commission
INSAG	International Nuclear Safety Advisory Group
LP/HC	Low Probability / High Consequence (failure, event)
MCS	Minimal Cut Set
NPP	Nuclear Power Plant
NTSB	U.S. National Transportation Safety Board
OIM	Offshore Installation Manager

LIST OF ACRONYMS (Continued)

PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
QRA	Quantified Risk Analysis
SAM	System-Action-Management (method)
SLI	Success Likelihood Index
WPAM	Work Process Analysis Method

Para Berenice y Agustín

PREFACE

I was aware of Prof. David A. Bella's writings when I first read the "Story of a Platform Audit" by Robert G. Bea. I took the paper to Prof. Bella for his opinion about the possible application of his approach to that case. He was delighted by the idea and encouraged me to do so. Prof. Bea immediately assisted me with background material. This work became a permanent topic of conversation with Prof. Bella from then on.

I thought I would like this work included somehow in my thesis about Reliability. I made sure my academic advisor Prof. Solomon C. S. Yim knew about my intention.

Later, Prof. Yim gave me the opportunity to expand the original work into the main topic of my thesis. Maybe I was waiting for that. Prof. Bea was again very supportive and encouraging. Prof. Bella became even more enthusiastic about the project.

What follows is the result of my work and the interactions with many people after this combination of events.

ORGANIZATIONAL FACTORS IN THE RELIABILITY ASSESSMENT OF OFFSHORE SYSTEMS

1. INTRODUCTION

1.1 Problem Definition

The reliability of an engineering system is a measure of the likelihood that it will perform as intended. It is the "probability of no failure" (Ang and Tang 1975). In terms of probability, it is the complement of its probability of failure and can be represented analytically as $R = 1 - P_f$; where R is the reliability and P_f the probability of failure. Therefore R is a number between 0 and 1.

Failure is defined as a condition of insufficient quality of the output. Failure is "an undesirable and unanticipated outcome; the lack of meeting expected performance" (Bea 1994). Safety is "a state of being free of undesirable and hazardous situations" (Bea 1994). Safety implies a minimum probability of failure and the actual lack of failures during a stretch of time. The concept of risk involves both the probability of failure and the consequences of the failure. It is defined as the product of the probability of failure and a quantified measure of the consequences of the failure.

Ocean systems, such as offshore oil platforms, are complex physical systems designed, constructed, operated and decommissioned through large and complex organizations. The physical system is comprised of a structural system (the platform itself) and interconnected mechanical systems (piping systems, oil and gas processing systems, personnel transportation systems, safety systems, etc.), all with significant spatial constraints, and operating in a harsh environment. Individuals act directly into the physical system (design, construction, operation, maintenance, etc.) or into the organization itself (managers' decisions, operators' reports, supervisors' assessments, etc.). Given the large scale of this enterprise, many individuals of

several organizations participate in each stage of the life cycle of the physical system.

Individuals, following a prescribed set of rules or procedures, operate the physical components. The environment influences the technological system and its components, both physical and human. The physical and organizational subsystems are strongly interconnected at several levels. The outcome of the system is influenced by its components and their interactions. In other words, "...the performance of a highly complex socio-technical system is dependent upon the interaction of technical, human, social, organizational, managerial and environmental elements..." (Gordon 1998).

Ocean systems can be characterized as complex technological (also called socio-technical) systems. They are comprised of two different natures: physical and human. Components are many and closely interrelated in multiple ways. Some components of the technological system respond following only laws of physics, while other components are human beings with a much more complex input into the system. Physical components are organized into structural and mechanical subsystems, and human components into human organizational subsystems. Subsystems of both natures are closely interconnected.

Technological systems have non-linear, dynamic and organic behavior. Physical components may have non-linear responses, especially under extreme conditions, but physical systems may also have non-linear responses when they have many components and subsystems highly interconnected. Behaviors of human individuals and organizational systems are inherently "non-linear". Physical subsystems may be changed, adapted or expanded with time. Organizational subsystems are always dynamical and evolving in an adaptive way, either progressing or decaying. Physical systems are mechanic, organizational systems are organic.

Historically, the first approach to the assessment of the reliability of technological systems focused only on the physical subsystems. Later, errors of

individuals were identified as a significant factor affecting the probability of failure. Reason (1990a) states:

> *The shifting preoccupations of reliability specialists [were]: an initial concern with defending against [physical] component failures, then an increasing awareness of the potential of active human errors, and now, in the last few years, a growing realization that the prime cause of accidents are often present within systems long before an accident sequence begins.*

Nowadays it is recognized that human organizational systems play a significant role in the reliability of the technological system. In the case of ocean systems, it has been identified that human and organizational factors are involved in more than 80% of system failures (Bea 1994). Moreover, individual human errors do not constitute the main cause of catastrophic system failures since more than 80% of the failures were identified to be contributed and compounded by organizations rather than individuals (Bea 1996). For other technological systems, Hollnagel (1993) estimates that the contribution of human errors (including operation, design and maintenance) to system failures is nowadays accepted to be in the order of 80%. Factors beyond the probability of failure of physical components and the probability of isolated errors of operators do significantly affect the reliability of technological systems. And these factors, rooted in organizations, usually become necessary underlying conditions for system failures.

Reliability is an engineering property of a technological system. Experience indicates (Bea 1996), and the literature in different fields reveals (e.g. Reason 1990a, Roberts 1993, Basra and Kiwan 1998, Embrey 1992, Goldfeiz and Mosleh 1996, Apostolakis *et al* 1993, Bea 1994, Hurst *et al* 1990, Gordon 1998), that human components and the organizational subsystems have to be considered in order to evaluate the reliability of a technological system. This is still an active area of research, since neither theoretical approaches nor practical methodologies are yet accepted widely to deal successfully with this problem.

This work focuses on the organizational aspects that influence the reliability of offshore systems.

1.2 Approach

1.2.1 Interdisciplinary Basis for Engineering Assessment

The problem addressed is clearly interdisciplinary. Moreover, "the systems approach to failure is not only a multi-disciplined one but also one that demands and open mind" (Bignell and Fortune 1984).

The determination of an engineering property is sought, but an engineering approach is not sufficient. Other disciplines are required to deal with the human and organizational factors, but their understanding are expected to be used to characterize an engineering property.

Historically, the initial approach was to look only at the physical system. The tools were probabilistic design and probabilistic reliability analysis of the physical system. The approach and tools fell mostly within traditional engineering areas of specialization. Then, human-machine interactions and studies in the field of ergonomics were included, after failures occurred. Approaches opened to other disciplines and other quantitative results were obtained. However, they did not reflect accurately the reliability of technological systems, as failure modes and contributing and compounding causes not considered in these methods kept arising in post-mortem accident studies. A significant aspect of the system was still missing in the theoretical approach.

An approach based solely on Social Sciences (this name is used in a broad sense here and includes cognitive psychology and behavioral science, among other fields) may not give an engineering answer, although it can provide useful insights for understanding the underlying processes at individual and social levels. Traditional engineering methodologies have also been insufficient. This work is intended to bridge the gap between both approaches, in order to provide a useful

answer from the Engineering point of view, while incorporating many concepts from the Social Sciences background.

1.2.2 Complementary Approach

It is proposed here that this problem demands complementary approaches. No single approach can satisfactorily address all the aspects with adequate generality and precision.

Some models are unable to "see" features that are readily apparent for others. A physical analogy may be useful to describe this concept. One point of view is not sufficient to graphically describe an irregular 3-D shape. More than one is needed, no matter how appropriate the first one is. Similarly, a unique approach to this complex problem is insufficient, no matter how good it may be.

Rutledge (1991) uses stronger words, but he is also demanding a complementary approach for a complex problem. "But the world can be viewed from many perspectives and those who stick religiously to one view or the other forgo a great deal of insight from approaches which advance an understanding of phenomena in other ways".

Quantitative methods are limited by the qualitative model they are based upon. The models are assumed to include "all the relevant aspects" of the phenomenon under consideration. And it is precisely here where the warning needs to be raised. "It is the resulting discrepancies between the way in which the world is believed to be, and the way it really is, which contain the seeds of disaster" (Turner 1978).

A traditional quantitative probabilistic approach may provide precise responses for a simple physical system, but is not accurate for a complex technological system. Limitations should be acknowledged. The analytical principles and tools that are useful for systems governed by laws of physics and mechanics are not adequate for systems governed by actions of people within organizations. Hollnagel (1993) describes this concept within the reliability assessment as follows:

"...the engineering approach to human reliability analysis is ... generally considered to be insufficient, not just by the behavioral scientists but also by those who actually use the methods in practice..."

Regulatory agencies for the safety of offshore oil installations (in this case, from the U.K.) also warn in relation to present quantitative tools:

> *... QRA [quantified risk assessment] should not be used in isolation in a mechanistic way. It is a tool to assist management in making decisions, for example in the matter of ranking and balancing risks. QRA techniques should always be used in conjunction with sound engineering judgement; they are not a substitute for it (Barrell 1992).*

Complementary approaches allow for the consideration of different aspects of the same phenomenon in order to reduce the probability of not considering a relevant one.

1.2.3 Qualitative and Quantitative Assessments

Engineering methods have been usually developed following a gradual process. At an initial stage, it is common that only a qualitative understanding of a phenomenon is achieved. And that may be the only basis available for engineering decision-making in early stages. This basic knowledge becomes the driving force to develop quantitative formulations, which is done under certain simplifying assumptions. Quantitative formulations may be semi-empirical or based on detailed understanding of processes, but in any case, they provide numerical results. Semi-empirical (or semi-analytical) formulations usually tend to be replaced by more rigorous analytical ones, when basic mathematical tools become available or/and adequate understanding of processes is achieved (whichever was missing).

Decisions can then be based on the numerical results and engineering judgement. Engineering judgement is required for the correct interpretation of numerical results, for the adequate weighing of assumptions versus the conditions of the actual problem, for the assessment of the applicability of the method used, for the understanding of the limitations inherent in the numerical result, for the adequate estimation of uncertain values of input variables, etc. In summary, engineering

judgement cannot be replaced by accurate numerical results, but it is only assisted by them when available.

The sequence of this work follows this process. It starts by the development of a qualitative understanding of the influence of "people within organizations" in the reliability of ocean systems. An empirical qualitative method is described to assess organizational factors and their influence on reliability. Based on this understanding, quantitative formulations are revised and improvements are proposed in order to incorporate organizational factors fully into methods of reliability analysis. At the end of the process, when numerical results based on these formulations could be obtained, engineering judgement (based on the qualitative understanding) should still be used to interpret the results and perform an engineering assessment.

The limitations of the traditional engineering tools should be carefully considered so that the final assessment can be representative of the system. The quantitative understanding presented here helps to identify limitations of the quantitative methods. The history of Engineering is full of cases where major failures occurred due to inappropriate use of analytical tools. That is, engineering judgement is and will always be required.

The qualitative understanding presented demonstrates the need for the incorporation of organizational factors in reliability assessment and becomes a framework for both qualitative and quantitative assessments. It helps to identify "the problem". As presented by Peet and Ryan (1998):

> *Quantification can only be of value after the problem has been set up appropriately and, in fact, many of the benefits of risk assessment can be gained with minimal or no quantification with "hard numbers"... This is particularly important when dealing with complex systems, as the effort spent in understanding the nature of the risk, and the structure of the problem, is critical to a successful result.*

Qualitative and quantitative approaches should be complemented if reliability was to be adequately evaluated and system failures would be avoided.

> *The avoidance of failure must include, with equal ease and accuracy, qualitative data as well as well as quantitative data in our pursuit of*

success. The mere thought of human behaviour and political factors being integrated into an overall risk-based failure avoidance methodology presents an exciting frontier for us to seek passage. For this is where we now need to reduce significant risks. This is the missing link in the integrated risk management (Stephens 1998).

1.2.4 Complementary Qualitative Approach and Quantitative Formulations

This work develops a complementary qualitative approach for the reliability assessment of complex technological systems. It is a qualitative top-down approach that captures the dynamic and non-linear characteristics of the organizational system in a simple way, in order to provide information about its reliability. The model has been developed and used by Bella in various systems and for different purposes (e.g. Bella 1987, 1997a, 1998a). A specific methodology is developed so that it can be used as tool in Safety Audits.

The qualitative approach –that can be used as a complementary qualitative method by itself to assess the reliability of an organizational system– can also be used to improve a quantitative approach and to identify guidelines for its use. A probabilistic formulation based on conditional probabilities is proposed to include explicitly organizational factors. The probabilities are expressed conditional to a state of the system, which is defined in terms of the qualitative approach. Preliminary guidelines, based on the qualitative approach, are proposed for the use of quantitative methods after the recognition of their limitations.

1.2.5 Trite Points

Almost two decades ago, when assessing the human element in the safety of structural design, Blockley (1980) stated:

... In engineering, only the product, the hardware, is a physical system; the system which designs it, produces it and uses it, is human and, therefore, complex and vulnerable... These points are perhaps so obvious that they sound trite, and yet engineering science has developed with little attention given to them. Certainly, for example, as far as any formal assessment of the safety of a structure is concerned, they are ignored.

At a certain point in this work the reader might feel a similar effect. That is, it can be found what Torroja (1960) called "*verdades de perogrullo*" (again, a way of saying trite, in Spanish) when presenting the fundamentals of structural design. However, as these authors stress, some obvious statements need to be recovered, since failures keep on emerging when they were not considered. Significant improvements have been achieved in the last decade but –after reviewing the methodologies applied– it is easy to recognize that the progress is not enough to forget some "trite points".

1.3 Description

This work is comprised of two main parts. Part I (Chapters 2 to 7) develops a qualitative approach to the organizational factors in the assessment of reliability of ocean systems. Part II (Chapters 8 to 12) proposes improvements and guidelines for the use of quantitative formulations of organizational factors, which are based on the findings of the previous part.

Chapter 2 covers the most significant theories and models related to human errors and organizational factors. Some of the most important contributions in the field of reliability in ocean and nuclear power industries are also included.

A different systems approach to complex organizations, the CANL model, is introduced in Chapter 3. The model is applied to a case study and its fundamentals are used to understand major failures of the offshore industry in Chapters 4 and 5 respectively. A qualitative methodology to assess the reliability of an organization as part of a safety audit is summarized in Chapter 6. Chapter 7 contains the concluding remarks of the first part.

Chapter 8 contains a brief review of some of the relevant established quantitative methods applied in this field. In Chapter 9, four probabilistic formulations recently proposed by different authors are reviewed. The findings of the qualitative approach provide the basis to the concept of Reliability State. Chapter 10

provides a definition and a method for determination of this indicator of the system. Improvements to the present probabilistic formulations to explicitly include the organizational factors are presented in Chapter 11. The formulation is based on probabilities conditional to the Reliability State of the Organization. Preliminary guidelines for the use of quantitative methods are proposed based on ranges of values of this indicator. Chapter 12 contains the concluding remarks of the second part.

PART I

2. BACKGROUND TO HUMAN AND ORGANIZATIONAL FACTORS

2.1 Human Errors

2.1.1 Introduction

Within the scope of what has been called Human Factors or Human and Organizational Factors (HOF), the study of errors of human individuals comprises a significant part. The first efforts to introduce the consideration of the human components in the analysis of the reliability of technological systems centered on individual human errors. The focus of this work goes beyond the individual errors and focuses on their context. Nonetheless, the theories developed on human errors provide a necessary background for the understanding of the HOF issues.

This chapter describes some of the contributions of Cognitive Psychology and Social Sciences in general to the understanding of human errors, and examples of the "Engineering approach" to human errors and organizational factors.

2.1.2 Definitions

A "working definition" of human errors "in a psychological rather than a philosophical sense" is proposed by Reason (1990a):

> *Error will be taken as a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency.*

The planned sequence of activities may fail to produce the intended outcome because the actions could not be achieved as planned, or they may fail because, even if performed as planned, the plan was not adequate. In the former case it is an execution failure, it includes slips and lapses. In the latter it is a planning mistake.

Rasmussen (1987a) defines human errors in a system as "causes of unfulfilled system purposes". He further points out that errors cannot be identified objectively by considering the performance of an individual in isolation, but that it can only be defined with reference to external expectations. That is, the performer does not always know the framework for the definition of an error. The error may not only be due to a performance falling short of an acceptable level, but also when the criteria for judgement vary and subsequent actions are not modified accordingly. Changes in requirements of the systems performance, safety requirements or legal framework may transform a previously acceptable action into an error. An action identified in a post-mortem study as a cause of a system failure is identified as an error, independently of the individual attitude of the operator.

2.1.3 Taxonomy of Human Errors

Reason (1987, 1990a) proposes a Generic Error Modeling System (GEMS), which is based on the skill-rule-knowledge classification of human performance by Rasmussen (1986, 1987b). The three levels of performance defined correspond to decreasing familiarity with the task. At the skill-based level, human behavior represents a performance that takes place without conscious control after the statement of an intention. The rule-based level deals with familiar problems, for which stored rules are available. The knowledge-based level corresponds to new situations where both analytical processes and stored knowledge must be applied. With increasing expertise, the main control mode usually shifts from knowledge based towards skill-based levels.

GEMS yields three basic error types: skill-based slips and lapses, rule-based mistakes and knowledge-based mistakes. Skill-based errors involve routine actions, while rule-based and knowledge-based errors occur during problem-solving activities. Rule-based mistakes are related to the application of the wrong rule or the following of incorrect procedures. Knowledge-based mistakes arise from analytical limitations and incomplete or incorrect knowledge. It is also pointed out by Reason

(1990a) that while individuals usually detect skill-based errors rapidly and effectively, mistakes are difficult to detect and usually require external intervention.

The influence of factors external to the individual in the probability of human error is described by Reason (1990a) as follows. "... Errors at each of the three levels will vary in the degree to which they are shaped by both intrinsic (cognitive biases, attention limitations) and extrinsic (the structural characteristics of the task, context effects) factors". Among the three error types, extrinsic factors are likely to predominate only for knowledge-based mistakes. However, extrinsic factors may have significant importance (Norman 1988):

> *A subtle issue that seems to figure in many accidents is social pressure. Although it may not at first seem to be relevant in design, it has strong influence in everyday behavior. In industrial settings social pressures can lead to misinterpretation, mistakes, and accidents. For understanding mistakes, social structure is every bit as essential as physical structure.*

Rasmussen (1986) describes the influence of external factors as follows: "Frequently, the mismatch [human error] is not due to spontaneous, inherent human variability, but events in the environment, which act as precursors can be identified". Performance-affecting factors are described as persistent conditions that do not produce errors but change (usually increase) their likelihood. Therefore, individual human errors –especially of the knowledge-based type– are influenced by factors that are external to the individuals. That is to say, in these cases the context plays a significant role.

As part of a systems analysis, Reason (1990a, 1990b) proposes that "unsafe acts" can become local triggers and compounding factors for accidents. Unsafe acts are human failures (errors or violations) committed in the presence of a potential hazard (Reason 1990a). Therefore, human active participation in system failures is not limited to the previous classification of human errors, but it is expanded to include violations.

Violations are defined by Reason (1990a) as "deliberate –but not necessarily reprehensible– deviations from those practices deemed necessary ... to maintain the

safe operation of a potentially hazardous system". Violations are deliberate, but in general not intended to produce a damage. Deliberate violations aimed at producing damage fall into the category of sabotage and are not considered here. Reason (1990a) further classifies violations into routine and exceptional violations. Routine violations are usually influenced by a tendency to take a path of least effort and a relatively indifferent or permissive environment is needed. Exceptional violations can occur only under a rare and particular set of conditions. Routine violations may become usual and widespread in certain work environments and they may contribute to the unexpected propagation of otherwise insignificant local failures.

Considering the human contribution to system failures, Reason (1990a, 1990b) proposes a distinction between two kinds of human failures or unsafe acts: active failures and latent failures. Active human failures have an immediate and apparent effect on the performance of the system. They are usually associated with actions of front-line operators that fall within the category of errors or violations. Latent failures do not have visible consequences immediately. They lie dormant, only to become apparent when they combine with a local triggering factor. Local triggering factors are usually active human failures, physical component failures, and atypical system or environmental conditions. Latent failures are usually associated both with human and physical components of the technological system. Unsafe acts and decisions induced by organizational pressures, lack of maintenance, and routine violations are all examples of latent failures. Because of their intrinsic characteristics, latent failures tend to persist and expand through the system, thus increasing the vulnerability to local active failures.

The limitations of an approach that only focuses on the human errors of individuals in a limited set of conditions and is based on a single discipline is described by Reason (1990):

> *While cognitive psychology can tell us something about an individual's potential for error, it has very little to say about how these individual tendencies interact within complex groupings of people working in high-risk systems. And it is these collective failures that represent the major residual hazard.*

Organizations, where those "collective failures" may occur, play a significant role in the reliability of a technological system. The study of individual human errors does not account for all the factors that influence the probability of failure of members of the human organizational subsystem.

2.1.4 Alternative Taxonomy of Human Errors

Bea (1994) develops the concepts of human errors for its use in engineering assessment. He defines human errors as "actions and inactions that result in lower than acceptable quality". The description of error types by Reason (slips or lapses and mistakes) is adopted, including violations, as in Reason's unsafe actions. Bea (1994) also points out the significance of mistakes, since they are hard to identify by the user, and the potential significance of circumventions (violations) when unexpectedly combined with errors.

He proposes a taxonomy for human errors based on the study of accident databases and case histories (Bea and Moore 1993a, Bea 1994). Human errors are classified as caused by:

- Communications: transmission of information
- Planning and preparation: program, procedure, readiness
- Slips: accidental lapses
- Selection and Training: suited, educated, practiced
- Violation: infringement, transgression
- Limitations and impairment: fatigue, stressed, diminished senses
- Ignorance: unawareness, unlearned
- Mistakes: cognitive errors

This list is proposed to be a mutually exclusive and collectively exhaustive list of factors that can result in human errors. Even if a list of mutually exclusive and collectively exhaustive events is very convenient for a probabilistic manipulation, this characterization is hardly adequate in this case. Multiple factors usually combine to produce individual human errors. The probability of a violation is reduced if

planning and training is well done, and is enhanced if ignorance and mistakes are present. A specific unsafe act may be a violation and simultaneously a cognitive mistake based on ignorance, thus combining different factors into one error. Communication errors can flourish in an environment that induces limitations and where slips are usual. This list is arguably exhaustive, but does not contain mutually exclusive events or factors. Other aspects of his approach to human errors within the framework of organizations are presented later in this chapter.

2.2 Organizational Factors

The influence of organizations in the reliability of technological systems is widely acknowledged (Turner 1978, Perrow 1984, Reason 1990a, Roberts 1993, Sagan 1993, Bea 1994, Goldfeiz and Mosleh 1996, Apostolakis *et al* 1993). A central question of this work is how organizations affect the reliability of a complex technological system, and what can be done to improve both the actual reliability and its assessment.

Sagan (1993) reviews the literature about reliability of complex technological systems and identifies two general competing schools of thought. The High Reliability Organizations Theory proposes that extremely safe operations can be achieved, even with hazardous technologies, if appropriate organization design and management techniques are applied. The second view, the Normal Accidents Theory, states that serious accidents (catastrophic system failures) are inevitable in complex technology systems. In between these philosophical positions, engineers and managers daily try to achieve high reliability when they participate in and make decisions about the design, construction, operation, and decommission of ocean systems. This work addresses their needs and concerns.

The following sections cover relevant aspects of these schools of thought and summarize work by particular authors that specifically relate reliability to organizational factors.

2.3 High Reliability Organizations Theory

The authors that support a point of view identified by Sagan (1993) as High Reliability Organization Theory have observed that relatively few major accidents have occurred in some high-risk enterprises. The basic assumption is that properly designed and managed organizations can compensate for human errors thus achieving error free systems. This would be achieved by elimination of some human errors and by the timely introduction of corrections that avoid escalation, so that system failures do not occur.

Morone and Woodhouse (1986) state that "given the challenge posed by modern technologies, the record is surprisingly good: despite dire warnings, no catastrophes have occurred". A multi-disciplinary research group based at University of California at Berkeley maintain that "we have begun to discover the degree and character of effort necessary to overcome the inherent limitations to securing consistent, failure free operations in complex social organizations" (La Porte, as cited by Sagan 1993). Wildavsky (1988) proposes a "theory accounting for the considerable degree of safety achieved in contemporary society". Rochlin (1993) characterizes these organizations as "demanding of perfection". He identifies three defining criteria: the activity is inherently complex; the activity has social demands that require performance at the highest level obtainable; the activity contains inherent technological hazards in case of failure.

Sagan (1993) identified four critical causal factors for High Reliability Organizations (HRO): the prioritization of safety and reliability as a goal by the organization leadership; high levels of redundancy in human and physical safety systems; the development of high reliability culture in decentralized operations; and elaborate forms of organizational learning.

The first requirement for high reliability organizations is that both political leaders and the heads of the organization must hold reliability and safety as a priority objective (Sagan 1993). La Porte and Consolini (1991) note that this goal can "nurture an organizational perspective in which short-term efficiency has taken a

second seat to very high-reliability operations". It is recognized that a lack of sufficient commitment to safety –the will to devote considerable resources– will make accidents more likely. This requirement also implies that very clear and consistent goals are defined within the organization (with safety as the most important), and that they are clearly and consistently communicated to all its members.

Redundancy has been proposed as the second causal factor for high reliability organizations. Redundancy is required both for the physical and organizational subsystems. Since humans operate with limited and fallible cognitive capabilities, it is proposed that the only way to achieve high reliability on a human system is with an organization that shows overlaps, duplications and checks. In other words, "redundancy is absolutely essential if one is to produce safety and reliability inside complex and flawed organizations" (Sagan 1993).

The third factor includes three related concepts. While redundancy is considered essential, additional operations and management strategies are also asked for to reduce the burden placed on it to attain reliability. It is argued that this can be achieved through decentralization in decision-making, the creation of a "culture of reliability" (also referred as safety culture) and the maintaining of continuous operation and training.

Decentralization is not considered an opposite of hierarchy. Hirschhorn (1993) proposes that people can respond flexibly to their task demands working in hierarchies. This can be achieved when authority is widely delegated and the chain of command is preserved and secured. However, he proposes that procedures need to have certain flexibility. Guiding procedures establish general objectives that have to be strictly implemented. Detailed procedures could be modified by lower-level personnel as long as they fulfill the intentions, unless they correspond to emergency conditions. "By applying policy strictly, they can change specific procedures safely and creatively" (Hirschhorn 1993). This hierarchical and flexible structure is proposed to avoid the ambiguity that was described by a supervisor of a nuclear power plant as follows: "Responsibility for success or failure in implementing a

procedure is on the operator right now. If he violates a procedure, even if he's right, he's wrong. If he doesn't violate a procedure and it's wrong, he's wrong" (Hirschhorn 1993).

Safety culture is proposed as a response to unexpected and unique hazards. It is a required complement to decentralized authority to successfully cope with unusual circumstances. The purpose is to ensure that low-level personnel can identify situations properly, behave responsibly and take appropriate actions during crisis. Recruitment, socialization and training are key elements proposed to achieve a culture of reliability. All members of the organization are required to have a high level of knowledge, so that no mistakes are made under unusual conditions.

The fourth factor necessary to obtain high reliability in complex organizations, according to the review by Sagan (1993), is a strong capability to learn. This factor recognizes the significant importance of the evolution and dynamics of organizations. The two modes of organizational learning summarized by Sagan (1993) are trial and error and simulations.

Trial and error is an incremental learning process, which will be successful as long as adequate designs and operation standards are maintained, and inadequate ones eliminated. Even if this approach is supported as necessary (Wildavsky 1988, Morone and Woodhouse 1986, Rochlin *et al* 1987), it is of limited applicability because of the high social costs of this kind of system failures.

Simulations and imagination of trial and errors is the alternative to avoid the cost of actual failures. It can be seen also as a "sophisticated trial and error strategy" (Morone and Woodhouse 1986). Its use is widespread as it speeds up the learning process with minimum risks.

Argyris and Schön (1978) have described organizational learning as a process that can be developed in two different levels. Single loop learning uses a prescribed set of assumptions to improve the performance, to be more efficient. A higher level of learning is achieved when the basic assumptions are questioned after the analysis of the performance. The later, called double-loop learning, allows for a high quality

organizational learning, which is ultimately demanded by HRO. It aims at effectiveness and is based on a critical review of assumptions.

Schulman (1993) describes that in most organizations, when resources reach points of diminishing marginal returns in relation to valued outputs, their allocation is likely to be reduced. This process requires a framework of understanding of causality and marginal cost/benefit tradeoff, which is adjusted by trial and error. However, in HRO this is almost impossible, since the demand for reliability is of utmost importance, the priority objective of the organization. The consequences of failure strongly limit organizational learning through trial and errors, and complexity does not allow developing an accurate model for causality. Under these conditions, reliability needs to be actively pursued if it is to be maintained. "Unless continual reinvestments are made in improving technical systems, procedures, reporting processes, and employee attentiveness, those performance standards that have already been attained are likely to degrade" (Schulman 1993).

The observation that safe organizational behaviors naturally tend to degrade is significant. As a corollary of the prioritization of reliability and organizational learning factors, HROs must consider reliability as a non-marginalizable property. This approach is hard to implement strictly in any commercial enterprise, and is obviously a major challenge.

2.4 Normal Accidents Theory

Perrow (1984) presents the basis of the Normal Accidents Theory. He described it as a "theory of systems, of their potential for failure and recovery from failure" (Perrow 1984). The main statement is that serious accidents are to be expected in complex technological systems; they may be rare, but they are inevitable. The two basic characteristics that a system has to fulfill to be considered in this category are "interactive complexity" and "tight-coupling". Interactive complexity indicates the way the parts are connected and interact. It gives origin to

unexpected and –at least temporarily– incomprehensible interactions of local failures. When a system is tightly coupled it does not allow for buffers, so local failures can propagate fast and get out of control (escalate) easily, thus producing system failures.

Perrow (1984) defines accident as a "substantial damage to a system that disrupts the ongoing or future output of a system". The concept of accidents defined as a disorder was also proposed by Turner (1978). "All accidents and disasters are measured in terms of an order which was intended or at least anticipated...". According to the level where the disruption occurs the damage may not be substantial. The levels defined are "part" (the smallest component of the system that is identified), "unit" (a functionally related set of parts), subsystem (array of units), the "system", and the "environment" (outside of the system under study). Damage occurring at a part or unit level is considered an incident. An accident is also defined as "failure in a subsystem or a system as a whole that damages more than one unit and in doing so disrupts the ongoing or future output of the system" (Perrow 1984). Accident and system failure will be used as synonyms in this work.

Within accidents, Perrow (1984) distinguishes two types, based on the nature of the interactions of component failures that lead to the failure at the system level. Component failure accidents involve failures of components (part, unit or subsystem) that occur due to interactions anticipated, expected or comprehended by the designers or knowledgeable operators of the system. System accidents are the outcome of unanticipated interactions of multiple component failures. Both types of accidents are initiated by component failures, but only system accidents –as defined by Perrow– are the product of "unexpected interactions" among component failures.

Interactive complexity is a fundamental property of systems which may experience "system accidents" (also called "normal accidents"). In systems with linear interactions, the consequences of local component failures are understood and –even if unexpected– are readily apparent. Complex interactions occur less frequently. Perrow (1984) defines complex interactions as "those in which one component can interact with one or more other components outside of a normal

production sequence, either by design or not by design". They may be related to common mode functions (when parts serve several functions, thus its failure has more dispersed consequences), proximity (when parts of different processes are physically close, so a failure can spread easily across subsystems), and indirect information sources. Unexpected non-linearities such as branching paths, feedback loops and phase shifts can also produce complex interactions.

Hidden interactions also identify the complexity of a system. Complex systems have many operations and they are designed so that only a few parameters are controlled. Therefore, operators have less flexibility to respond and have less information about the actual events to understand interactions during an incident due to indirect measurements.

Tight coupling is the other key property of a complex system, as described by Perrow (1984). It is strongly related to the capacity for recovering after a local failure. Tightly coupled systems have more time-dependent processes, they are rigid in its procedures, have little slack (which requires more precision), and safety devices, redundancies and buffers between parts are limited to the ones designed. All these characteristics lead to little opportunity to recover from unexpected failures. Tight coupling is a very convenient property for simple systems with linear interactions, but can become unsafe when interactions are complex.

Complex systems have been characterized as more efficient than simple ones. They have less slack, less underutilized space, more multifunction components and less tolerance for low quality performance. "If a system has many complex interactions, unanticipated and common-mode failures are inevitable; and if the system is also tightly coupled, it will be very difficult to prevent such failures from escalating into a major accident" (Sagan 1993).

2.5 Resident Pathogen Metaphor

Reason (1990a, 1990b) proposes a systems approach to accident causation that he calls Resident Pathogen Metaphor. It is based in a classification of human failures in two kinds: active and latent. This classification can be extended to all local failures of parts (components) or units, either physical or human. In fact, it is stated that latent failures are residual problems that "do not belong exclusively to either the machine or the human domain... they emerge from a complex as yet little understood interaction between the technical and social aspects of the system" (Reason 1990b). Therefore, latent failures are not only human.

Reason (1990a, 1990b) suggests that latent failures are analogous to resident pathogens in the human body, which combine with external factors to develop a disease. Latent failures set the stage for system failures. They provide the conditions for several local failures –a priori unrelated– to occur and combine in a lethal way. "Accidents in complex, defended systems do not arise from single causes" but through the "concatenation of several different factors, each one necessary but singly insufficient to cause the catastrophic breakdown" (Reason, 1990b).

Following this metaphor, Reason (1990b) proposes the following basic assumptions about accident causation:

- the likelihood of an accident is a function of the total number of latent failures (resident pathogens) present in the system;
- the more complex, interactive, tightly coupled and opaque the system (following definitions by Perrow 1984), the greater will be the number of resident pathogens;
- the higher an individuals position in the structure of an organization, the higher potential to generate resident pathogens;
- it is virtually impossible to foresee all the possible local triggers.

And an important corollary is that efforts should be oriented to the proactive identification and neutralization of latent failures, rather than to the prevention of active failures.

The importance attributed by Reason to managers and designers is not needed to arrive to the most significant conclusions about accident causation. However, it may be considered a needed warning for the "decision-makers", who have been traditionally out of the "accident chain of events" identified in post-mortem reports. His approach may obscure the fact that they are also members of the organization and, as such, they are subject to similar pressures and conditionings as regular operators.

It is proposed here that latent failures are organizational outcomes, rather than the immediate consequences of an individual's decision or action. They "emerge" from a complex interaction between physical and organizational components of the system and their environment. The organization as a system is involved, and the decision-makers play their role as members of the organization. Emergent systemic outputs are not the direct result of any action or decision by an individual or group (these concepts are developed in Chapter 3).

The relationship proposed by Reason between the resident pathogens and the system properties of interactive complexity and tight-coupling (the number of resident pathogens is determined by the characteristics of the system) is not evident. In some cases it has been noted that latent failures can make a system more complex and with tighter coupling. Weick (1990) describes how latent failures that induced stress affected the system in that way. He further states that Perrow's characteristics (interactive complexity and tight coupling) should not be considered static properties of organizations but dynamic ones. Paté-Cornell (1995) describes how organizational attitudes induced modifications that turned a platform into a more complex and tightly coupled mechanical system. It should be noted, then, that the number of latent failures and the complexity of a system are strongly related, and that they affect each other in a bi-directional and dynamical way.

Reason (1990a, 1990b) proposes a general framework for accident causation in complex systems. He defines the "healthy" human components of a production system and then the various human contributions to system failures.

The healthy components identified by Reason (1990a, 1990b) are:

- decision makers: top-level management, set the production and safety goals and strategic guidelines, allocate resources;
- line management: specialists that implement strategies;
- preconditions: qualities of the physical system and of the organizational arrangements at operators' level;
- productive activities: actual performance of machines and people;
- defenses: safety devices and systems.

These components are described in layers or "productive planes" (Reason 1990a), in sequence, and with feedbacks only to the decision-makers. Only the defenses are shown as off the sequence, acting solely upon the output of the productive activities.

It is arguable that some components are defined as individuals (decision-makers, line management) and others as qualities (precursors) and actions (productive activities). As described by Reason, preconditions would only affect operators and machines. This approach does not reflect the fact that the performance of the physical system and the workforce –as well as the existence of latent failures– affect the quality of the decisions by top-level managers and the implementation of strategies by line managers. That is, management decisions are affected by preconditions as much as operator's performance. On top of that, they are also influenced by information feedback.

Whalley and Lihou (1988) highlight the influences of the system upon the managers. "It is important for individual managers to be aware of what aspects can be influencing themselves and hence the success of their decision making. As people, managers are as susceptible to the negative influences of their general 'environment' as shop-floor workers" (Whalley and Lihou 1988).

Reason (1990a) describes a condition for system failure under his framework as a sequence initiated by fallible decisions at the top management or designer's level. At the line management level, these wrong decisions show up as several types of failures, which are also latent. Psychological precursors (in the precondition plane) are the latent states that may promote a wide variety of unsafe acts. It is acknowledged by Reason that both line management deficiencies and psychological precursors may also be originated in individuals in other levels of the organization. Unsafe acts become active failures as a result of a complex interaction between intrinsic system characteristics (the previous three planes) and environmental conditions. For an unsafe act to develop into a system failure it has to break the defenses of the system. Inadequate defenses can arise due to latent or active failures.

The attention placed on the decision-makers is justified by Reason (1990a) on the strong factors that contribute to fallible decisions. He describes these factors in relation to the conflict between safety and production in the allocation of resources by top-management. Decisions oriented to improve productivity have a high certainty about their output, and an unambiguous, rapid and reinforcing feedback. Decisions oriented to improve safety have a high uncertainty, and the feedback is negative, intermittent, often deceptive, and only compelling after a major accident (Reason 1990a).

It is proposed by Reason (1990a, 1990b) that the best strategy to avoid system failures is to eliminate the psychological precursors of unsafe acts. Several causal factors are required for a system failure, or a "trajectory of opportunity through multiple defenses". These include latent failures in the organization, failures of defenses, external triggering factors and unsafe acts. Of all these, the one that allows for a better control is the first one.

Reason (1990a, 1990b) defines an effective safety information system for the organization with the components he described. The system provides information to the top-managers. Loop 1 is the feedback information about accidents and incidents, and it is the minimum requirement for any safety information system. Loop 2 provides information about unsafe acts, and is assessed to be potentially available.

Loop 3 provides feedback about the psychological precursors and loop 4 about line management deficiencies. Reason (1990a, 1990b) argues that loops 3 and 4, which constitute a "pathogen auditing", are the most effective but they are rarely in practice.

2.6 Human and Organizational Factors for Reliability Assessment

2.6.1 Organizational Factors Research and Regulations on Nuclear Power Plants

Recent research on safety of nuclear power plants (NPP) is aimed at the incorporation of organizational factors into reliability analysis (Apostolakis *et al* 1993, Haber *et al* 1995, Goldfeiz and Mosleh 1996, Tuli *et al* 1996). This effort is supported or developed by national and international organizations such as the US Nuclear Regulatory Commission (NRC) and the International Atomic Energy Agency (IAEA). The main qualitative concepts are described here, and the quantitative formulations are described in Part II (Chapter 9).

The International Nuclear Safety Advisory Group (INSAG) of IAEA states that the management of a NPP has to establish a "safety culture" in the organization as one of its fundamental management principles in order to achieve safe operations (IAEA 1988). INSAG defines safety culture as "the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear power plant safety issues receive the attention warranted by their significance" (IAEA 1991). This definition recognizes the complex and pervasive influence of organizational factors in safety, and relates the concept to a significant characteristic of HRO: priority of safety.

Studies contracted by NRC have identified some of the most significant organizational factors to affect safety performance. Several methodologies have been proposed to assess these factors (e.g. Haber *et al* 1995, Apostolakis *et al* 1993).

Tools applied include analysis of organizational structure, behavioral observation, questionnaires and interviews.

A set of "organizational dimensions" represent what is believed to be a comprehensive taxonomy of organizational elements that relate to the safe operation of NPPs (Jacobs and Haber 1994, Haber *et al* 1995). The 20 organizational dimensions identified were called: centralization, communication (interdepartmental, intradepartmental and external), coordination of work, formalization, goal setting, organizational culture, organizational knowledge, organizational learning, ownership, performance evaluation, personnel selection, problem identification, resource allocation, roles/responsibilities, safety culture, technical knowledge, time urgency and training. These dimensions are grouped under 5 headings: culture, communications, decision-making, administrative knowledge, and human resource administration by Jacobs and Haber (1994).

Haber *et al* (1995) modified and arranged this original list in order to use existing NRC documentation. They developed a two-tier, four-factor model that comprises 17 organizational dimensions. The first tier includes one factor, culture, and comprises four organizational dimensions: organizational culture, organizational learning, safety culture, and time urgency. Culture is labeled as a higher-order factor, since its dimensions have a broad impact on other factors and the organization as a whole. The second tier includes three organizational factors: communications, human resource management and management oversight. The communications factor comprises internal communications, external communications and organizational knowledge dimensions. Human resource management factor comprises training, technical knowledge, performance quality, performance evaluation and personnel selection. The management oversight factor includes coordination of work, formalization (extent of standardization, rules and procedures), problem identification, goal prioritization and resource allocation, and centralization dimensions. The grouping is different (even if headings are similar) to the one proposed for the 20 factors by the same research group (Jacobs and Haber 1994).

One significant regulatory case related to organizational factors is the closure of the Millstone Nuclear Power Plant. After a reactor unit was shutdown due to safety violations, the operating company was ordered to certify by an external audit the modification of working conditions and safety culture before the reactor was to be restarted. On December 10, 1997, the NRC fined Millstone $2.1 million. The Notice of Violation and Proposed Imposition of Civil Penalties by NRC to the president of the operating company states the following (NRC 1997):

> *Although violations described in the enclosed Notice did not result in any actual consequences to public health and safety, many of these violations and underlying causes were long-standing and indicative of a deficient safety culture, fostered by plant and corporate management, which neither set high standards or actively encouraged workers to identify and report safety issues or act upon issues once they were reported.*

The initial detection of violations to NRC regulations had triggered further inspections that showed persistent behaviors within the organization that revealed a dangerous state. The lack of an adequate safety culture was assessed objectively through qualitative standards. NRC considered the alarming proliferation of latent failures, low consequence local failures and repetition of unsafe behaviors within the organization (many of which were actual violations) as enough justification for a strong penalty. In particular, a $1.0 million fine was established because "the licensee did not assure that conditions adverse to quality were promptly identified and corrected" (NRC 1997). It was then established that "... the units will remain shut down until adequate programs have been established and demonstrated to the NRC to be effective" (NRC 1997).

The restriction to restart operations was based on the understanding that organizational factors created a condition of significant reduction of reliability. In particular, it was detected a persistent management attitude to stop the raising of safety concerns by operators and contractors (NRC 1996). In this case, the Nuclear Regulatory Commission imposed a very strong penalty that jeopardized the overall operations of the company based on a qualitative assessment of the reliability of the technological system, focused on its organization.

2.6.2 Human and Organizational Factors Research in Offshore Oil Industry

The Piper Alpha accident triggered a stronger interest on Human and Organizational Factors (HOF) in the offshore oil industry (e.g. Vinnem 1998, Gordon 1998). One of the significant contributions to the field of HOFs in the reliability assessment of offshore systems was performed by Bea and his co-workers (e.g. Moore and Bea 1993a, Bea 1994, 1995a, 1995b, 1997a, 1997, 1998a, 1998b, Bea *et al* 1997b).

It has been identified that less than 20% of the accidents of offshore systems were due solely to structural failures (Bea 1994). In most cases, low probability, high consequence accidents (LP/HC) are due to human errors or "unanticipated actions of people that have undesirable outcomes (something more than 80%)" (Bea 1998b). About 80% of the accidents due to human errors occur during operations and maintenance. About 80% of the compounding and contributing causes of failure are directly related to organizations (Bea 1994). He further states that root causes for human errors can be found in design, construction, operation and maintenance (Bea 1998b). These root causes can be understood as the "latent failures" described by Reason (1990a).

Bea (1998b) proposes as an important stating point to recognize that "while human and organizational errors are inevitable, their occurrence can be reduced and their effects mitigated by improving how we engineer systems". Furthermore, he encourages looking at the experience of other scientific and engineering communities such as the ones concerned with air and spacecrafts, nuclear power plants, medical facilities, and chemical refineries.

Bea (1998b) proposes that systems should be designed to "minimize excessive physical, mental, financial, and social strains in each of the life-cycle phases of an offshore structure", to provide early warning systems, and with damage and defect tolerance (robustness), combining redundancy, ductility and excess capacity. He also mentions that organizations and management can influence the safety of the system, and they should develop a safety culture.

The author warns against analytical-quantitative approaches (Probabilistic Risk Analysis, Quantitative Risk Analysis) when the physical system has profound interactions with people. In such cases, analytical models applied tend to be mechanical and static, while actual systems have organic and dynamic behaviors.

Bea (1994) defines the components of a system as individuals, organizations, procedures, (physical) systems and environments. The four later are related to the individuals through four different interfaces. These components and interfaces can lead to human errors.

An alternative definition proposed in this work is that individuals are part of organizations; procedures are the rules that individuals follow to deal with the physical systems; and the environment represents all the physical and organizational constraints and conditioning factors that do not belong strictly to the system. Individuals can lead to human errors, through particular actions. Organizations only indirectly influence human errors, mainly by the development of states that influence their probabilities. The relationship is bi-directional. Organizations affect individuals, and individuals –through the complex interaction of patterns of behavior and decision making of many of them– produce organizational outcomes. Some of these basic relationships can be sketched as shown in Figure 2-1.

Technological systems usually fail through their physical components. The physical components fail either directly due to environmental extreme conditions (excessive wave action, wind, earthquake, etc.), directly due to one human error, or due to compounded human errors or/and failures of other physical components. The technological systems as a whole usually fail by a combination of failures of physical components and human errors, where an organizational setting encourages them.

Bea (1994) describes that human errors may develop from "states" or from "actions". The former are influences that induce errors, the later are actual human errors as defined above. "States can lead to human errors, and actions can lead to undesirable states" (Bea 1994).

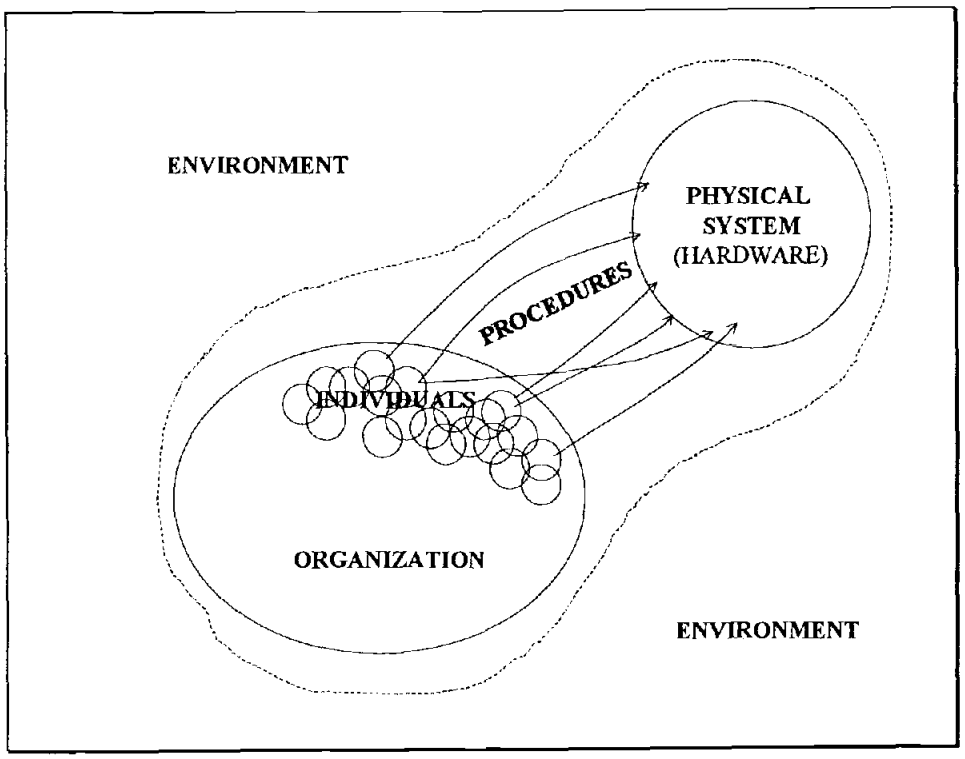


Figure 2-1
Components of a technological system and its interconnections.

In this sense, actions are produced by individuals, and states are the outcome of patterns of behavior within organizations, which may include performance of the physical components. Undesirable behavioral patterns within organizations induce human errors, thus increasing their probability of occurrence. The states – organizational factors– are not errors or failures by themselves, but latent system failures, following Reason's definition. Actions by individuals affect –in a complex and nonlinear way– the systemic behavioral patterns within organizations so that their outcomes may become undesirable.

Bea (1994) defines organizational errors and human errors in a similar way. Organizational errors are defined as "a departure from an acceptable or desirable practice on the part of a group of individuals that can result in unacceptable or undesirable quality".

Bea (1994) classifies organizational errors into communications, culture, violations, ignorance, planning and preparation, structure and organization, monitoring and control, and mistakes. Some of these (violations, ignorance, and mistakes) can only be individual human errors, unless characteristics of individuals are assigned to organizations. This definition assigns to groups of individuals or organizations the properties of individuals themselves. From a systemic approach, it may be described as a confusion of "parts" with the "whole".

It is proposed in this work that human errors, induced by human factors and organizational factors, can contribute to failures in technological systems. It is rare that a technological system may fail, or be unable to perform its intended function with a prescribed level of quality, solely due to organizational factors. In fact, it is usually a combination of human failures and organizational factors that directly or indirectly cause the failure of several physical components, thus producing a system failure. Moreover, organizational errors are hard to identify *a priori*, since most of the time the same actions that are considered efficient practices during normal operation are defined as organizational errors in post-mortem studies.

Gordon (1998) proposes a definition of human factors that encompasses the effects that individual, group and organizational factors have on safety. Human factors are regarded as those factors that describe underlying causes, while the human errors are the specific acts –which are caused by the human factors– and are seen as the immediate cause of an accident (Gudmestad and Gordon 1997).

Safety culture (climate of reliability or organizational safety climate) is a generic description proposed for a set of behaviors that characterize an organization. Conversely, "the organizational climate represents the context in which behavior occurs and the basis of people's expectations" (Gordon 1998). Factors identified as related to safety are management commitment to safety, safety training, open communication, environmental control and management, stable workforce, and positive safety promotion policy. Characteristics found to exist and to have a negative impact were financial pressures, priority to short-term production goals,

pressures for cost minimization, high turnover of personnel, bad communication, and a culture of denial of risks (Gordon 1998).

Group factors refer to group dynamics that can lead to reduced or enhanced safety. Gordon (1998) includes within group factors those related to middle management, supervision and crews. It is mentioned that a management style that enhances open and informal communications across groups and regular appearances on the field improve safety. Shortage of time due to excessive pressure for production, poor scheduling and planning, and conflicts over assignments are mentioned as error inducing. Supervisors are characterized as key elements to correct fallible decisions of higher organizational levels. However, it is pointed out that it is unlikely that those fallible decisions could be identified if supervisors are limited by resources, put under time pressure, and have inappropriate perceptions of hazards (Gordon 1998). Crew factors found to affect safety include attitudes towards communication, coordination, command responsibility, and recognition of stressor effects.

The broad factors that affect a person's performance, beyond the historical main focus on man-machine interface (ergonomics), are summarized (Gordon 1998). The individual factors that were found to affect safety include the level of training and experience, clarity of work instructions, being overworked and not given enough responsibilities.

A categorization of human factors developed by other industries and a classification for the reporting of accidents and incidents are also provided. Gordon (1998) proposes accident and incident reporting and auditing of unsafe acts and latent failures as ways to reduce accidents based on human factor data. The state of an organization can be assessed through a Failure State Profile, which incorporates the latent failures. The general failure types proposed (Gordon 1998) include hardware, design, maintenance, procedures, error enforcing conditions, housekeeping, incompatible goals, organization, communication, training and defenses.

In this work, the definitions by Bea are maintained. Therefore, Gordon's individual human factors are called "human factors". The focus of this work is on the human factors at organizational and group level defined by Gordon, which are called here "organizational factors". In Part II of this work a method to identify and evaluate the Reliability State of an Organization it is proposed. Gordon (1998), among others, also assume that this state can be assessed.

Bea (1994) classifies the sources of human errors following his definition of the components of a system. Factors that contribute to human errors are categorized into organizational, individual, and systems (physical system and procedures) errors. He places the sources of organizational malfunctions into three general categories: upper level management, front line management and design/construction/operation teams. Upper level management can allocate inappropriate resources for safety given the conflicting goals of productivity and safety. Front line management can influence organizational malfunctions by information filtering and redirection of resources to increase productivity at the expense of safety. Low quality at design/construction/operation teams often arises though lack of adequate verification, "wishful thinking" (lack of commitment for problem solving), lack of teamwork and poor communications. These insightful observations by Bea and Gordon are reflected in the model proposed in the following chapter.

Human-systems interfacing is also a significant source of human errors. The design of physical systems and elaboration of guidelines and procedures can have a significant impact on human error probabilities. The focus of this work is, however, on the organizational factors. Human errors in general, and human-system interactions studies have been specifically developed and are somewhat integrated in present methodologies of reliability assessment.

A qualification of failures of the components of the system can be proposed considering the components defined by Bea, the relationship among them described above (Figure 2-1), and Reason's concept of latent failures. Individuals, either operators or managers, may produce human errors, which may take the form of active or latent system failures. Malfunctions of organizations (organizational

factors) define a state that emerges from interactions of actions and decisions by individuals. These malfunctions induce latent failures. Procedures, such as guidelines and operation manuals, induce latent failures when they are not adequate. The physical system may have local failures of its elements, which can become both active or latent system failures.

In the specific case of human errors by individuals, other human errors, organizational factors, procedure deficiencies, physical component failures or/and extreme environmental conditions may induce them. It is very usual that when system failures occur, many error-inducing conditions are present.

Previous attempts to provide a comprehensive qualitative understanding of organizational influences to technological failures or system reliability have not been successful. Turner (1978) points out that historically Social Sciences had failed to provide the understanding for the processes that lead to failures in technological systems, while Engineering had failed to incorporate social aspects (organizational factors) in the analysis of conditions that lead to system failures. Reason (1990a) states the problem, but fails to propose a comprehensive model to understand the dynamics of the organizational system and its effect on the technological system. Other authors have recently recognized significant elements to consider, but a generic model where all these observations could "fit" is not available. This work attempts to contribute to the provision of this need.

The following chapter describes an approach that is expected to provide a comprehensive qualitative understanding of some complex systems. The subsequent chapters of Part I demonstrate its applicability to the understanding of organizational influences on technological failures.

3. CANL MODEL

3.1 Introduction

The CANL (Complex, Adaptive, Non-Linear) model proposed by Bella (1997a, 1998a) is an approach for understanding the processes driven by human interactions within organizations and for the explanation of their emergent outcomes. Emergent outcomes are system responses that can not be reduced to the analysis of individual behaviors and their immediate interconnections. The focus is on the "whole" rather than on the "parts". This approach was used to describe behaviors in very different organizations, including the ones that perform environmental impact assessments (Bella 1987, 1996, 1997a, 1997b, 1998a).

Structural engineers look first at the drawings, rather than the calculations. Generic loading and foundation characteristics are enough for a first "visual" assessment of the structure and its load paths. The product of the application of this model would also allow for a graphical identification of the general characteristics of the system. That is to say, a formal process is applied in order to perform a qualitative assessment.

In this work the CANL model will be applied to understand and assess the influence of organizations on the reliability of offshore systems, as a case of complex technological systems. Various applications to case studies and a methodology for its use in safety audits are presented in Chapters 4 to 6.

The general model developed by Bella is introduced in this chapter in three ways. First it is presented based on a metaphor, the CANL generator metaphor. Then it is briefly illustrated with an example, and finally it is described through a generic conceptual rationale extracted from previous applications of this approach (Bella 1997a, 1998a).

3.2 CANL Generator Metaphor

The CANL model provides a conceptual tool to understand and describe complex organizational systems. It is proposed to be a different way of looking at human organizations, based on a new "metaphor". The "causal chain" metaphor and box models (stock and flow) are replaced by the CANL generator metaphor for the understanding of human organizational systems. Bella developed this metaphor as a mechanical analogy to the conceptual CANL model. The "CANL generator" is an ideal device that produces outputs consistent with the CANL model, through the application of simple deterministic rules.

The models adopted for the understanding of different phenomena tend to shape our expectations and explanations of what is found.

> *Instead of perfect knowledge, the human organism operates with a variety of maps and models which organize available knowledge about the outside environment, and direct the collection of new information (Turner 1978).*

The awareness of this tendency to "direct the collection of new information" is as important as the assumptions embedded in a model.

The CANL model implies a different approach and is based on different assumptions. Therefore it is likely that the results produced would be different from the ones obtained with other models. The type of information required and expected is also different.

The CANL generator seeks to represent the principles that human behaviors follow within a complex organizational system. General observations about human behaviors were summarized as follows (Bella 1998b):

1. *Many different kinds of behaviors arise, often in unpredictable ways.*
2. *Some behaviors provide support to (reasons for continuing) other behaviors.*
3. *Behaviors tend to persist when they have support (reasons for continuing).*

4. *Behaviors tend NOT to persist when they lack support.*
5. *Disorders (contrary behaviors, conflicts, challenges, etc.) arise to disrupt patterns of behaviors.*

The model represents these characteristics through a set of deterministic rules. Bella (1998c) states that the CANL generator can be imagined as a device similar to a cement mixer. It churns around constituents thrown inside it so that they bond in a specific way, and through this process it produces an outcome of a nature different from the one of the original constituents.

The cement mixer provides an interesting analogy. Its product has a nature and properties different from its constituents. The outcome can be understood based on the constituents only when a very deep knowledge of the processes involved is possessed. In complex systems, however, all the potential interactions and processes are usually beyond any possibility of detailed and exhaustive analysis. In this case, the understanding has to be focused on the whole rather than the parts.

The CANL generator is fed by "behavior statements". The device throws away the statements that do not have a reason. A behavior that has a justification by another one gets bonded to it, and is retained. The behavior statements retained in the device form arrangements of interconnected behaviors.

The operational rules of the CANL generator are directly related to the general behavioral tendencies listed above (Bella 1998b):

1. *Many different behavior statements are shoveled into the generator and tossed around.*
2. *As the tossed statements come in contact with each other, arrows arise between some statements linking them together.*
3. *Behaviors with incoming arrows (support) are not ejected.*
4. *Behaviors without incoming arrows (support) are ejected.*
5. *The tossing generator can occasionally remove (break) arrows and eject statements previously supported.*

The "mixing" inside the generator is a random process. Constituents (behavior statements) get in touch with each other in a non-deterministic way. If

statements in touch are related by a justification (a reason or support of one for the other), bonds get formed. Justifications may be graphically represented as unidirectional arrows. The interpretation of these links is apparent when two linked statements are read replacing the intermediate arrow by "therefore" (if reading forward), or "because" (if reading backwards).

Behavioral statements that do not have an incoming arrow at the end of each cycle of the process get ejected from the device. Only statements with incoming arrows stay in the generator. The device is continuously being fed by a random distribution of behavior statements.

Behavior statements, for which several other statements provide reasons, are more likely to stay in the generator. Statements receiving support will be found inside the generator far out of proportion to their input rates. Statements with little support will be rare.

The only way for a set of behaviors to be sustained over time is to form loops. Open chains are easily destroyed, as there is always one statement without support. Even if their links are strong, chains do not persists inside the generator. On the other hand, loops are sustained because all statements have a reason (even if they are ultimately self-referencing). Figure 3-1 shows these two basic examples, but only the loop survives inside the CANL generator.

Over time, loops become relatively stable forming persistent patterns inside the CANL generator. Consequently, they also function as attractors for other behaviors and other loops, when statements in the loops provide reasons for other ones. Loops behave as attractors because they provide statements that can give justifications for new ones. Chains with justification provided by statements of a loop will not be ejected, since the original loop provides the stability (Figure 3-2).

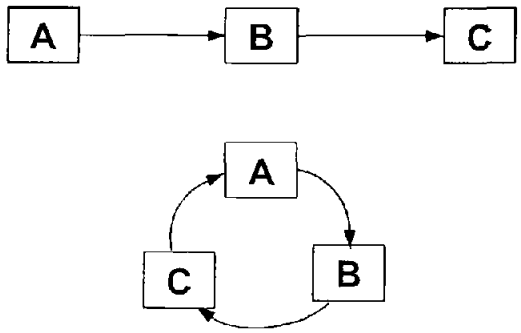


Figure 3-1
Example of chains and loops. A, B, and C are different generic statements.

One statement can be part of two different loops. Such case may be caused by the merging of previously individual cycles (Figure 3-2). Complex patterns with multiple connections can be expected as individual loops and new incoming statements get linked. When patterns of statements with multiple connections are formed, the individual links do not need to be strong (deterministic, permanent), since other links may ensure the permanence of one particular behavior through other paths.

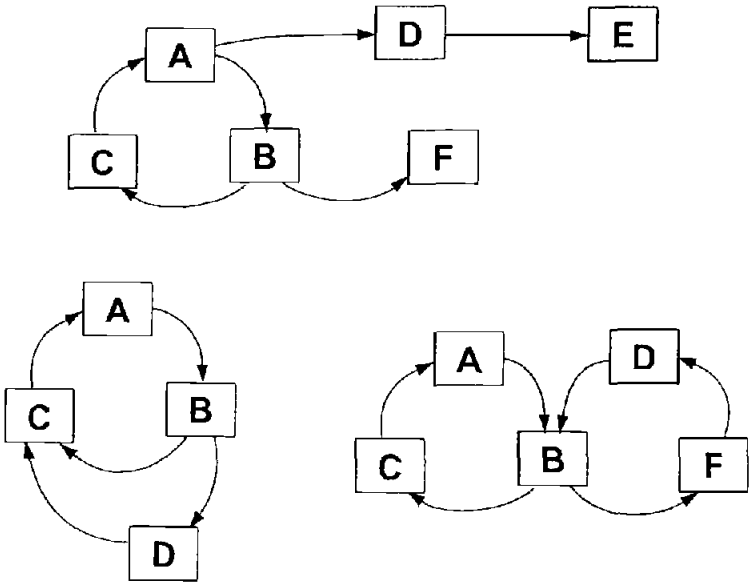


Figure 3-2
Loop as an attractor and examples of simple multiple loops.

When two statements become in contact, one statement may provide a negative reason for the other, instead of a justification as described above. If the negative support at the time of contact is stronger than the combined positive support, the statement gets ejected. The more strongly supported loops are likely to eliminate the weaker ones when they conflict with each other. Through this process, simple loops may get destroyed, and complex ones may get altered (Figure 3-3).

The relative resistance of multiple loops (as compared to simple loops) to the elimination of one of its behaviors can be shown in a probabilistic sense. Multiplicity of connections, rather than their individual strength, defines the probability of permanence of behavioral loops.

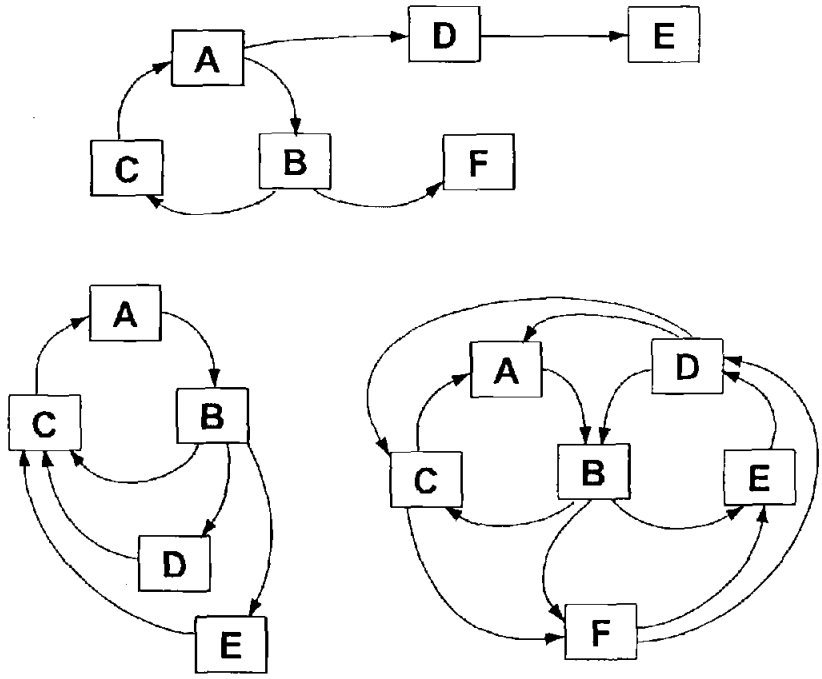


Figure 3-3
Simulation of disorders. To get a feeling of the relative stability of loops, randomly eliminate one statement and apply operational rules 3 and 4 of the CANL generator.

When inputs to the system are always the same (all statements shoveled are not conflicting and do not vary with time) a very stable arrangement can be sustained. In such case, the only behavior statements added are the ones already

being reinforced by the existing patterns. Very stable and rigid patterns develop when new behavior statements are already in context with the actual system.

The process described (following Bella 1998b) shows how complex patterns of behavior can emerge from very simple rules. It also shows that disruptive behaviors may modify existing patterns. As the process continues the contents of the CANL generator show a dynamic response. Moreover, if the relative composition of behaviors that comprise the input vary with time, the model describes an adaptive response, which is strongly non-linear with respect to its inputs.

Under the given set of rules, the product of the CANL generator (what persists inside it) evolves in ways that can be inferred. The emergent outcomes, as listed by Bella (1998b), are:

1. *Reinforcing behavioral patterns in the form of multiple loops tend to emerge, endure, grow, reform and accumulate.*
2. *Behaviors tend to endure when they are supported by reinforcing behavioral patterns in the form of multiple loops.*
3. *The individual connections (linkages, reasons) within these behavioral patterns are often tenuous rather than rigidly deterministic.*
4. *The reinforcing behavioral patterns that we experience reflect the history of disorders (the disturbance regime) from which these patterns emerged.*

The CANL generator is a conceptual model that represents a natural process in human affairs. The CANL generator by itself is "as morally concerned as a cement mixer" (Bella 1998c), even if the individual behaviors and actual outcomes that get sustained through these processes can be judged morally or legally.

The type and relative quantities of the input can vary with time, as some behaviors are more likely to occur randomly (to get shoveled into the device) at different moments. In some cases, a specific intention may induce this variation, for example through external regulations or policies in the organization. However, the resulting patterns of behavior are not (and cannot be unless all aspects of human behavior could be controlled) the product of design, but emerge through the multiple

interactions of individual behaviors. When actions disruptive to a behavioral loop persist in time, the overall pattern is modified. After the disruption, the loop could be rearranged into a very similar pattern, or flip into a completely different one. Strong instantaneous disruptions that completely eliminate certain behaviors would also produce rearrangements or elimination of the whole loop (Figure 3-3, follow instructions).

The CANL generator is a metaphor. It provides an analogy for the understanding of a conceptual model that is called here "CANL model". The CANL model provides a framework for the understanding of complex organizational systems. The model is able to provide explanations for non-linear organic responses and their evolution in time.

It has been recognized that the CANL generator could be implemented into a computer code. However, this research path has been discouraged in the past in order to concentrate efforts in the qualitative understanding of complex systems (Bella 1998c). In fact, a computer-based CANL generator would produce loop diagrams, which can already be inferred.

3.3 Illustration: Distortion of Information

A clear consequence that may be identified from the dynamics of the CANL generator is that there is a strong tendency to support certain behaviors (the ones reinforced by the system), and to suppress others. This phenomenon may lead to imbalance. It has been shown that "distortion of information" and a "shift of the burden of the proof" may develop when loops become stable due to lack of disruptions (e.g. Bella 1987, 1996, 1997b, 1998a). In particular, distortion of information is introduced by Bella (1987) with the following description:

> *...Modern organizational systems, by their very nature, distort information to meet organizational needs. Moreover, such systematic distortions do not require unethical behavior on the part of individual persons. The distortion of information is not merely the outcome of*

individual or group intent. Distortion of information is often a systemic property of organizational process sustained by basically good people. The technological consequences of such distortions can be disastrous.

The loop diagram that resulted from this approach, described above by the CANL generator metaphor, was:

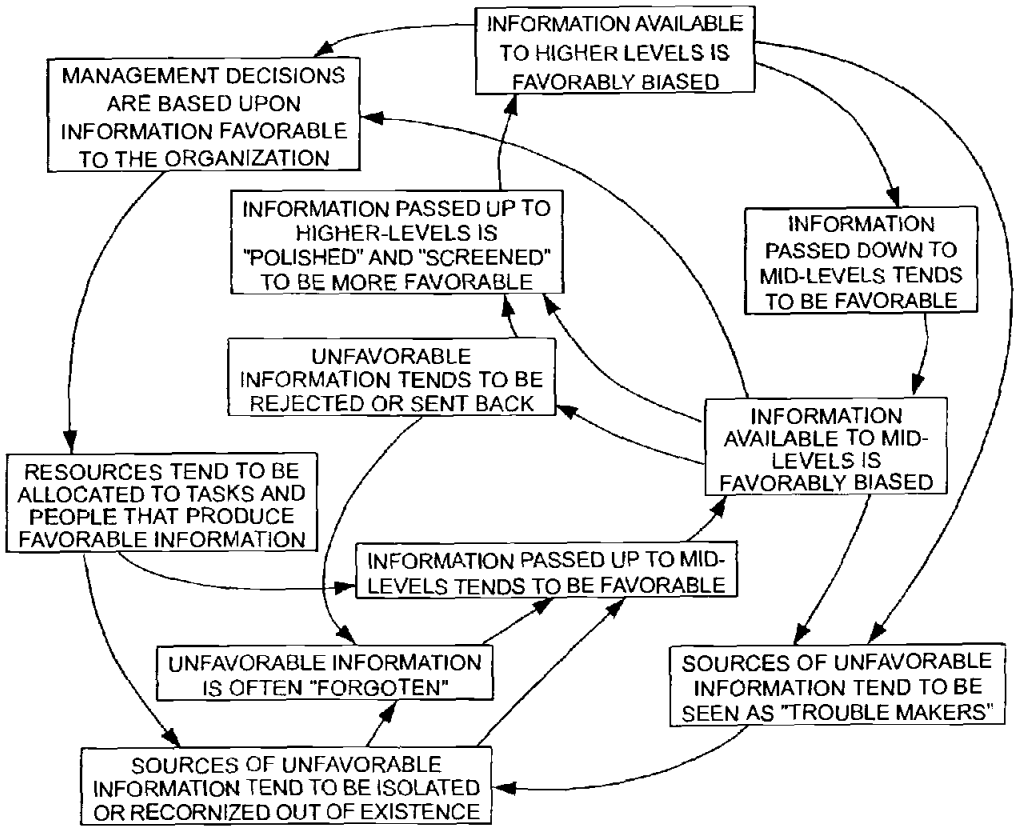


Figure 3-4
Distortion of Information Loop (redrawn after Bella 1987)

In order to understand the system described, read a statement, proceed forward along an arrow reading "therefore" or backwards reading "because". This loop diagram has been tested in conferences, seminars and courses for a long time. People usually smile as they recognize familiar patterns... This diagram summarizes the patterns of behavior within the organizational system that lead to the distortion of

information. However, this distortion is not due to the intention of the members of the organization, it is an emergent outcome.

Bella (1987) also presents an interpretation of how the organizational systems may be seen from within, for the particular case when a biased environmental assessment report has been produced (Table 3-1).

All the behaviors of Figure 3-4 are justified in the given context. They may not seem reasonable from a broad perspective (in fact, they induce the negative outcome described) but they can be justified easily in the short-term and narrow-context.

3.4 Basic Concepts of the CANL Model

This section provides an alternative presentation of the CANL model extracted from two specific applications of the approach (Bella 1997a, 1998a).

A technological system is defined as "pattern of humans, devices, infrastructure, processes, communications, resources, and procedures that interact to produce coherent outputs" (Bella 1998a). A technological system comprises both physical and organizational subsystems tightly interconnected. An organization is a system comprised of interconnected human components.

Large organizations are defined as complex systems. They are systems that adaptively change and self-organize. They display non-linear responses. The emergent outcomes of the system cannot be reduced to the intentions of the individuals that make it up. They are defined as complex, adaptive, non-linear systems; and can be described by the CANL model (Bella 1997a, 1998a).

Table 3-1

Organizational system as seen from within. Distortion of Information (Bella 1987).

Person in the System	Question	Assumed answer to question
Higher-level manager	Why didn't you consider the unfavorable information your own staff produced?	I am not familiar with the information that you are talking about. I can assure you that my decisions were based upon the best information available to me.
Midlevel manager	Why didn't you pass the unfavorable information up to your superiors?	I can't pass everything up to them. Based upon the information available to me, it seemed appropriate to have this information re-evaluated and checked over.
Professional technologist	Why wasn't the unfavorable information checked out and sent back up to your superiors?	That wasn't my job. I had other tasks to do and deadlines to meet.
"Trouble-maker"	Why didn't you follow up on the information that you presented?	I only worked on part of the project. I don't know how my particular information was used after I turned it in. I did my job. Even if I had all the information, which I didn't, there was no way that I could stop this project.
Higher-level manager	Why has the organization released such a biased report?	I resent your accusation! I have followed the development of this report. I have reviewed the drafts and the final copy. I know that the report can't please everybody but, based upon the information available to me, I can assure that the report is not biased.
Midlevel manager	Why has the organization released such a biased report?	It is not just my report! My sections of the report were based upon the best information made available to me by both my superiors and subordinates.
Professional technologist	Why has the organization released such a biased report?	It is not my report! I was involved in a portion of the studies that went into the report. I completed my tasks in the best way possible given the resources available to me.
"Trouble-maker"	Why has the organization released such a biased report?	Don't ask me! I'm not on this project anymore and I really haven't kept up with the project. I turned in my report. It dealt with only a part of the project.
Higher-level manager	Why was the source of unfavorable information (the "trouble-maker") removed from the project?	I hardly know the person. A lot of people have worked on this project. I must, of course, make decisions to keep this organization running, but there has been no "plot" to suppress people! On the contrary, my decisions have been objectively based upon the available information and the recommendations of my staff.
Midlevel manager	Why was the source of unfavorable information removed from the project?	I don't like your implications! I've got task to complete and deadlines to meet with limited resources. I can't let everybody "do their own thing"; we'd never finish anything. I base my recommendations and assignments on the best available information!
Professional technologist	Why was the source of unfavorable information removed from the project?	I'm not sure about the details because I don't work with him. I guess that it had to do with a reorganization or a new assignment. He is a bright person, somewhat of an eccentric, but I've got nothing personal against him.
"Trouble-maker"	Why were you removed from the project?	My assignment was completed and I was assigned to another project. I don't think that anybody was deliberately out to get me. My new job is less of a hassle.

Individual human activity within CANL systems is unpredictable, however it displays non-arbitrary tendencies. Generic tendencies can be described or explained by patterns of behaviors and their outcomes. Individual actions, decisions and behaviors are non-deterministic and unpredictable, but self-reinforcing patterns induce tendencies. "Organizational systems are defined by the mutually reinforcing networks of information and resource transfer that provide coherence and coordination to human activities" (Bella 1997a). Self-reinforcing patterns of behaviors are emergent outcomes of organizational systems that shape, condition, and provide context to the behaviors of individuals within it.

"Complex organizational systems can be characterized by a dominant attractor, through which resource flow, information and activities are mutually reinforcing" (Bella 1998a):

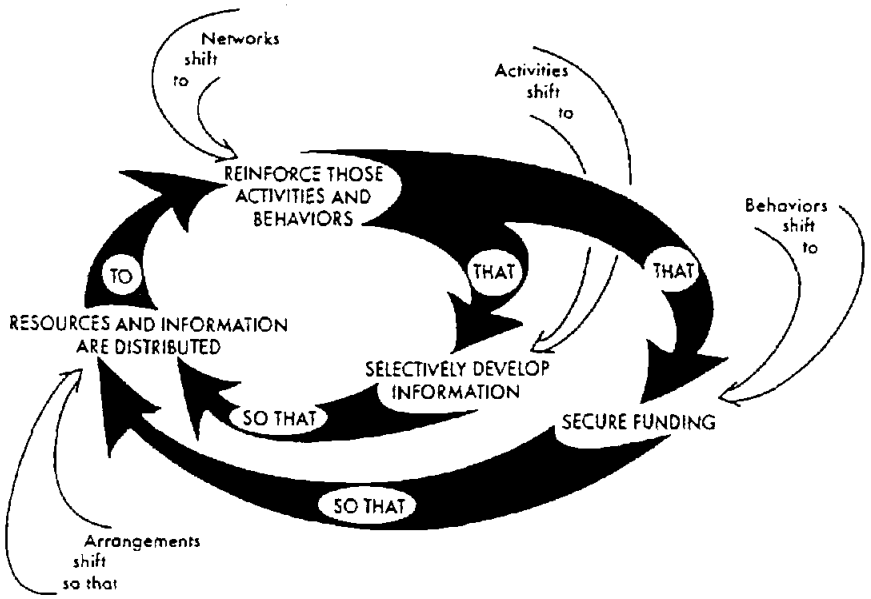


Figure 3-5
The Dominant Attractor (Bella 1997)

This "dominant attractor" or pattern of self reinforcing behaviors, has been shown to occur in very different organizational systems (Bella 1987, 1997a, 1998a,

1998b), and in the following chapters it will be shown that it affects the reliability of offshore systems (and complex technological systems in general).

Behaviors compatible with the patterns of the system are more able to endure. Human activity tends to settle into those patterns of reinforced behaviors. Behaviors that do not fall within systemic patterns constitute disorders and can destroy or rearrange existent patterns. Therefore, disorders naturally tend to be dampened. Systemic patterns tend to endure when disorders are successfully dampened below disruptive levels.

Failures in technological systems are a particular kind of disruptions when they are internalized. The complete loss of a platform is a significant internal failure for an oil company, due to its large economic impact. The environmental impact of continuous minor spills and leaks could be externalized. For example, they may have no significant impact on the company if not realized by government agencies or environmental groups. The consequences of internal failures (disruptions) involve an adaptive systemic response of the technological system.

The processes that produce systemic patterns of behaviors are dynamic and organic. The interplay of order and disorder shapes the character of the system. Order is found in reinforcing patterns; disorder is found in events that disrupt established patterns. "The systemic behavior of an organizational system –in particular the activities it tends to reinforce and suppress– reflect its history of experienced disorders" (Bella 1997a).

The persistence of behavioral patterns depends on the successful dampening of disorders. Behaviors within the system are systematically reinforced or suppressed according for their potential for production of disorders. As only certain behaviors are sustained, systemic imbalance emerges. Systemic imbalance is a natural tendency of self-organizing systems. It is an emergent outcome, which does not require the intention of individuals within the system. "As organizational systems shift to dampen disorders over time, they tend toward systemic imbalance, reinforcing some activities and suppressing others" (Bella 1997a).

Catastrophic failures can emerge from histories of accumulating behaviors – latent failures as defined by Reason (1990a)– induced by systemic imbalance. Systemic imbalance causes what Bea (1994) defines as contributing and compounding factors of accidents. In many cases, however, each individual within the organization is performing as expected, doing "his job", and still a negative outcome can emerge.

Productivity and safety are typical types of activities that may become conflicting and selectively reinforced and suppressed within a technological system. If behavioral patterns tend toward a systemic imbalance that reinforces productivity activities and suppress safety (maintenance, independent checks, and certain production limitations), probabilities of major failures increase significantly. Others (e.g. Schulman 1993) have observed this tendency, which is often called "degradation". It has been also recognized that conflicts between production and safety, resource constraints, and time pressures are common factors that reduce safety (Gudmestad and Gordon 1997, Paté-Cornell 1995).

Unless a minor failure or an alarming safety report produces a disruption to rearrange the degraded patterns of behavior, a major failure should be expected. Frequently, these warning signals are dampened below disruptive levels, and systemic imbalance is preserved. Systemic imbalance creates conditions for latent failures to flourish. It creates contributing and compounding factors that increase the probabilities of system failures or "normal accidents".

Information has the capacity to amplify or dampen disorders (Bella 1987). As organizational systems tend towards less disruptive arrangements, there is a natural systemic tendency to distort information. Information would be shaped to sustain, rather than disrupt, self-reinforcing organizational patterns. "As organizational systems adaptively shift in their normal manner, they settle into patterns that distort information to serve systemic needs" (Bella 1997a). Systemic distortion of information explains the lack of response to significant minor failures and alarming safety reports, that is, no action after warning signals. Many post-mortem studies

have been able to identify the "early warnings" that were not considered before an accident.

Premises and assumptions are basic to all human behaviors (including engineering assessments). They may also cause disruptions of systemic patterns of behavior if they are challenged. "Organizational systems tend toward the reinforcement of some premises and the suppression of others" (Bella 1997b). In particular, a crucial premise for decision making under uncertainty is the burden of the proof (which of two conflicting alternatives is required to be proved to justify a decision). The natural systemic tendency is to demand a higher degree of evidence to decisions or actions that may disrupt systemic patterns. Conversely, actions or decisions that are reinforced by the system require no additional evidence. "When information is inconclusive, the burden of the proof tends to dominate decisions" (Bella 1997b). The burden of the proof tends to be shifted to support existent behavioral patterns and, in general, the dominant attractor (Bella 1997b).

Behaviors of individuals within organizational systems can produce systemic disruptions required to avoid the consequences of systemic imbalance. Concerned individuals that are able to see beyond their prescribed activities to become aware of potential negative outcomes of the system can produce "credible disorders". Independent checks, external audits and personnel safety concerns become necessary credible disorders to avoid technological failures.

Organizational systems can also shape beliefs of individuals through a pervasive shift of assumptions and distortion of information during long periods. This effect may be observed more clearly in certain members of the organizations. A univocal relationship has been pointed out between individual success within an organization and adjustment to systemic patterns. "As people succeed within an organizational system, their understandings of responsibility, duty, integrity, proper behavior, evidence, history and justice are shaped (molded, shifted) in non-arbitrary ways" (Bella 1997a); toward reinforced behaviors and away from disruptive behaviors.

The basic concepts of self-reinforcing patterns of behaviors, emergent outcomes, systemic disruptions, credible disorders, systemic imbalance, distortion of information and shift of the burden of the proof were summarized as a presentation of the CANL model.

3.5 Application of the CANL Model

The CANL model can be applied to a complex system of the human kind through a discipline based on the "search for behavioral loops". Bella applied it, in different forms and stages of development, to several cases (Bella 1987, 1996, 1997a, 1997b, 1998b). Loop diagrams provide the graphical representation of the results. In loop diagrams, each behavior is described by a statement, and unidirectional arrows represent the links that provide their justifications. Arrows are to be read "therefore" when reading forward between statements and "because" when reading backwards.

One basic characteristic of the methodology is to get information provided by members of the organization, "listen to their stories". It is important to identify in the wording of the statements when they only represent a point of view (of an individual or a group), rather than a fact.

Experience of acting these behaviors is of significant value. When individuals are aware of justifications for their own behaviors within their organizations, they may provide information to describe dysfunctional systems. In particular, it has been mentioned that "frustrations of concerned individuals" are a valuable source of information to describe the system with this approach (Bella 1998b, 1998c). Individuals that are able to "see beyond their specific responsibilities" and are aware of systemic pressures provide important insights into the organizational system.

This method for obtaining information does not seem as a typical Engineering one at a first glance. However, professional engineering assessment does make use of lessons gained through experience. The formalization of this

process, however, is weak. Blockley (1980) points out this fact when he defines "Social Sciences of Engineering" as the missing aspect in Engineering formal education and communication:

> *The exchange of experiences through discussion is one of the important functions of the professional 'learned' societies ... Such discussion occurs at an informal social level, which is often rewarding in itself, and at a formal level of discussion of technical papers... A feature of them [at formal level], however, is that they rarely discuss design and organizational decisions; they concentrate almost entirely on technical detail...*

That is, our professional practice does not have a formal means for communication and discussion of "experience" as a source of technical data. Influence of organizational factors in usual engineering practice is largely limited to coffee break chats. The CANL approach could contribute to the establishment of a formal framework to introduce relevant experience, which is of significant importance to reliability issues.

The "Story of a Platform Audit" (Bea 1996) provides an example of information that can be employed by the CANL model. This reference is a rather unique example in the engineering literature on reliability of offshore systems. Information obtained by personal dialogue was used in that case to assess the accuracy of a formal quantitative reliability study of an offshore platform.

Among other examples, Bea (1998b) proposes similar approaches as part of the SMAS methodology, Embrey (1992) includes this approach explicitly in the MACHINE methodology, and Hokstad *et al* (1998) includes it as part of the process to use expert judgement in reliability studies.

Another significant concept embedded in the CANL approach is that "all behaviors have a reason". The rules described indicate that only behaviors that have justifications may persist. In many cases, these justifications could be understood as such only within the existing context. The systemic patterns of behavior provide the context.

Finally, the aim of the discipline is to understand the system, not to blame anyone. Pugsley (1973) reminds that:

> *As more and more structural accidents are studied one becomes increasingly aware that the appointment of blame ... is in human society much less important ... than the appreciation of the broader factors that have produced the 'climate' in which the accident is set...*

The CANL model assumes that reinforced behaviors and negative outcomes may persist without any individual's intention to produce harm. Intention to harm may exist, but it is not necessary for the occurrence of negative outcomes and it is not the objective of the application of the model.

The existence of behavioral loops can usually provide an explanation for "unexpected", unwanted or negative outcomes of organizations. These are emergent outcomes, which are usually not apparent to individuals within the system. They can explain failures. Systemic imbalance, identified by the application of the CANL model, indicates a reduction in the reliability of a technological system. This "climate" can be assessed before a failure, but –paraphrasing Pugsley (1973)– "this does not mean that they could point to a particular mistake ... that would lead to an accident". It defines a "state", according to the definition of Bea (1994).

The application of this model is an exercise of capturing the essential behavioral patterns of an organizational system, mainly through information provided by its members. Overall patterns assessed with this model are similar, even if different evaluators may vary the wording for the statements and some links. Loop diagrams are a valuable tool for a disciplined understanding of behaviors induced and reinforced within organizations.

Peer review also improves the descriptions. All members of an organization can discuss loop diagrams and concepts of the CANL model. Different individuals, without a deep specific training, can review the results obtained. In this respect, this method can become a tool for diagnosis and communication that may break professional or hierarchical barriers (which are reinforced by some other

approaches). The method of validation is based on the response by individuals from the system.

The result is proposed to be general and representative of the main characteristics of the system, with few details. By no means this approach is intended to replace more detailed quantitative methods, but it is aimed at complementing them. In some cases it may provide an overall check (as a paper and pencil order of magnitude check for a computer model output is usually performed in structural engineering). It can also help to identify "the question" that is most appropriate for quantitative methods to address. In general, it can point out considerations that should be included in quantitative analysis, or show the limitations of certain analysis.

A specific methodology proposed for the application of the CANL model to the assessment of the safety within a technological system is presented in Chapter 6. The CANL model is applied to several case studies in Chapters 4 and 5. In Part II, the model is also used as a basis for the analysis of reliability formulations.

4. CASE STUDY – "STORY OF A PLATFORM AUDIT"

4.1 Introduction

The CANL model is applied to identify the behavioral patterns that lead to reductions in the reliability of an offshore system that did not fail. The initial source of information for this description is the "Story of a Platform Audit" (Bea 1996). This case provides a very valuable insight into the issue of reliability and organizational factors. It is a unique example in the ocean engineering literature where organizational behaviors are clearly described for a system where no major failure has occurred. The application of the CANL model to this data shows its usefulness as a tool for the understanding of organizational systems and for the assessing of its influence on reliability.

The author of the paper participated in a safety audit, which included a month-long series of meetings and reviews at the platform owner's head office, at the regional office and on the offshore platform. The audit also included the review of a two-year duration Safety Case based on Probabilistic Risk Analysis/ Quantified Risk Analysis (PRA/QRA), which was being performed at the head office. The PRA/QRA based study was budgeted in excess of $2.5 million. The studies and audit were triggered by the desire to extend the life of the facility another 20 years (Bea 1996).

The epilog of the "Story of a Platform Audit" reads (Bea 1996):

> *At the end of this set of experiences, to say the least, I was concerned. I had seen the perversion of a technology and a way of thinking that I firmly believed in. I had seen hard-won progress to achieve safety rendered much less effective in the wake of re-engineering. I witnessed a greed of technology to perform PRA/QRA based Safety Case studies that bore little resemblance to the realities of the platforms. I could only feel that there had to be a better way to use technology and scarce resources to achieve safety.*
>
> *As I left the platform, I commented to the OIM [Offshore Installation Manager]: 'it might have been better if the money and effort that had been invested in performing the Safety Case study was invested in*

making some of the obviously needed improvements on the platform'. He replied, 'dream on and have a safe trip home'.

None of the platforms on which these auditing experiences occurred have experienced any major accidents. This is a tribute to the operating personnel, engineers, managers and organizations that are able to keep these systems out of harms way.

Loop diagrams according to the CANL model were performed for the description of this system. Statements directly obtained from the "Story of a Platform Audit" (Bea 1996) are first presented in different diagrams as loops or chains. Each partial diagram contains statements related to one concept or piece of information provided by Bea. Then, basic concept diagrams are condensed and rephrased, and finally merged into one general loop diagram. The strength of this approach is that it shows the global patterns of behavior that tend to reduce the reliability of the technological system. The basic concepts that will be described are common to different systems (Bella 1987, 1997, 1998), and have been identified in studies related to the offshore oil industry (e.g. Paté-Cornell 1995, Gudmestad and Gordon 1997, Gordon 1998):

- Search for profit, demand for productivity increase
- productivity vs. safety conflicts
- work overload, time pressure
- systemic distortion of information

4.2 Productivity and Safety

A loop that reinforces productivity demands and cost-cuts can be sketched based on quotations provided by Bea (1996). This loop includes specifically two levels in the organization (management, and engineering and staff at the head office) and an environmental influence (stockholders) that directly influence decisions within the organization.

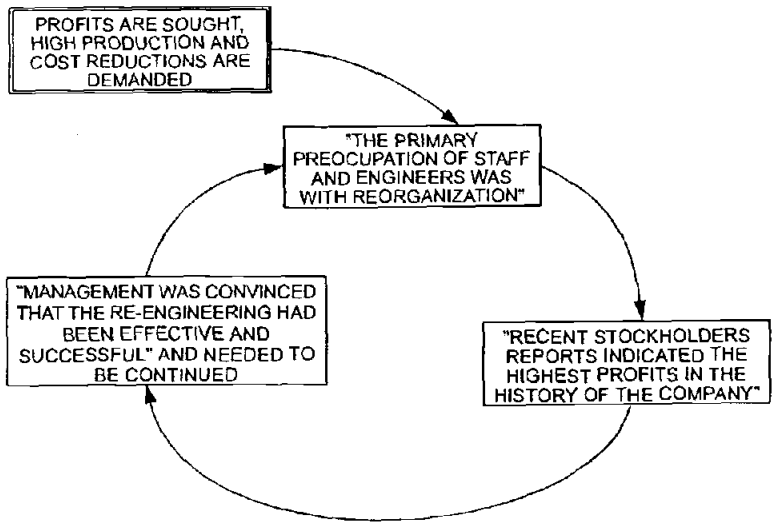


Figure 4-1
Productivity demand (re-engineering) loop based on the "Story of a Platform Audit". Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps back and forth.

Productivity is an "ideal" sought by most levels of the organization, as part of a natural aim at profits. The purpose of any commercial enterprise is to obtain profits. The placement of a too strong value on one required characteristic of a system, however, increases the tendency for imbalance. Since commercial organizations acting in a hazardous environment experience a conflict between productivity and safety (Reason 1990a, Sagan 1993, Gudmestad *et al* 1996, Paté-Cornell 1995), this imbalance may affect reliability.

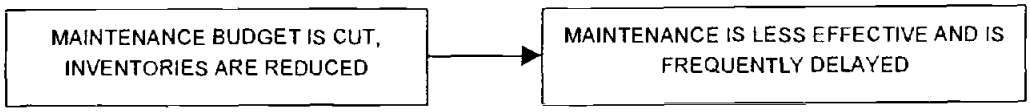
In this case, Bea describes how techniques to improve productivity are encouraged in a context of short-term objectives. The general concept was also described by Reason (1990a) as: "decisions oriented to improve productivity have a high certainty about their output, and an unambiguous, rapid and reinforcing feedback".

"Although it is widely recognized that ignoring safety can be more costly than giving it attention, it is often the case that production is the main focus" (Gudmestad and Gordon 1997). Paté-Cornell (1995) uses the image of "myopic

approach to financial performance", when short-term profitability is the foremost concern. The CANL model is able to provide an explanation to this common phenomenon.

Bea (1996) mentions downsizing, outsourcing and budget cost-cuts as primary results of the re-engineering effort. As a direct consequence of all of them, "this platform had become very dependent on contract crews" (Bea 1996). Because of budget reductions, contracts were based on a low bid process, which in turn induced contractors to "use marginally trained and experienced personnel" (Bea 1996). A direct consequence mentioned by shift foremen and the Offshore Installation Manager (OIM) was that in several instances "contract crews had come close to causing a major accident that was narrowly avoided" (Bea 1996). A simple chain of statements can be constructed as:

The budget for platform maintenance was also reduced. During a maintenance procedure to replace the gaskets of an emergency shut down valve, it was observed that the valve operator stem was severely corroded and eroded. The stem was not replaced because there was no replacement on the platform. "Due to cost cutting, the inventory of spare parts on the platform had been reduced to a bare minimum" (Bea 1996). The replacement had to wait for the order and delivery procedure and for the next scheduled shut down.



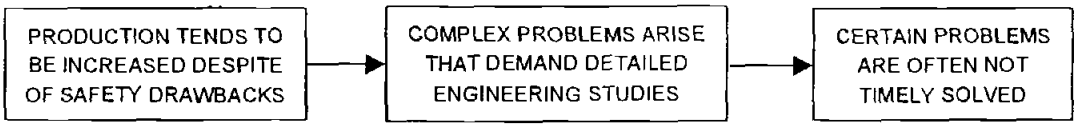
Beyond outsourcing and cost-cuts, the demand for increased productivity also has consequences in relation to safety. Upgrades and modifications are usually a difficult task in complex tightly connected physical systems. An increase in gas production had caused severe vibrations in the well head piping. In this case, "engineers 'on the beach' had been studying the problem for several months" (Bea

1996). Meanwhile, platform personnel had placed tires between some of the vibrating well head piping and rope snubbers were tied on the lines in an attempt to reduce vibrations. Operators hoped that "they [onshore engineers] would develop a solution soon and that the necessary work would be authorized and completed before one of the lines fatigued and ruptured" (Bea 1996).

It is worth noting that many decisions and actions during operation may shift components away from their design conditions. While this behavior can be done randomly under normal conditions, it is heavily stimulated and far more frequent when there is a strong productivity demand.

Some drawbacks of production facilities (presumably also resulting from upgrades) were not under study for improvement. The vent stack of a high-pressure gas reinjection facility was located next to the helipad, control room and quarters. The reason why this occurred was that "there was no place else to put it" (Bea 1996).

The following chain may describe a generic statement referred to these cases:



The core loop is rephrased and extended to include some of the consequences with safety implications that get attached when an increase in productivity is reinforced (Figure 4-2). The core loop behaves as an "attractor" of other behaviors.

The behaviors added induce the emergence of new consequences. In this local view, the attached statements are interconnected but do not reinforce the main loop. In fact, they all lead to an outcome of reduced reliability through different paths. The reliability of physical components and subsystems tend to be reduced due to persistent patterns of self-reinforcing systemic behaviors, even if at one specific moment not all of them were present.

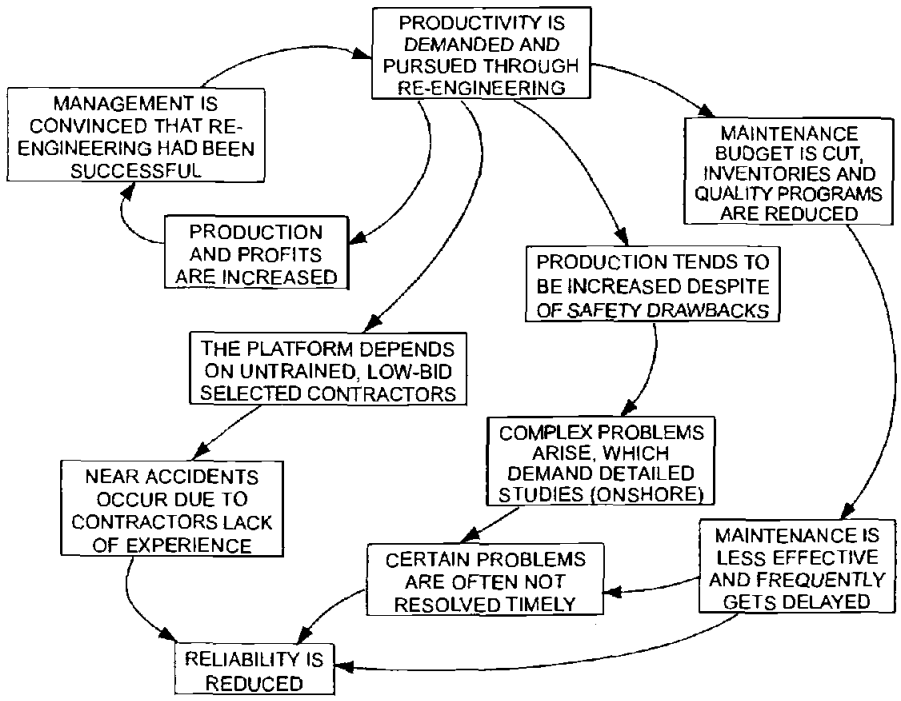


Figure 4-2
Extended productivity loop.

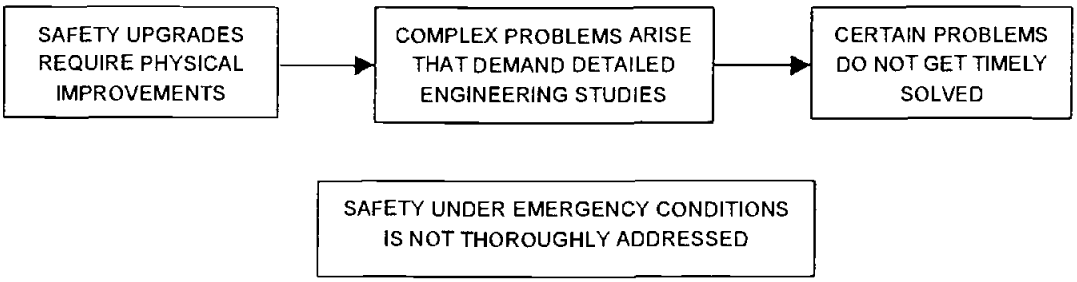
4.3 Safety Systems

Safety is a significant concern in the offshore oil industry. Any major failure has a direct economical impact and is likely to produce personal injuries and human losses. Most platform failures cannot be externalized; thus the aim is to avoid them. However, sometimes actions are not effectively taken to ensure safe operations. Bea (1996) describes several deficient safety systems.

Escape ways had been retrofitted into the platform. One of them went through the machine shop. There were several problems of potential and actual blockage of escape passages. "Unsecured floor-to-ceiling high tool cabinets lined the escape way through a part of the machine shop" and "in the center of the red-line marked escape way was an anvil" (Bea 1996). The problem had been identified

during a safety audit two years ago, but nothing had been done to correct the situation.

Some structural modifications related to safety were also defective. The complexity and tight coupling of the system made that modifications with adequate functionality and high reliability were extremely difficult to achieve. The platform control room power supply, instrumentation and communication cables were exposed next to the high-pressure gas reinjection unit. Studies for the protection took more than one year, and a solution providing protection and maintenance was not achieved yet. This information could be summarized as follows:



Safety procedures for routine activities were very thorough. Extensive, detailed and complex volumes of safety procedures had been developed. Meetings and briefings related to safety programs were frequent. Shift foremen mentioned an "endless succession of safety meetings" (Bea 1996). Heavy emphasis was given to routine and daily procedures. Daily safety measures were observed to be successfully enforced. As previously mentioned, it is a given condition that the organization considers safety a major objective. A simple loop is proposed in Figure 4-3 to describe these conditions.

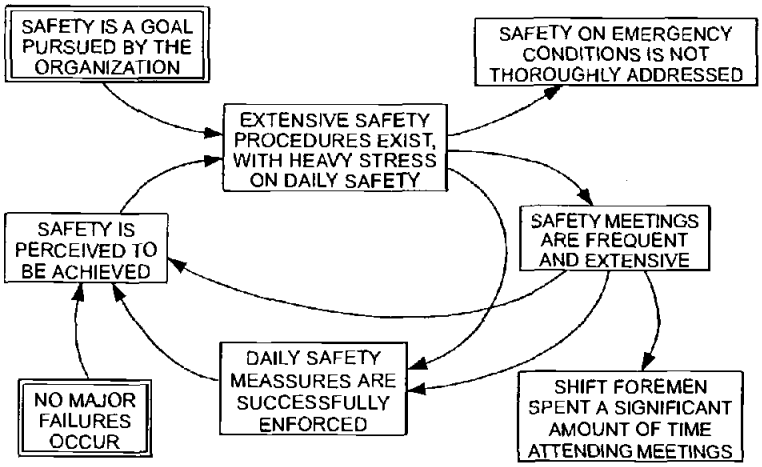


Figure 4-3
Safety loop. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; try to follow several paths back and forth repeating the previous steps.

4.4 Time Pressure and Work Overload

Work overload and time pressures are usually a significant organizational factor identified in previous studies (Bella 1987, Paté-Cornell 1995, Gordon 1998). Bea describes some of the working conditions of the OIM, which may fit this general characterization. The OIM defined his computer as "blessing and a curse". "The volume of correspondence and email had grown to such proportions, that he spent most of his time responding to inquiries and providing information on the platform production operations" (Bea 1996). He had little time left to perform walk downs on the platform. If the OIM had declared to be stressed as a consequence of work overload, that would have induced slips or lapses. However, the impact as described seems to induce knowledge-based mistakes. It is apparent that his awareness of the actual state of the platform and his ability to make assessments about it is diminished. The replacement OIM told the auditor that, "there are going to be some changes made before he became trapped behind the computer monitor" (Bea 1996). This "side comment" provides information of a "feeling" with which many other

individuals may identify. Some statements of the loop are not directly obtained from the data but inferred. A basic loop diagram is presented in Figure 4-4.

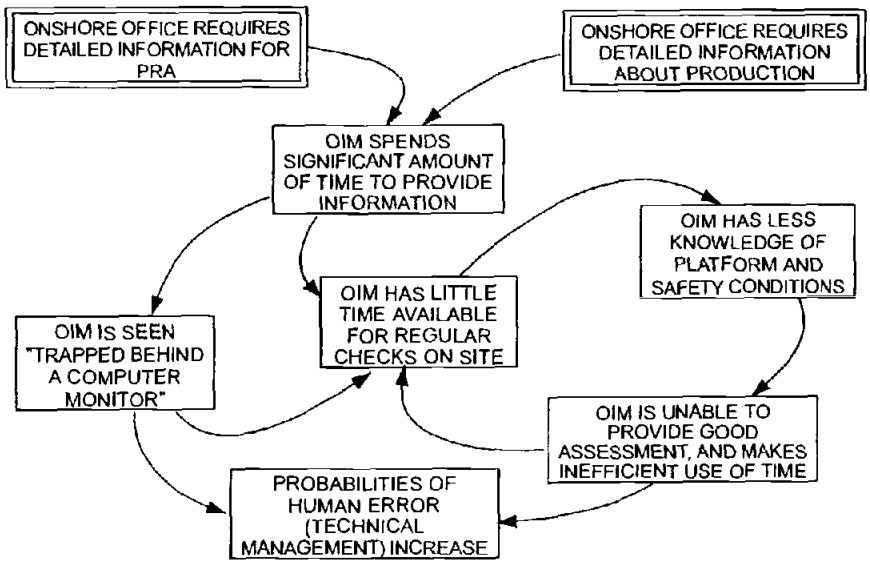


Figure 4-4
Example of work-overload loop for OIM

This is not an unusual circumstance. Wu *et al* (1991) quote from a safety report of nuclear power plant: "supervisors do not have sufficient time to be in the plant to directly observe and supervise the efforts of the work force".

A similar work-overload loop can be developed for the operating personnel. Consequences of previous local chains and loops provide statements that feed this loop. Extended supervision and paperwork related to contract crews, requests for information from regional office to feed the case study quantitative model, and proliferation of safety meetings are some of the time demanding activities described. In this case, even the formal requirement of safety measures affects the effectiveness for dealing with lower probability critical conditions. Work demands due to activities related to contractor crews (including supervision, paperwork, and specifications) are identified as significant so that foremen "often did their primary work during offshift

hours" (Bea 1996). Work overload and time pressures are typical human factors that increase the probabilities of human errors.

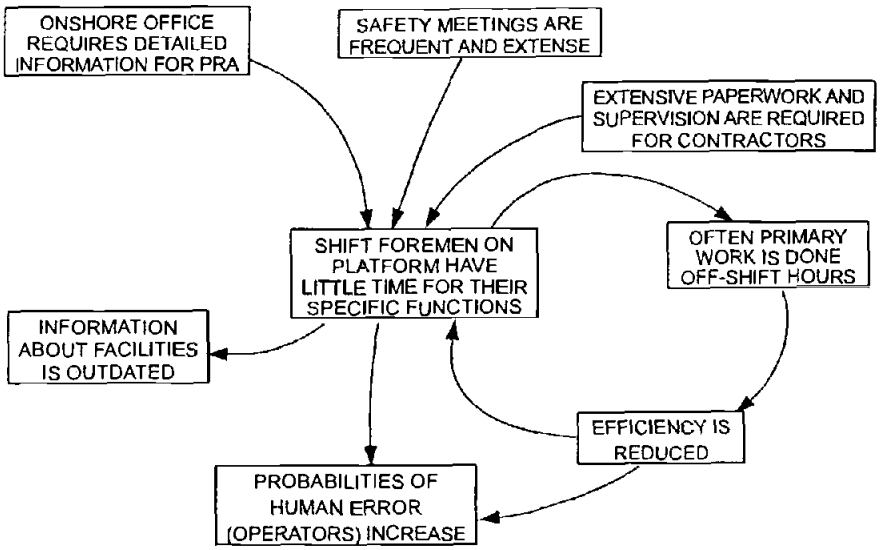


Figure 4-5
Example of work-overload loop for foremen.

4.5 Simplified General Loop for the System

A general simplified loop diagram of the system described by Bea is presented in Figure 4-6. It synthesizes behaviors and facts into general statements, and shows the most significant relationships among them.

The main consequences of the demand to increase productivity give support to further interconnected statements. Several modifications to the original design resulted in less than ideal solutions or caused problems, which were identified but not solved timely. A tendency to give priority to physical modifications in order to increase production despite of their safety drawbacks is observed. This behavior contributed to the emergence of complex, highly interrelated problems, where a win-win solution to the conflict of production and safety was difficult to find. In several

cases described by Bea, long delays occurred before any action was taken. Maintenance was also delayed or done inefficiently due to budget cuts. Outsourcing under the circumstances described produced an increase in potential accidents and a strong time demand for paperwork and supervision by platform personnel. Platform personnel mentioned the obvious lack of adequate response to maintenance and repairs that influence safety as reasons for distrust for "onshore engineers" (Bea 1996).

Extensive safety studies covered only some aspects, mainly daily safety procedures. An expensive PRA/QRA based Safety Case Study was being performed. Some flaws were identified in the study, mainly related to the quality of the information used in the model (in many cases outdated) and the lack of consideration for actual operating and safety issues. It was observed that consultants and company engineers participating in the study did not usually visit the platform (Bea 1996). The fact that a large sum was spent in a safety case study, that no major failures occurred and that routine safety programs were successful may have induced the corporate management to think that safety was not at stake. In fact, at the main office no one seemed to be worried by actual safety conditions.

However, it can be readily seen that several characteristics of the physical and organizational aspects of the system had reliability lower than expected. The auditor specifically noted this conclusion.

> Several of these unsafe conditions existed for long time. Two years before, "the earlier auditing team had identified 108 'high priority' things that needed to be corrected... Most of these things were still not corrected. But, they were being evaluated and studied" (Bea 1996). Still, the general opinion regarding safety by the corporate management was assumed to be good. There was no strong action towards the solution of obvious problems and the central concern in the head and regional offices (onshore) was the extension of the operating life and production increase.

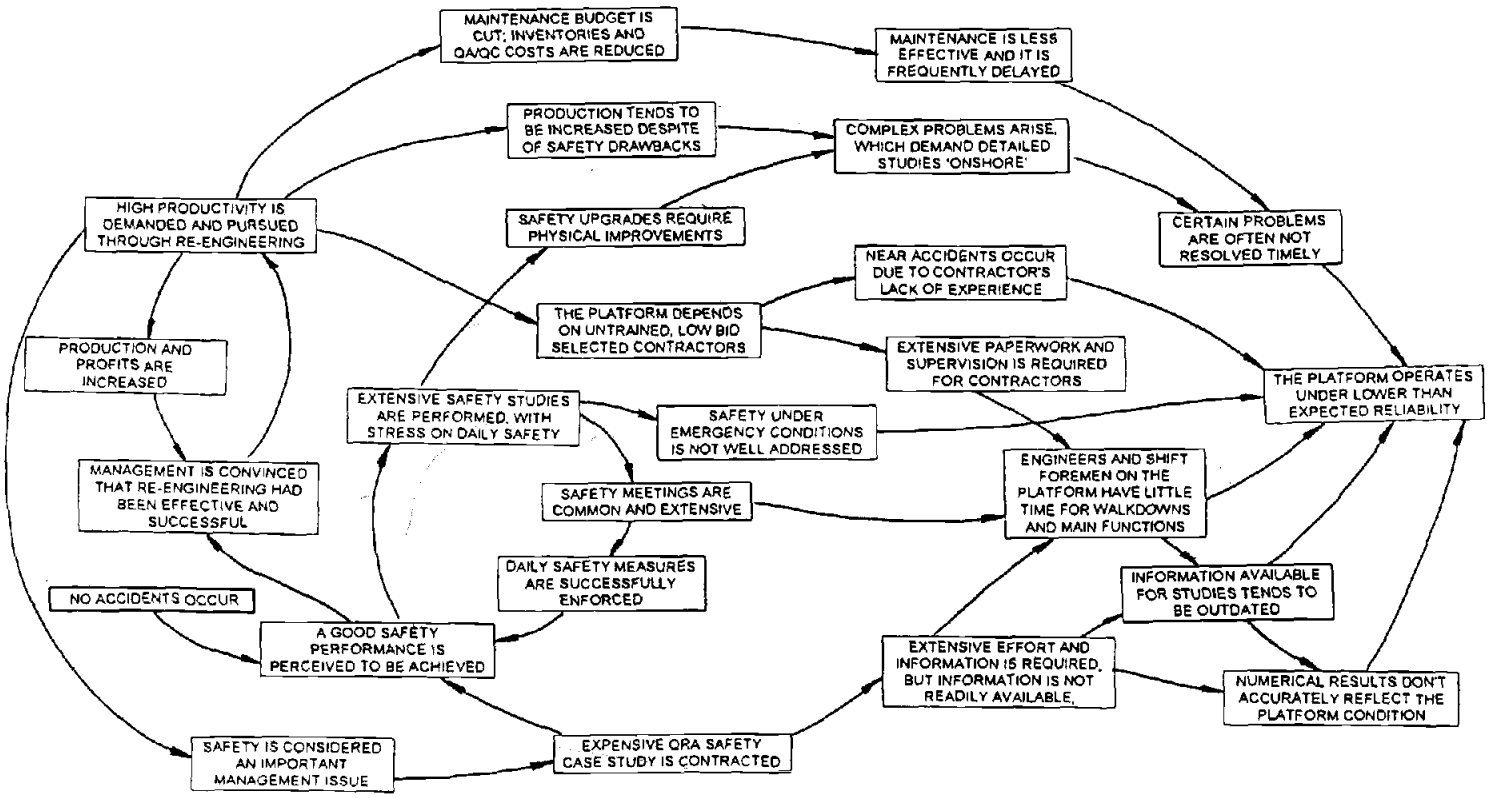


Figure 4-6

Simplified general loop diagram for the system. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

4.6 Observations from the CANL perspective

Following the principles of the CANL model, all behaviors need a justification to persist. Most of the behaviors described do have a justification. However, there is a seemingly inconsistency between the facts that "the platform operates under lower than assumed reliability" and "management was convinced that re-engineering had been effective and successful" and that safety is perceived to be achieved. The paradox upsets the auditor.

The only way both these statements can persist under the assumptions of the CANL model is if information about the actual state of the platform is not delivered effectively to the corporate management. This is not, of course, a condition that managers should ignore. Only a selective filtering –in which members of all levels of the organization participate– can allow for "closing the loop". The description available in the "Story of the Platform Audit" is only missing information about the way information gets distorted. The application of the CANL model reveals a gap in the data.

Several hypotheses could be raised to fill the gap in the description. During an audit, additional question would be asked to members of the organization in order to get the missing data. In this case, some alternatives are presented and a feasible hypothesis is proposed. In any case, following this model, some mechanism must exist to produce a distortion of information.

It could be assumed that corporate managers did not really care for safety, or that they are incompetent. It can also be proposed that middle manager and engineers tried to "hide" their faults and inefficiency, thus they may be assumed to be incompetent and untruthful. It can also be proposed that operating personnel were incompetent or not loyal enough to raise safety concerns to their superiors. All these justifications seek for the allocation of blame. Even if they may be true in some case, they are not needed to explain the outcome observed and will not be explored further

here. Pointing at someone to blame usually hides the actual systemic reinforcement of behaviors.

If no one is to blame, how can such a distortion occur? The CANL model proposes that the distortion of information is an emergent outcome in imbalanced complex organizational systems. It is a natural tendency, so it is rather widespread. It has been shown to exist in previous studies based on the application of the CANL model.

Another interesting question is, how much influence will the report by the auditor have on the organization? Judging by the previous reports, it may have not been enough to drive the top management towards effective safety actions. The "Story of a Platform Audit" also provides a tentative answer to this question. "As I left the platform, I commented to the OIM: 'it might have been better if the money and effort that had been invested in performing the Safety Case study was invested in making some of the obviously needed improvements on the platform'. He replied, 'dream on and have a safe trip home' " (Bea 1996). A member of the organization "knows" that the information produced by the auditor would not produce dramatic changes. In our language, he assumes based on his experience that it will be dampened below disruptive levels. The CANL model is able to explain this emergent outcome of the system by a distortion of information loop (see Chapter 3).

4.7 Distortion of Information

Low quality of assessment and decision making by top managers can be showed by a distortion of information loop, which Bella (1987) described through a generic diagram like the one shown in Figure 3-4.

In this case the distrust of platform personnel towards onshore engineers could also play a role. "The quickest way to not get something done is to ask engineering about it" (Bea 1996). Upper level managers did not receive the safety concerns in a compelling way. Somehow, they assumed that the "108 high priority"

issues were being taken care of, even if platform personnel knew that their concerns produced very few and inefficient responses. Onshore engineering is an area that demands exploration in order to unveil the paradox. But several issues do not involve unsolved engineering problems.

The loop presented by Bella (1987) most likely describes the lack of "feedback" to upper levels of management related to the negative impacts of cost-cuts, maintenance cost reductions and cuts of quality programs (which are in turn induced by top managers themselves). Most likely, there is also some kind of shift in the burden during the process of decision-making, so that the few signals that did get to the top management were not addressed.

4.8 Extended General Loop for the System

The previous general loop diagram is further simplified and "completed" with statements that show the distortion of information. They are hypothetical, since no direct reference is provided by Bea. They are based on experiences on other systems. In an actual safety audit, they would be provided by the answers to the new inquiries. The model allows for the identification of a kind of information to be sought.

After these additions, all observed facts follow the rules of the CANL generator. A table similar to Table 3-1 is presented as Table 4-1. As the system is seen from within, all behaviors can be "justified". Again, note that "good reasons" based on the context may not be justified given the emergent outcomes they contribute to. Moreover, they don't necessarily reflect what the individual truly believes, but rather the arguments he can show.

The emergent outcomes tend to be unknown or neglected, and short-term, narrow-context justifications are put forward. Table 4-1 is not based directly on the data provided by Bea (1996).

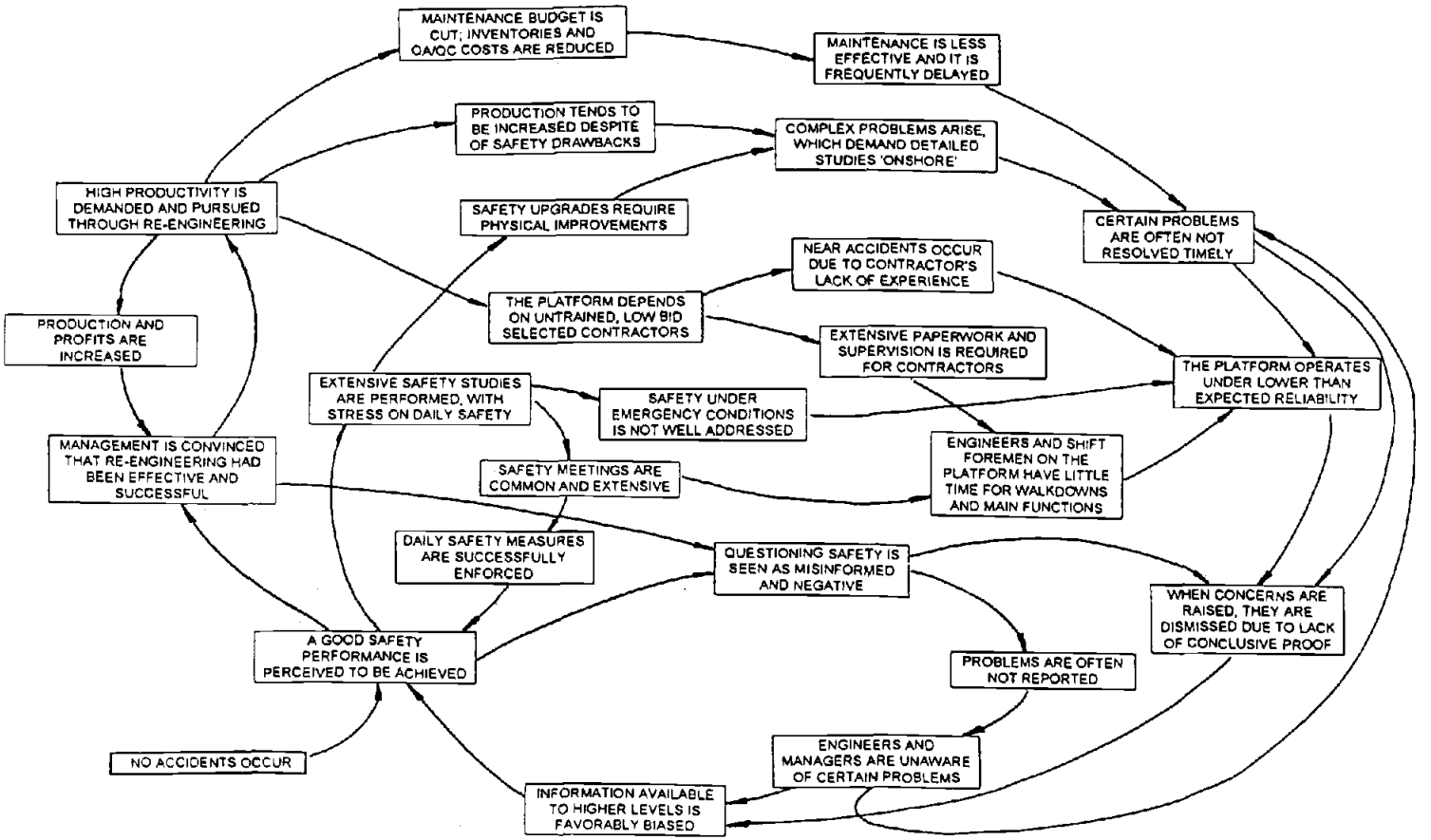


Figure 4-7

Extended general loop diagram for the system. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

Table 4-1

Organizational system as seen from within. "Story of a Platform Audit".

Person in the System	Question	Assumed answer to question
High-Level Manager (Main Office)	Why does the platform operate with so many safety problems?	I am not familiar with the problems you refer to. The company is very concerned with safety issues. I can assure you that my decisions are based upon the best information available to me. We have excellent productivity levels and we have a good safety record
Consultant PRA/QRA Safety Case Study	Why does the platform operate with so many safety problems?	We have been hired to perform a quantitative reliability analysis. We deal with long-term assessment, but we are not responsible for actual operations, repairs or maintenance.
Onshore Engineer (Regional Office)	Why does the platform operate with so many safety problems?	That is not my job. In our department we are doing our best to provide solutions for the platform. We study each problem carefully to fultill engineering and economic requirements, that is, the immediate needs of the platform and the goals of the company.
Shift Foremen (Platform)	Why does the platform operate with so many safety problems?	I also want to know that. From time to time we inform of our problems, but we don't make decisions. We do our best to have our work done safely. It is our skin, you know. But it is also our job. "You do with what you got to keep on production".
High-Level Manager (Main Office)	Why doesn't the PRA/QRA Case Study incorporate so many of the actual problems identified?	I am not familiar with the problems you refer to. We have a highly qualified team of external consultants and excellent company personnel working on that project. The company is spending a lot of money to get information based on the best engineering practice available. I am sure that if there it is a problem it will be addressed.
Consultant PRA/QRA Safety Case Study	Why doesn't the PRA/QRA Case Study incorporate so many of the actual problems identified?	Our job requires the development of a huge model. We are now using the information readily available, and requesting the missing one. We cannot face every issue at the same time. The final result would incorporate all those details, don't worry.
Onshore Engineer (Regional Office)	Why doesn't the PRA/QRA Case Study incorporate so many of the actual problems identified?	I don't know what you are talking about. That is not my job. Whenever I get an information request I answer it the best I can, and as soon as possible.
Shift Foremen (Platform)	Why doesn't the PRA/QRA Case Study incorporate so many of the actual problems identified?	I don't know. I suppose they will. For the time being, they have already asked for too much information we cannot answer. We are here to answer their questions; someone else onshore should be able to ask them. On the other hand, I have never seen any of them down here on the platform.
High-Level Manager	Why didn't you provide solutions to the '108 priority safety issues' identified two years ago?	I recent your accusation. The company has technical teams to study problems to provide cost-effective and safe solutions. Priorities need to be set; you cannot solve all problems at once. My decisions are based on the information available to me, and our records show that we are doing well.
Consultant PRA/QRA Safety Case Study	Why didn't you provide solutions to the '108 priority safety issues' identified two years ago?	That's not my job. We have a huge model to implement, and we are having a lot of work just to get the basic information to make it work.
Onshore Engineer	Why didn't you provide solutions to the '108 priority safety issues' identified two years ago?	I am not aware of that report. It's not my job to solve safety of operational issues. We study problems as we get them, and according to priorities set by others.
Shift Foremen	Why didn't you provide solutions to the '108 priority safety issues' identified two years ago?	That's not my job. I follow instructions; I don't make decisions. That is the way things work. Don't you think I would prefer a safer working environment?

4.9 Summary and Conclusions

Key characteristics of systemic behavior of complex organizations are search for profit and increased productivity, productivity vs. safety conflict, burden of proof problems, and systemic distortion of information, usually enhanced by work overload or time pressures.

An impact on the reliability of mechanical components and human members can be caused by organizational factors. It is noted that the organizational setting (states, according to Bea's definition) influences both operators and managers, the later by affecting their capacity of making meaningful assessments and thus reducing the quality of their decisions. The patterns of behaviors within the organization also alter the reliability of the mechanical or physical components of the overall system, for example through poor maintenance and structural modifications that increase complexity and tight coupling of the physical system.

The CANL model can be used to describe systemic behaviors and assess the impacts on reliability of emergent outcomes. A generic methodology for the application of the CANL model is presented in Chapter 6.

Generic loop diagrams could be developed by eliminating industry-specific wording of statements. This would be the first step towards an integration of experiences about reliability performance and organizational factors from different industries that involve complex technological systems. The distortion of information loop has proved a useful generic loop.

4.10 Loops of Offshore Oil Industry and CANL Concepts

4.10.1 Effect of Safety and Productivity Conflict

Safety and Productivity are simultaneous and usually conflicting goals. The way the organizational behavioral patterns affect the "burden of the proof" may be demonstrated by the following example constructed using basic information provided by Bea (1996).

Let's assume a condition where safety concerns are consistently enforced. A very simple loop of those "old good days" (as recalled by one of the interviewed operators in the "Story of a Platform Audit") may be assumed as follows:

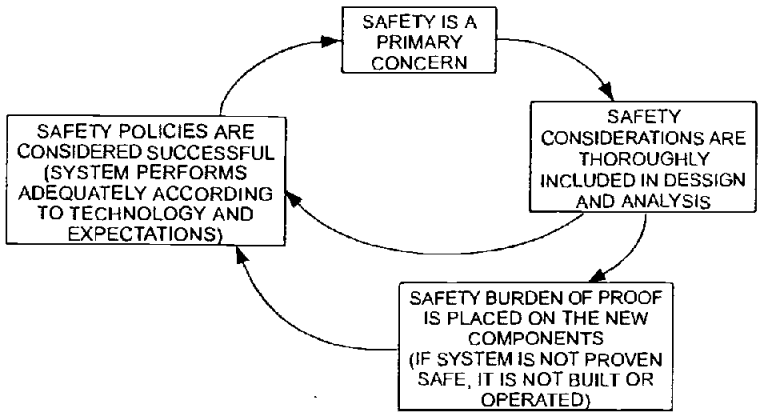


Figure 4-8
Ideal positive safety loop (that reinforces safety concerns).

This ideal pattern was disrupted by a history of decisions where the burden of proof was placed on the safety. In other words, while a Vice President of Production declared that "we are second to none in safety", he would demand that "repairs must be done without reducing production" (Bea 1996). This systematic favor of production increase over safety is directly opposing one of the main requirements of

High Reliability Organizations (see Chapter 2). The systemic imbalance reinforced by the patterns lead to a new arrangement, where the "safety concerns" have less practical consequences. In this case they are limited to routine procedures, since safety becomes a secondary aspect in projects that imply physical improvements or maintenance. A rearrangement –an organic response to the history of decisions– is presented in the next figure:

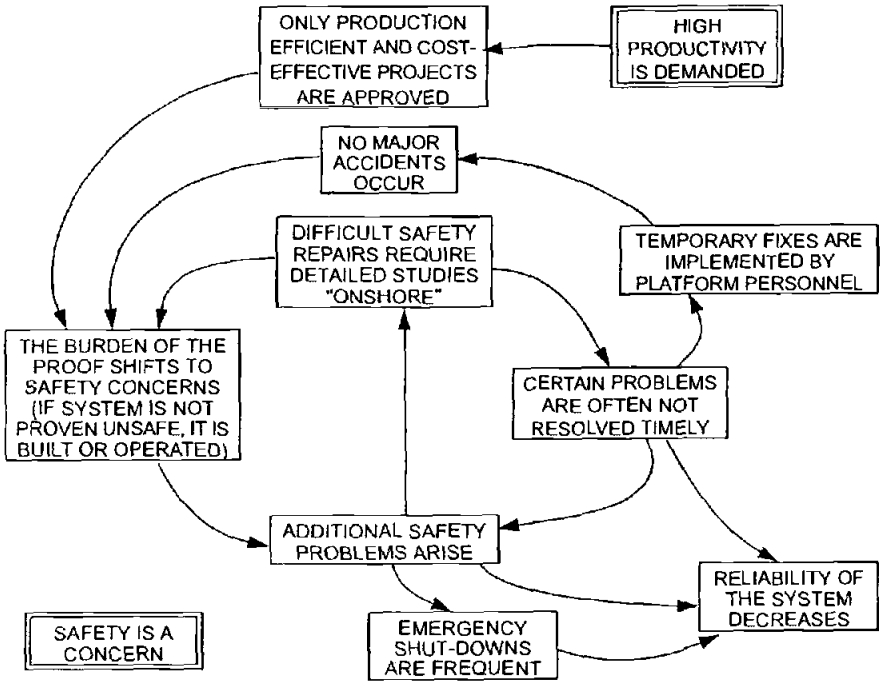


Figure 4-9

Behavioral loop that emerged after a history of shifts of the burden of the proof. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

Safety concerns have "nowhere to go" in this context of reinforced behavioral loops. In the CANL generator, even if "safety concerns" were a behavior shoveled into the device in large quantities, it would not get linked to any other persistent behavior, and most likely would finally end up being ejected. Even if nominally an objective, the pattern described (shift of the burden of the proof, time pressures and

productivity demands) prevent it to influence daily decisions and actions. The strong focus on production and the emergent systemic imbalance produce this unwanted outcome. Several different behaviors give reasons for a reduction in reliability, so not all of them need to exist permanently for their effect to persist.

The fact that "no major accident occurs" is due only partially to the efforts of the operating personnel, engineers and platform managers to keep the system "out of harms way" (Bea 1996). As time passes and negative behavioral loops persist and grow, the probability of failure increases. The lack of major accidents ends up reinforcing the behaviors that increase the probabilities of occurrence of a catastrophic one.

4.10.2 Effect of Time Pressure

Figure 4-4 describes a work overload loop diagram for the OIM, based on information provided by Bea (1996). The following section describes how that situation may have evolved from a healthier one. A sequence of loop diagrams can describe the dynamic and adaptive nature of the system.

A simple loop diagram that represents a "work load" of the OIM may be assumed for an ideal condition as follows:

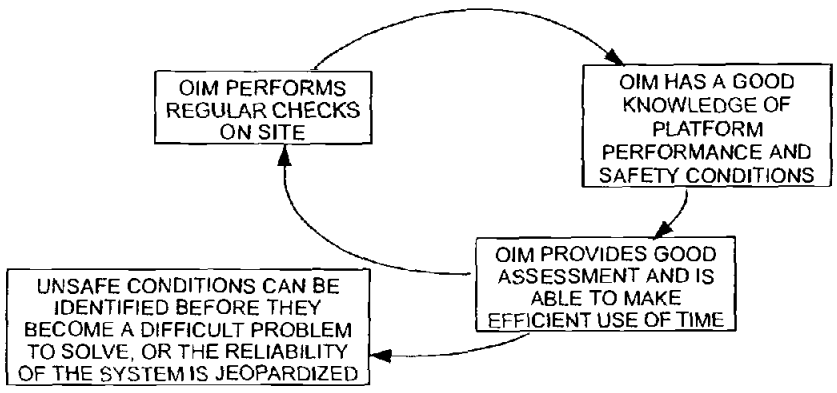


Figure 4-10
Ideal positive loop (that reinforces prevention). Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

This positive pattern that potentially existed was disrupted by the behaviors demanded by the system, described in the "Story of a Platform Audit".

The resulting pattern, shown in Figure 4-4, leads to a reduction in safety due to less reliable management assessment and decision making. This loop demonstrates one of the ways decision-makers can be affected by systemic behaviors.

4.10.3 Application of Quantitative Methods

The main point presented by Bea (1996) in this paper is the correct use of quantitative methods for the reliability assessment of offshore systems. "The purpose of these evaluations is not to produce numbers or elegant analytical constructs. The purpose of these evaluations is ... to improve the safety of such systems how, where and when it is needed" (Bea 1996). The "Story of a Platform Audit" describes a case when a quantitative methodology was not fulfilling that purpose.

The CANL model can also explain why this behavior may persist. In some cases, the inadequate use of engineering tools may contribute to the perpetuation of the problem, by hiding it. A conversation with a safety consultant included in the "Story of a Platform Audit" provides a clue (Bea 1996):

> *In the course of reviewing the details of the Safety Case studies, one of the engineers said that in his experience, one of the best Safety Case Studies that he had ever seen was written by field people, for implementation by field people, and did not contain any numbers. He said that the Safety Case studies did not have to be performed using PRA/QRA methods, but that many if not most owners/operators had chosen to use PRA/QRA in performing their Safety Case studies. I asked why he was so keen on helping perform this very intensive PRA when he had reservations concerning the utility of the analyses. He responded that this is what he had been asked to do and what his company did. His job as a contract engineer depended on performing PRA/QRA.*

A loop diagram can be developed based on this information.

This is not a unique case. The following recommendations by an experienced consultant reproduce some of these same characteristics:

In my consulting practice, I have found that one of the worst mistakes that I have made repeatedly is to accept the client's definition of the problem. If I let the client define the questions, I may give him technically correct answer –but at least as often as not, they are the right answers to the wrong questions. ... To choose the right questions requires understanding; the literature, and specially software packages, must not be expected to provide this. The practitioner must develop the necessary understanding: if he fails to do so, he is at best practicing what we used to call "cookbook engineering" (Gottfried 1996).

In the "Story of a Platform Audit" the were some "compelling" reasons not to follow this advise. "His job as a contract engineer depended on performing PRA/QRA" (Bea 1996).

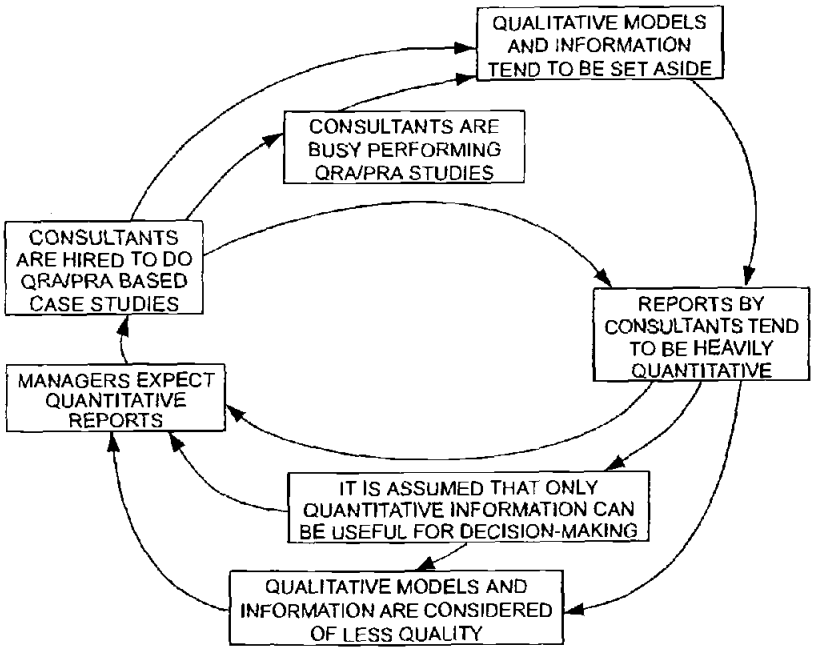


Figure 4-11
Quantitative studies distortion of information. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

Engineering professionals may get caught in behaviors that, while being reinforced by the context, are not in the best interest of the quality of their work. This is a warning, so as to realize the significance of systemic conditioning. Experienced professionals know that the quality of an engineering assessment is usually defined by the assumptions stated (or implied). In certain cases, there it is a systemic pressure to avoid questioning these assumptions and, therefore, to jeopardize the quality of the engineers work. Awareness of these systemic behavioral patterns may become of crucial importance, as it will be shown in the following chapter.

5. CASE STUDIES OF OFFSHORE ACCIDENTS

5.1 The Piper Alpha Accident

5.1.1 Introduction

The CANL approach is also applied to a post-mortem case study. The Piper Alpha accident is one of the large, recent and well-documented failures of ocean systems. However, the kind of information required for this method is not abundant, and hindsight and the allocation of blame may have altered the one available. The accident events and consequences are described based on Paté-Cornell (1995), Moore and Bea (1993b), Embrach (1992) and Visser (1992).

5.1.2 Accident Events

The offshore oil platform Piper Alpha was destroyed after a fire during the night of July 8, 1988 on the UK sector of the North Sea. A total of 167 men died, two rescue workers and 165 out of the 226 persons onboard. The platform was a total loss and the financial damage is estimated to exceed 3 billion US dollars (Paté-Cornell 1995).

The platform was under maintenance operations, while sustaining maximum production. The immediate cause of the initial fire was a leak of gas and condensate through a blind flange that was not well tightened and had replaced a safety valve. A contract crew had recently removed a backup pump for gas condensate, but the new shift on the control room was not aware of that modification, and routed gas to the missing pump when the alternate pump broke down. The leak was not detected until the escaped gas ignited and exploded. As immediate consequences of the explosion, the adjacent control room was heavily damaged, power was lost, the OIM and control room crew died, and the fire spread into adjacent rooms due to lack of fire protection. An unprotected fuel storage above the gas compressor unit (origin of the first explosion) was ignited and a thick black smoke engulfed the platform.

Automatic deluge (fire extinguisher) system did not operate because it had been set to manual operation during a recent underwater maintenance work, and there was nobody nearby to operate it manually.

There was no formal evacuation. While waiting for evacuation orders from the OIM, fresh air intake fans sucked the smoke into the quarters, which contributed to the death of several crewmembers that were waiting for instructions, according to procedures. A total of 109 persons died of smoke inhalation (Embach 1992). Emergency boats where located in only one area of the platform. An emergency support vessel, specially intended to fight fires and to assist during emergencies, stayed in passive position waiting for instructions of the OIM. When its master decided to assume an active role, the fire fighting monitors did not function properly, and the vessel pulled back from the escalating fire (Moore and Bea 1993).

Meanwhile, two other platforms kept on pumping oil and gas through pipelines immediately under Piper Alpha. Lines ruptured due to the fire in the platform. Emergency shutdown valves, that should have prevented its contents from escaping, were in the same area of the initial fire and could not be operated. A final explosion and fireball engulfed the platform approximately 20 minutes after the initial explosion (Visser 1992) causing the complete collapse. As it is apparent, several mechanical failures, human errors and organizational factors combined in an unexpected and lethal way the night of July 8, 1988.

5.1.3 Assessment of Causes

Moore and Bea (1993b) identify three states: (1) contributing and underlying, (2) initiating and direct, and (3) compounding events, decisions and actions that lead to such consequences. The main underlying event identified was the decision to conduct maintenance work simultaneously with high production levels. Initiating actions and events were: the low quality of the temporary condition of the maintenance work, the lack of information of the operating room crew and the failure of a condensate pump. Compounding events were the inoperability of safety devices, death of OIM during initial stage of emergency, expansion of fire to

adjacent areas, blockage of escape routes, and sustained input of oil and gas from other platforms, among others.

Paté-Cornell (1995) describes four main organizational factors: personnel issues, economic pressures (including questionable practices in production and safety management), flaws in design, and inspection and maintenance practices. Most of these factors are identified as "rooted in financial constraints from the corporation, with emphasis on the short term" (Paté-Cornell 1995). It is also mentioned that UK regulations were not adequate, probably because "the British government was eager to accelerate production of oil in the North Sea, and the safety operations may not have been at the forefront of their concerns" (Paté-Cornell 1995).

Tombs (1990) stresses the communication problems in the organization. Among the communication distortion cases, he mentions that "examples of warning information known but not fully appreciated, coming from a 'mistrusted source', are numerous" (Tombs 1990). The 'mistrusted sources' were trade unions and individual workers. Moreover, it is mentioned that some evidence indicates the fear of some workers to raise safety issues in the offshore industry at that moment.

Paté-Cornell (1995) highlights that the platform had significant modifications in order to increase its production levels. A combination of weak regulations and economic pressures (for reduction of design, construction and operation costs) induced conditions leading to diminished safety, especially due to increase in complexity and tight coupling, combined with a poor safety system.

The culture of the organization regarding safety, in particular the incentive system, is considered very poor by Paté-Cornell (1995):

> *There is no golden rule for managing the tradeoff between safety and productivity. What is clear is that a culture that exclusively rewards production encourages a myopic approach to safety. Managers who avoid small, visible problems that may disrupt production and who dismiss the possibility of large, rare accidents that are unlikely in anyone's watch are inviting catastrophe.*

This description matches the system dynamics described by the CANL model. Under the factors related to personnel issues, Paté-Cornell (1995) stresses the lack of experience of contractors and company personnel. The OIM during the accident was inexperienced and had recently arrived to the platform, but was placed in charge while the more experienced one was on vacation. Tombs (1990) mentions that only 37 out of the 223 crew onboard were employees of the operating company.

5.1.4 Loop Diagram

A loop diagram is constructed based on the information described (Figure 5-1). Upon a detailed observation, loops that reinforce systemic imbalances can be identified. A given condition for these patterns to sustain is the lack of major accidents. They existed until a catastrophic failure destroyed the platform.

5.1.5 Closing Remarks from a CANL perspective

The sources for the description and analysis of the Piper Alpha accident include several effects that have been identified by the CANL model. A loop diagram including CANL concepts such as distortion of information and systemic imbalance (shift of the burden of the proof and productivity vs. safety) was presented. The identification of "economic pressures" by various authors is explained by the "dominant attractor" (Figure 3-5).

The model is also able to explain the consequences of the accident. An accident of these characteristics is a major disturbance for the system at the corporate and industry level. Immediate consequences of the accident that affected the company were: platform loss, loss of production income, loss of reserves, pollution and clean up costs, impact on public opinion, and modifications in insurance conditions and government regulations.

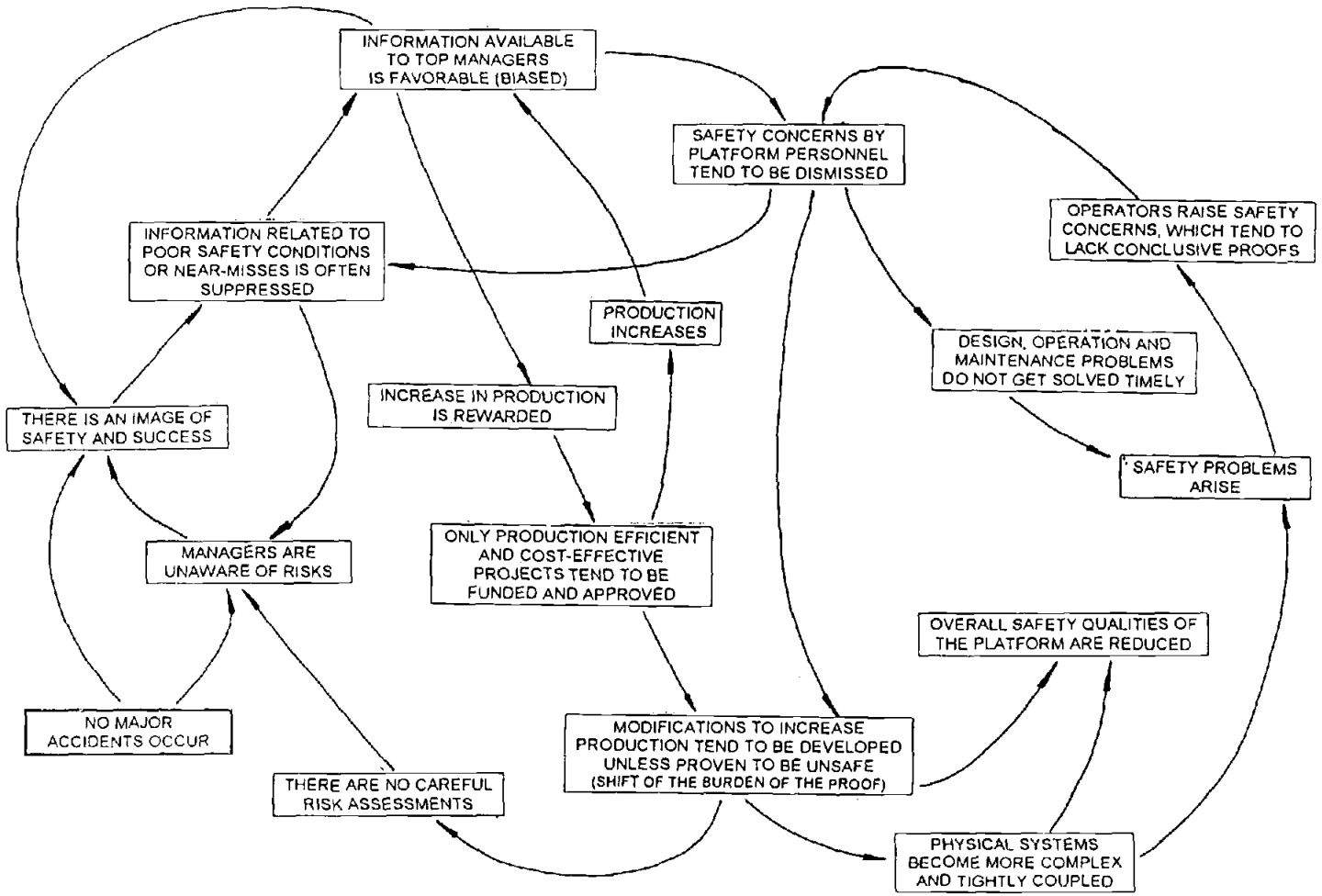


Figure 5-1

Loop Diagram for the Piper Alpha Platform. Instructions: Read a statement; read the arrow as "therefore" when moving forward or as "because" if moving backwards; read the next statement; repeating the previous steps.

A thorough study of the accident was conducted by UK government agencies. The resulting Cullen Report included many recommendations for improvements in safety regulations for the offshore oil industry in the UK North Sea sector. In particular, Visser (1992) states:

> *...these losses may far transcend the direct financial loss from the accident if it results in new, more restrictive, regulations or, worse, in precluding opportunities for further development. It is estimated, for instance, that as a result of the Cullen Report recommendations, as many as ten percent of the remaining undeveloped United Kingdom offshore fields may no longer be commercial because of increased development costs.*

After the accident, the company and the whole industry rearranged some of its behavioral patterns in order to cope with the disturbance. The challenge is to allow for the lower impact disruptions to modify the system, before one of catastrophic consequences arises. The CANL model successfully describes the organizational factors that led to the failure of the Piper Alpha platform.

5.2 Capsizing and Sinking of the Ocean Ranger

5.2.1 Introduction

The loss of the Ocean Ranger mobile drilling platform occurred on February 15, 1982 offshore Newfoundland. The 84 people onboard were killed. The estimated value of the platform was $125 million (Johnson and Cojeen 1985). The Ocean Ranger was the largest semisubmersible drilling rig in the world. The President and CEO of the company owner of the platform declared to the National Transportation and Safety Board: "... when I look this photograph and this magnificent rig... it is hard to believe something 18 inches in diameter could begin a chain of circumstances that ended in such a calamity" (NTSB 1983). The triggering event was the breaking of a porthole of the control room during a storm.

The documentation reviewed is not enough to apply the CANL model. However hypotheses are presented that could explain contributing and compounding causes of the accident identified by post-mortem studies. Initial information about the accident was reconstructed based on radio communications prior to the capsizing. A detailed diving survey on the wreck confirmed hypotheses based on other stability analyses that provide an explanation for the chain of events that lead to the catastrophic failure. Events and assessments of causes of the accident described here are based on Johnson and Cojeen (1985), NTSB (1983) and Embrach (1992).

5.2.2 Accident Events

At about 7:30 PM on February 14, 1982, the tool pusher (officer in charge of the drilling operations) informed that preparations were underway to disconnect from the well due to heavy weather. About the same time, communications overheard from other units in the area indicate that a porthole in the ballast control room was broken by a large wave—the porthole was about 10m (33 ft) above still water level. Water came into the control room causing a malfunction of the electrical controls of the ballast system. By 10:00 PM it was reported that the porthole has been secured and that all was well. At 12:52 AM, on February 15, the Ocean Ranger sent out an emergency message requiring assistance and informing of a 10 to 15 degrees list. The last known message was at 1:30 AM, reporting that crewmen were going to the lifeboat stations.

Divers on the wreck verified the overall integrity of the structure. Two portholes were broken and evidence was found that ballast valves had been operated manually.

5.2.3 Assessment of Causes

Information obtained by the diver inspection and stability studies demonstrated that when the control room personnel tried to operate the valves manually they aggravated the condition. The operating manual supplied to the crew

was incomplete and inaccurate and ballast control personnel were not familiar with the manual operation of the system.

Design deficiencies contributing to the system failure comprised the ballast operation system vulnerability, lack of provisions for effective manual operation, and the location and lack of protection for the control room (including inadequate strength of the portholes). Procedures were poorly defined and the crew was considered undertrained. Other deficiencies and violations further compromised the emergency evacuation (Johnson and Cojeen 1985, Embrach 1992). It has been noted that the crew may have not blocked the portholes, as required during storm conditions (NTSB 1983).

The triggering event was a local failure of a porthole, given the contributing factor of the severe weather, location of the control room and a possible human error (notice that none of these are sufficient, but all are necessary for the failure of the porthole). Design deficiencies contributed to an initial failure of the ballast system. Human errors, compounded by organizational factors, caused the initial failure in the ballast system to become a system failure. The accident would have not happened if all these events had not combined in this way.

5.2.4 CANL perspective

Two types of organizational factors could be identified as hypothetical contributing conditions, one during design and the other one during operation.

It is not clear with the information available which were the underlying causes for the design deficiencies. Time pressures, productivity demands and/or distortion of information could have induced the design team to overlook the potential consequences of the location of the control room. It is not clear either if the design of the automatic ballast system considered the possibility of water entering the control room. In any case, the manual valves were very difficult to operate correctly, which is a direct ergonomic problem also overlooked by designers.

Moreover, documentation for manual operation was very poor. It seems as if manual operation was not expected.

Johnson and Cojeen (1985) provide a clue for an organizational behavior leading to poor training. "The dilemma faced by the owner is that he does not want to spend money to train personnel who could leave after a short period". There were justifications for this unsafe performance and there was not enough awareness of its risks. The productivity demands and contracting conditions seem to have combined to reinforce organizational behaviors that lead to unwanted consequences. These consequences may have not become apparent if it were not for the accident.

This system failure may seem unique and bizarre. However, this is not an exception. Among other examples, one is quoted by Wu *et al* (1991) from the nuclear energy industry (the Three Mile Island accident). "Among the major causes which contributed to the accident were inappropriate operator actions which turned a minor equipment failure into a very serious event". The assessment in that case was that given the deficiencies in the control room design and the organizational factors present an accident like that "was inevitable". The same characterization of "inevitable accident" for the existing organizational conditions was given to the Chernobyl accident (Wu *et al* 1991). In other words, for the Ocean Ranger case, given the failure of a porthole during a storm, the probability of system failure was extremely high (maybe even above 10^{-1}).

5.3 Destruction of Sleipner A Platform

5.3.1 Introduction

The gravity base structure (GBS) of the Sleipner A platform sank and was completely destroyed on the Gandsfjord (near Stavanger, Norway) in the morning of August 23, 1991. The accident occurred during a controlled ballast test operation

under favorable environmental conditions. The 14 people onboard were safely evacuated.

The Sleipner A was the twelfth in a series of GBS designed by the same company, and did not deviate significant from earlier platforms. It was intended to operate in a water depth of 82.5 m (271 ft), which is relatively shallow compared to previous platforms of the series. The company's experience with this type of structures was no less than twenty years. The Norwegian sector of the North Sea contains most of the concrete offshore oil platforms existent in the world thus regulatory agencies were also experienced.

The typical design of these platforms consists of a gravity base concrete structure and a steel superstructure. The construction procedure requires the concrete structure to be submerged below the operation depth in order to place the steel superstructure on top. Norwegian fjords are ideal for this operation. Hydrostatic pressure upon the base of the structure under those circumstances is the maximum of the entire life cycle. After mating with the superstructure, the platform is towed to its final location. The following description is based on Jakobsen (1992), Offshore (1992) and Collins *et al* (1997).

5.3.2 Details of the Structure and Accident Events

The concrete base of the Sleipner A platform was 110 m (361 ft) high and consisted of a cluster of 24 cells, four of which extended to form four shafts. In plan view, the exterior walls of the cells were circular, with a radius of 12 m (39 ft), but the walls between cells were made up of straight segments. At the intersection of the cells a triangular void called "tricell" was formed. Tricells were open at the top, thus water pressure acted upon its walls.

On August 23, 1991, ballast water was being pumped into the buoyancy cells, in order to lower the structure until its base reached 104 m (341 ft) below water level. The structure was descending at a rate of 1 m (3.3 ft) every 20 minutes.

When a depth of 99 m (325 ft) was reached, a loud noise was heard from one of the two drilling shafts and water started pouring in. The location of the failure was estimated about 2 m (6.6 ft) above the surface of the ballast water. After a few minutes, the structure was sinking at a rate of 1m per minute and had to be abandoned. A few minutes after it disappeared from the surface, a series of implosions occurred. The implosions were recorded as a 3.0 magnitude earthquake on the Richter scale (Collins *et al* 1997, Offshore 1992, Jakobsen 1992).

5.3.3 Assessment of Causes

After the failure, an internal investigation committee was appointed by the construction company, which worked in parallel with investigations by the operator. Two subsea inspections were performed with Remotely Operated Vehicles, which showed that the structure was completely demolished. The investigation, therefore, focused at analyses and elaboration of hypotheses based on eyewitness observations.

The investigation detected only one area with significant weaknesses. The weak area, which corresponded to the initiating event, corresponded to the tricell walls and their supports at the cell joints. The reasons for the weaknesses and corresponding reduced load bearing capacity were recognized to be (Jakobsen, 1992):

- Unfavorable geometrical shaping of some finite elements in the global analysis. In conjunction with the subsequent post-processing in the analysis results, this lead to an underestimation of the shear forces at the wall supports by some 45%.
- Inadequate design of the haunches at the cell joints, which support the tricell walls. This lead to too short T-headed bars and absence of stirrups in the joints.

A most probable failure mode was identified that matched all eyewitness observations. Numerical computer models and physical tests performed verified this hypothesis (Jakobsen 1992, Collins *et al* 1997).

Collins *et al* (1997) highlight the extensive use of a sophisticated computer software for the design. The software was intended to identify critical locations and loadings, which engineers then could check manually. However, because the applied shear was underestimated by the global analysis, and the shear strength was overestimated by the sectional analysis, the ends of the tricell walls were not identified as critical locations by the computer model. According to analyses performed, it would have taken about an additional 70 tones (77 tons) of stirrups for the platform not to fail. "The failure of the Sleipner A base structure, which involved a total economic loss of about $700 million, was probably the most expensive shear failure ever" (Collins *et al* 1997).

5.3.4 A Personal Story

The first time I heard about the destruction of the Sleipner A platform, I had recently finished my 6-year program in Civil Engineering at the Catholic University of Argentina. One day, a former professor[1] of concrete structures gave me a copy of a paper from a German journal of structural engineering. He told me about the accident (I could have never read it form the paper in German) and he immediately showed me the figures. He draw schematically the main acting forces, pointed at the joint and said something like: "See this reinforcement? No stirrups. This T-headed bar is too short. See the location of the anchor plate? This can't take the tension far enough for the concrete to work properly (for the rebar to anchor into the concrete). How could have this happened?". It was puzzling indeed. I am sure any of his former students could have seen that there was "something suspicious" in that reinforcement detail, to say the least.

---

[1] Ing. Martín Öffele taught basic and advanced courses on reinforced and pre-stressed concrete structures to several generations of Civil Engineers at the Catholic University of Argentina (UCA). He is the Director of the Department of Structural Engineering of the College of Engineering at UCA and member of the Academic Council of that college. He participated in the 1970s in the elaboration of the Argentine national rules for the design of reinforced and pre-stressed concrete structures CIRSOC 201.

My recollection is vague. Nevertheless, the question was, and is, a striking one. How could have this happened? Why wasn't this design error detected and corrected?

5.3.5 Independent Evaluation

In order to assess the previously described personal recollection, a series of informal surveys were performed among Civil Engineering students at Oregon State University. Students were shown a detail of the reinforcement at the tricell and were asked to answer the following questions:

- *Is there anything in this design that calls your attention? Please explain*
- *Please, indicate on the figure how you would guess this element may fail, if loaded until failure. In other words, draw where you expect to see cracks when overloaded.*

The complete results of the survey are presented in Appendix I. Approximately 50 students responded after taking one week of classes of a concrete design course, which started with a conceptual and qualitative introduction to reinforcement location. Almost 25% identified something wrong with the short T-head bar, and showed cracks approximately right.

After responding to the questionnaire, students were asked:

> *Imagine now that you are working for a large company. You get this reinforcement design (which is part of a large structure) and a computer output—which implies that this is not a critical point and that the indicated reinforcement seems to be well dimensioned. After your specific work (final dimensioning, for example), this detail will go directly to the construction site. What would you do?*

Almost 90% of these students mentioned either that they would perform hand calculations to roughly verify model results, revise the design, consult with more experienced co-workers or raise their concerns to their supervisors if they had doubts. More than 40% mentioned two or more of the above. Close to 20% indicated specifically that they would not send the plans to the construction site if they had

doubts about its safety. Their good attitude seems the result from their education. According to the CANL approach it also reflects their lack of professional working experience. Their response shows no influence of organizational factors.

After responding the questionnaires, they had a presentation with the explanation of the survey, the case study, and the consequences of the failure. They were presented with the hypothesis that the raise of safety concerns within the design team could have avoided the collapse.

5.3.6 Closing Remarks from a CANL perspective

An assessment of the causes of the Sleipner A accident, based on a probabilistic analysis, is reported by Bea (1994). It concludes that the single management decision that would decrease the probability of failure the most (by 77%) was to "improve training and selection" for the designer team.

Other conceptual recommendations, after the analysis of the structural aspects of the failure (Collins *et al* 1997), state that:

> *No matter how complex the structure or how sophisticated the computer software it is always possible to obtain most of the important design parameters by relatively simple hand calculations. Such calculations should always be done, both to check the computer result and to improve the engineers' understanding of the critical design issues. In this respect, it is important to note that the design errors in Sleipner were not detected by the extensive and very formal quality assurance procedures that were employed.*

It is apparent that this design error was not due to poor technical level of the design team. The design teams were good enough to provide a good quality computer-aided design for all other aspects of the structure. Moreover, it can be argued that even inexperienced structural engineers would have been able to identify "some weakness" in the reinforcement detail, since even some students were able to do so. Something else must have happened. At this moment there is not data to prove an alternative explanation, even if the one available seems enough to discard the hypothesis of "training and selection" as a major cause. Nonetheless, a potential scenario can be described.

One of the tendencies felt by engineers that perform computer-assisted structural design is a shift of the burden of the proof. You tend to believe in the computer output. When in doubt and under pressure, "the computer seems" more reliable than your extremely simplified model and the pencil and calculator computation. This is a very broad observation of a "danger". This might have contributed to the Sleipner A destruction. Collins *et al* (1997) mention in their conclusion that a manual check may have not been done. We don't want to admit this may happen to us; we know that it should not be done and that it may have negative consequences. We are taught the right way at the University. However, special conditions of the working context may set the stage for this to happen.

What are the types of systemic imbalances that arise from the application of the CANL model to different organizations that have produced negative emergent outcomes? Distortion of information, imbalance between safety and productivity, time pressure, and shift of the burden of the proof. If the assumption that most young structural engineering should be able to "see something suspicious" in that reinforcement detail is correct, systemic imbalance must have occurred. A design assistant and a constructor might have feared criticizing the a plan of the detail of the reinforcement; a supervisor, a project manager and a constructor may have assumed a detailed calculation was done; the computer model "said that not much steel is needed there"... "Why should we place reinforcement that is not needed?" "It will look good if we reduce the cost here". "Do you want to add 80 tons of steel because of a paper and pencil sketch? Would you increase the cost because of a hunch?" "We need to move on, each day we delay construction because of our structural design, the company misses a million dollars in production". Put all these together: the computer "says" we don't need it, we are in a hurry, we can save some tons of steel, and we are doing what it is expected from us... Why should we design something that "looks" safer but you can't prove it is needed? As it turned out, a wrong answer –most probably implicit, since the question may have never been asked– was worth 700 million dollars.

This implicit response was "in context" with an unbalanced hypothetical organizational system. Maybe, informally gathered information would verify, modify or enlarge this hypothesis in the future.

5.4 CANL Model and Accident Investigations

Most accident records reviewed do not provide enough information to sketch the organizational patterns of behavior that lead (or presumably lead) to the failure. Moore and Bea (1993a), among others, also note that "the current state of written casualty reports and databases leads to the conclusion that little good information is available to study the complex interactions of human errors in operations of marine systems". This lack of information may indicate a lack of sufficient understanding, thus a deficiency in the investigations. A traditional process for improvement in engineering has been to "learn from failures". Blockley (1980), in his analysis of structural design, describes this learning process:

> *Clearly lessons have to be inductively learned from the collective experience. These experiences concern successful projects, failures and, perhaps most importantly, near misses, when disaster is averted through a realization that something is wrong.*

If, however, methodologies to investigate failures do not include the pervasive effects of organizational conditioning, this learning cannot be fully achieved. If near misses are neither recorded nor transmitted, learning is strongly limited.

Rutledge (1991), after his extensive assessment of flight safety, proposes the research of new forms of accident investigation:

> *...the current approach of explaining an accident solely through its causal mechanism could be complemented and extended beyond the ambiguous scattering of initial conditions which limit it pretty much to the operator and equipment domain. Through a better understanding of the pattern of technology, the patterned behavior of organizational complexes, and so forth, accident investigators would have a broader framework from which to pursue a more comprehensive explanation of the accident, penetrate the context of*

the accident and ferret out the "fundamental surprise" content of the accident.

The CANL methodology imposes a discipline, so that an investigation can capture a more complete picture of the behaviors leading to catastrophic failures. The application of the CANL model to accident investigations would allow for the description of behavioral patterns within organizations, which may show to be identical among different industries. That is to say, even if specific technical events will differ, the patterns of organizational behaviors may be the same ones. If this common characteristic can be shown, both reliability assessment and management in general could benefit from a much broad range of experiences.

The inclusion of the CANL approach and loop diagrams is strongly encouraged as a complement of accident investigation in all industries that can be described as composed of complex technological systems.

Moreover, the awareness of members of these complex organizations is of outstanding importance. By including the principles of the CANL model and loop diagrams of illustrative case studies within training at all levels, people should be better prepared to recognize this patterns. Of utmost importance, however, is to educate all members of these complex organizations so that they would be driven to correct negative patterns before a catastrophic failure arises. The presentation of the Sleipner A story to the concrete design students is a very simple example of what can be done.

6. QUALITATIVE METHODOLOGY FOR RELIABILITY ASSESSMENT

6.1 Introduction

The CANL model was presented in Chapter 3. The approach was applied to several case studies of offshore systems in Chapters 4 and 5. In particular, it allowed for the explanation of behaviors observed during a Safety Audit and the ones that contributed to offshore accidents. It was shown to provide a discipline for the understanding and description of a state of the organization.

This chapter provides a generic methodology for the application of the CANL model to any Safety Audit. It is proposed that this methodology can be used to assess the Reliability State of an Organization of the offshore oil industry.

6.2 Definitions

The technological system is a whole that has properties at a global level. The parts, individuals, equipment, units, components have properties and behaviors (actions, decisions, responses, performance) at a local level. System characteristics, at global level, are the emergent consequence of complex, dynamic, non-linear interactions at local level. Responses of organizations can not be explained exclusively by the intentions of their individual members.

The organizational system and the physical system could each one be referred as a "whole" for some purposes. However, it must be always acknowledged that interconnections between organizational and physical systems are very profound, so their isolation has significant limitations. The actual system is one with both human and physical components.

For a general and simplified view of organizational levels, some descriptions refer to upper level management, middle (or technical) management, and front line

operators (which includes maintenance crews and any operator "down in the organizational chart"). Individuals at all levels share many common properties, despite of this simple and broad classification.

The relationship between individuals and the technological system is bi-directional. Actions and decisions by individuals, interacting in complex ways, which tend to characterize patterns, produce emergent outcomes at the system level. Conversely, systemic emergent patterns tend to shape and condition behaviors of individuals.

Organizational factors represent malfunctions that increase the probability of human errors and local failures of physical components. Organizational factors are a set of conditions that provide context for human behaviors (decisions and actions), they emerge from the interaction of events and individual behaviors that persist within organizational systems, and they alter the probabilities of human errors. Organizational factors are emergent outcomes of system dynamics, which in turn can be understood with the CANL model. The model also indicates that systemic imbalance is in the root of all organizational factors.

Loop diagrams are a graphical representation of qualitative causal relationships within the system. These relationships are non-deterministic and dynamical. Statements of behaviors are presented in boxes and linked by arrows. Arrows are to be read "therefore" when reading forward between statements and "because" when reading backwards. In a loop diagram, "given" behaviors may be defined as ones that do not need a justification. This is a license to simplify the presentation, since they can usually be traced back to another loop. Given statements are included in a box with double lines.

The purpose of the diagram is to visualize patterns of behaviors sustained in time. According to the CANL approach, emergent patterns are closed (thus self-reinforcing) sequences of behaviors. Typical patterns observed are in the form of loops, simple or with multiple interconnections.

The theoretical background is defined by the CANL approach. The construction of the diagrams has to fulfill specific rules. However, the process of capturing the essential characteristics of the complex system can be done with human intuition and judgement, within the framework of a discipline.

The simple rules of representation and interpretation provide a valuable tool for communication among fields of specialization and practice.

6.3 Methodology for Application in a Reliability Audit

The methodology proposed for the incorporation of the CANL approach into a reliability audit is based on four steps:

1. Elicitation: Information is gathered through interviews with members of all levels of the organization.
2. Loop diagrams: diagrams are performed to understand internal processes and emergent behaviors of the system.
3. Review: preliminary findings are presented to members of all levels of the organization for comments.
4. Diagnosis and Recommendations: final diagrams are prepared and the final recommendations are presented openly within the organization.

6.3.1 Elicitation

The elicitation process is a complement of a regular safety audit, for example, the one described in the "Story of a Platform Audit" (Bea 1996). It can be considered a common practice, but specific characteristics that are necessary for the implementation of the CANL approach are highlighted.

Every technical, business or informal meeting with members of the organization is a valuable source of information. In fact, the more informal the environment, the more valuable the information might be. It should be noted clearly

that all the information provided is confidential. The purpose of the study, and the permanent aim of the auditor is to understand the behaviors within the organization and not to blame any particular individual, operator, manager, area, section, team or professional group. The auditor needs to get involved –as opposed to "detached"– in order to understand. Bea (1996) transmits this attitude in his description of the "Story of a Platform Audit".

It would be natural that the initial meetings are done at the higher levels of management, and proceed "down the organizational chart". The main topic of the meetings may be the formal safety or production procedures, but in many cases the context, stories and side comments will provide utmost valuable information for this method. Top level managers should be warned that they would be revisited in the future with further inquiries. That will be the case especially if distortion of information is identified.

The auditor should be very alert to identify apparent inconsistencies between safety goals and actual behaviors. It should be very clear to the auditor that "every behavior has a justification in order to persist", and such justifications should be identified. Another significant inconsistency to identify is between formal procedures and actual practice. This conflict (which usually indicates an evolution or degradation) may help identify the organizational context and systemic reinforcement of behaviors of individuals. The auditor should understand and show understanding for the context of the individuals, even if he would not justify their actions or decisions. The loops presented in the case study could provide a guideline for the identification of some behaviors and justifications.

When recording statements, personal and group opinions and feelings should be clearly identified as such. Most probably, some of them will be stated as facts, but they may not be.

Significant sources of information are the "frustrations of concerned individuals". These members of the organization are already aware of problems and systemic pressures within the organization. Frustration can result from the inability

to modify the systemic patterns of behaviors that produce negative outcomes. This study allows for a positive use of this personal circumstance.

It is very important for the auditor to identify any possible informal network of information or work practices. These are organic responses within the system, which are usually hidden from upper levels of management and may reinforce the distortion of information.

This first step is not completed until integrated with the second one.

6.3.2 Loop Diagrams

Loop diagrams and the CANL model, are the key elements of the proposed methodology. Loop diagrams should be sketched and recorded since the initial interviews. In most cases, initial diagrams may not show loops, but open chains or branches. Initial impressions may change significantly after interviews at different levels of the organization. In any case, the loops are the language of the methodology, and should be exercised. They have rules that need to be followed. The use of these rules in order to obtain an understanding of the organizational system constitutes a discipline. Numerous revisions may be required to construct the diagram that best describes the condition observed. This exercise improves understanding. The discipline allows for a formal incorporation of experience in an interdisciplinary framework.

Loop diagrams also indicate what information may be still missing after several interviews, as shown in the case study. In order to provide an explanation of the systemic behaviors "everything should fit". The elicitation step, for information gathering, cannot be ended until complete and consistent loop diagrams can be performed.

Loop diagrams could be drawn both for specific (local) circumstances and for generic behaviors within the organizational system. The local diagrams (even if not closed loops) should identify clearly the implications on safety of behaviors, if any. As the audit proceeds, more general statements would be identified in order to "show

the big picture". For this purpose, several statements may be condensed in a simplified one, as shown in the "Story of a Platform Audit" case study.

The generic loop diagrams presented in the case study can be used as a guideline for the identification of behavioral loops within the organization. More general templates, as the distortion of information loop, could be developed in the future to assist this task, even in other industries. However, the auditor must always be ready to modify the diagrams and change his/her assumptions when faced to new evidence. The diagrams should represent the system under study, not repeat a preexistent cliché.

After the integration and completion of the two initial steps, the general findings of the auditor should be presented to members of the organization from all levels.

6.3.3 Review Process

The review process constitutes a partial validation for the evaluation. The validation is partial, since some members –strongly identified with the existing systemic reinforcement of behaviors– will not be ready to acknowledge the implications of the description of the system. Individuals should help to verify that the justifications for their behaviors are accurately described.

The main goal of this step is to modify the loop diagrams as necessary and double check justifications and simplifications performed. The goal is not to obtain unanimous acceptance. It is expected that some members of the organization may tend to reject or deny some of the apparent conclusions of the description. That could constitute one of the systemic outcomes described.

For the review process, meetings and interviews can be held "up the organizational chart", starting by maintenance and front line operators. Whenever possible, informal and personal dialogues should be attempted. All members despite of their background can understand loop diagrams. The informal networks of information –if identified– should be actively used to review the loop diagrams.

It is also important to expand the concept of "credible disorders". Each member of the organization should be aware that his/her participation and "speak up" is crucial for the safe and healthy operation of the system. The diagrams may show "why they couldn't speak up" in the past. However, members from all levels of the organization should realize that multiple effective channels for clear communication of safety concerns should always be maintained active. The negative outcomes of not doing so should become apparent. Education based on the application of the CANL model to case studies is another way to achieve this understanding.

The review process can be a difficult step, especially when significant problems have been observed. Experience indicates (Bella 1998c) that, in a presentation to a group, it is usually convenient to describe first a very similar loop diagram that corresponds to a different organization. In that way, personal identification with the description may be observed, without individuals fearing to be pointed at as "the one to be blamed". Similar observations were found elsewhere (e.g. Whalley and Lihou 1988). The goal of the auditor should be to understand the system, but he/she also needs to show convincingly to every individual that blaming will not be an outcome of the process. The final aim is to improve safety.

6.3.4 Diagnosis and Recommendations

The final diagnosis is the description of the corrected loop diagram. It is an instantaneous picture of the evolving system at the moment of the audit. It incorporates its history and context; it shows tendencies but cannot predict the future in a deterministic or quantitative way. A set of recommendations could be elaborated based on the patterns of behaviors identified. It should be noted that the organic response of the system to them can not be predicted. The effectiveness of the recommendations is uncertain, while the diagnosis may be accurate.

The conclusions and recommendations should be presented openly within the organization, and still be open for further comments. A short report should be easily available to any member.

Ideally, follow up audits should be implemented in order to assess the evolution of the organizational behaviors.

6.4 Characteristics as a Management Tool

The described methodology provides information on the organizational behaviors that affect safety. Since organizational factors affect the probabilities of human errors and the existence of common-cause type failures, they are key indicators in the assessment of the reliability of a technological system. They have been shown to represent a significant portion of actual failures (e.g. Bea 1996, Hollnagel 1993).

Most quantitative reliability analysis methodologies are unable to effectively incorporate the organizational factors in their procedures. In those cases, the final result (a number) is unable to accurately show the variations of probabilities of failure due to systemic behaviors. The result would be the same (or very similar) if the organization were like the one at the Millstone Nuclear Power Plant on 1996 (when it was fined for its unsafe organizational culture) than if the organization behaved like the one at a US Navy Aircraft Carrier–identified as a High Reliability Organization (see Chapter 2).

The methodology, however, is not intended to replace any present decision-making tool, but to complement them. It aims at capturing in a structured but simple way the complex organic behavior of the large organization, thus filling a gap in the type of information now available for decision-making.

It allows for participation of all members of the organization, both in the elaboration of the diagnosis and its review and in the final comments. Moreover, it provides a tool for simple transfer of information across cultural, technical and hierarchical barriers.

It is a snap shot, and a series of analysis along a period will show the evolution of the system or the adaptive response of the system to policies implemented.

It is proposed to provide an effective description of the organization with respect to the reliability of the technological system, by focusing on the organizational factors. It can indicate how close an organization may be to a HRO or to the one of the Millstone NPP, through a determination of existence of systemic imbalance. It is a tool for the direct evaluation of organizational factors, such as distortion of information, shift of the burden of the proof, productivity vs. safety imbalance, and time pressures. A structured quantification of systemic imbalance is proposed in Chapter 10.

6.5 Incorporation into Existent Reliability Assessment Methods

The CANL methodology described can be incorporated into existent programs for reliability assessments with qualitative components. One of such programs is the Safety Management Assessment System (SAMS) proposed by Bea (1998b).

SMAS comprises 5 major steps:

1. Select the system for assessment
2. Identify assessment team
3. Coarse qualitative assessment
4. Development of scenarios
5. Mitigation measures suggested

According to Bea (1998b), the third step consists of a coarse qualitative assessment of seven categories of elements that comprise the system: operating personnel, organizations, hardware (equipment and structure), procedures (normal and emergency), environments and interfaces. The product of this step is the identification of factors of concern. The CANL methodology proposed here can be

used to assess the organizational influence on reliability, as part of the evaluation process. The stages proposed for the evaluation process (background information onshore, visiting facility offshore, final evaluation onshore) are compatible with the methodology described here. The elements of the system defined by Bea do not match the ones defined for this approach, but the understanding obtained through the application of the CANL model could provide information for the determination of SMAS factors and attributes related or affected by organizational patterns. Loop diagrams could be included as part of the output report generated by the process.

7. CONCLUDING REMARKS – PART I

The CANL approach has been applied in the past to understand several different organizational and technological systems. The CANL model allows for the understanding of organizations and their emergent outcomes. The discipline involved in the application of the model facilitates the formalization of an assessment procedure. The output documentation, the loop diagrams, is well suited for interdisciplinary and inter-hierarchical communication.

This approach to organizations is useful for the assessment of organizational factors. Systemic imbalance was found at the root of all organizational factors that lead to a reduction in reliability. The most general organizational factors identified correspond to the following emergent behaviors: distortion of information, profit vs. safety imbalance, shift of the burden of the proof, and time pressures (work overload).

A proposed methodology for safety audits, based on the CANL approach, can give information for the determination of the existence and degree of systemic imbalance and for the evaluation of generic organizational factors. The product of this assessment could be used to evaluate the Reliability State of an Organization.

The application of the CANL model may improve accident investigations by providing a new disciplined approach to the collection of data. It is expected that significant information now largely missing from accident databases could be identified and recorded. Moreover, generic patterns could be developed in order to identify loops that may be common across different industries. This could satisfy the need to learn from a broader set of experiences.

Further theoretical research could be undertaken to unveil a more complete link to existent classifications of organizational factors. They are many (one for each research group) and based on data analysis or other empirical source. The CANL model can provide a unifying theoretical framework, as it explains with few concepts most (if not all) of the specific organizational factors mentioned in the literature.

The methodology proposed for the implementation of the CANL model to safety audits has to be tested. Applications performed for this work were only based on written references. The method should be implemented in actual field studies.

The CANL model is used as a background to the evaluation of quantitative probabilistic formulations and to assess a Reliability State of an Organization is developed in Part II of this work.

PART II

8. BRIEF BACKGROUND TO QUANTITATIVE ANALYSES

8.1 Introduction

The bases of quantitative reliability (or risk) assessment have been a set of analytical tools usually called Probabilistic Safety Assessment (PSA), Probabilistic Risk Analysis (PRA), and/or Quantified Risk Analysis (QRA). These tools include Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and lately Influence Diagram Analysis (IDA), which are used as part of the analytical process. Usually these different names are applied to the same procedures and "Analysis" and "Assessment" are interchanged by different authors. Risk, as used in these titles, is usually defined (and calculated) as the probability of a given failure multiplied times a quantification of its consequences. When "R" stands for reliability, only the probability of failure is evaluated. In any case, the evaluation of the probability of system failure is a significant aspect of PSA, PRA or QRA.

When the probabilities of human errors need to be introduced into these evaluations, a similar structure is applied. Human Reliability Assessment (HRA) is intended to provide the probabilistic information regarding human errors in the format expected by the QRA tools.

8.2 Quantified Risk Analyses

The main aims of QRA are to identify potential areas of significant risk for improvement strategies and to quantify the overall risk of a particular system. The core of traditional QRA is based on the construction of logical tree models. Fault tree analysis and event tree analysis allow for the understanding of fundamental causal relationships and for the calculations of a probability of failure of the system under study.

The general structure of a QRA, as originally described in 1975, involves the following steps (Reason 1990a):

1. Identification of sources of potential hazard
2. Identification of initiating events that could lead to this hazard
3. Establishment of sequences of basic events that could follow from various initiating events
4. Quantification of each sequence that may lead to system failure
5. Determination of the overall plant risk as a function of probability of possible accident sequences and their consequences

After the initial use of this methodology (when all basic events were assumed statistically independent), it was improved in several ways, including the consideration for human errors and common cause hardware failure. The Three Mile Island Power Plant accident in 1979 constituted a major impulse for the inclusion of human errors in accident risk assessment. This method, despite of its improvements, is still considered by some as a reductionist approach that is insufficient for the accurate quantification of risk in complex and hazardous technological systems (e.g. Perrow 1984). Some of its limitations are pointed out in this work.

Fault tree analysis (FTA) is a systematic method for the identification of potential failure modes in large systems. For its use in QRA, it includes a quantitative evaluation of the probabilities of local failures that may lead to a main failure event, also called top event (in particular, a system failure). In many cases, FTA may identify a failure path that is most significant in terms of probability of occurrence. This analysis may be performed even if the top event is not a major failure. A fault tree is a graphical decomposition of a top event into the union and intersection of subevents (usually local failures), which are analyzed until "basic events" can be identified (Ang and Tang 1984, Bea 1994). The basic events are the basic causes considered of interest, and for which probabilities of occurrence can be assessed.

A fault tree can be formulated as a network so that Minimal Cut Sets can be identified. Each Minimal Cut Set (MCS) represents an irreducible set of basic events

that may lead to a top event. In other words, it is one of the potential chains of events that may lead to a system failure according to the FTA. A large fault tree may be simplified by analyzing the MCSs with significant probabilities of occurrence (Ang and Tang 1984). When all potential failure paths are assessed for every failure mode, a probability of system failure can be calculated.

Event tree analyzes the consequences of a particular initiating event. The diagram is constructed after the identification of mutually exclusive sets of subsequent events, until the consequences of significance for the analysis are established. The probability of each consequence can be calculated as the product of the conditional probabilities of all events of each path (Ang and Tang 1984, Bea 1994). The concept that triggering events may take unpredictable forms (tokens) to produce system failures (Reason 1990a, 1990b) brings at least a shade of doubt to this approach when applied to complex systems.

Influence diagram analysis (IDA), (Oliver and Smith 1990) has been also proposed as a useful tool for representation of relationships among components in systems (Bea 1994, Paté-Cornell 1996, Mosleh *et al* 1997). In some of these cases, the method was used to model the organization rather than the whole system. This method improves the representation of common-cause-type dependencies, which may become obscure and difficult to reflect in fault tree and event tree diagrams. Moreover, it is not necessary that events be ordered. It is proposed that these three analytical methods can be used to complement each other (Bea 1994).

These methods force the analysts to try to understand the system. "Development of fault trees requires considerable thought and investigation to ensure that all possible sources of risk are accounted for" (Peet and Ryan 1998). Moreover, the data needed for these analyses requires considerable research. In any case, "overall risk levels derived from quantified risk assessments are more valuable when the purpose is to compare the change in risk level when introducing a new regime... Risk levels tend to be of lesser value when comparing dissimilar situations" (Peet and Ryan 1998).

These methods have certain limitations in complex technological systems. In general, these methods tend to be focused on physical malfunctions. Non-operational human errors and organizational states that increase the probability of local failures tend to be disregarded.

All quantified probabilistic analytical methods are based on the identification of events that may have the form of "tokens". They are based on the assumption that all significant MCSs can be identified. Furthermore, it is implied that the MCSs that determine the actual probability of failure of the system can be selected among them. The conditions required for these assumptions to hold include –among others– that the character of the minimal cut sets is not time dependent, and that the significant initiating events can be accurately and comprehensively identified. Complex technological systems are dynamic by nature, and several post-mortem investigations have shown initiating events that were not –and might have never "reasonably" been– included in reliability analyses.

8.3 Multiple Related Failures

Multiple Related Failures is the label adopted for multiple failures provoked by existing dependency structures or components interconnections. It has been identified in several major accidents that correlations or dependencies among local failures destroy the assumption of independence (Amendola 1989a):

> *In reality, major accident occurrences ... have shown that the multiple defenses built-in to protect a NPP from meltdown events [system failure] can be lost as a result of very complex dependency structures involving combination of causative factors related to design, procedural, operational and management aspects as well as to hardware failures. Consequently, the final undesired event may be provoked by a sequence of related events (affected by either physical dependencies or by stochastic ones), among which it is difficult to find a single underlying effect.*

Definitions proposed for these type of failures (Amendola 1989b) include:

- Dependent Failure: The failure of a set of events, the probability of which cannot be expressed as a simple product of the unconditional failure probabilities of the individual events
- Common Cause Failure: This is a specific type of dependent failure where simultaneous (or near simultaneous) multiple failures result from a single shared cause
- Common Mode Failures: This is a term reserved for common cause failures in which multiple equipment items fail in the same mode

Davoudian *et al* (1994b), among others, highlight the significance of organizational factors as a source of multiple related failures in complex technological systems (also called "common-cause effect" of organizational factors). In particular, Goldfeiz and Mosleh (1995, 1996) describe organizational factors as a common cause of a class "where a single underlying cause increases the failure rate of multiple components", rather than one that produces near simultaneous multiple failures. Therefore, organizational factors would not usually produce a common cause failure, according to the previous definitions, but a dependent failure one.

For the analysis of common cause failures, Contini (1989) identifies critical common cause failures as the ones where common attributes are present in all elements of a MCS. Relevant common cause failures of order $w=k-j$ are those where j out of k basic elements of the MCS have the same dependence. Organizational factors can be characterized, by analogy, as factors that usually induce relevant dependent failures and even might induce critical dependent failures. The dependency can usually be assumed high since many basic events j can be related to organizational factors (all human errors and some physical component failures). The relevant dependent failure would then be of low order ($w=k-j$). The number of dependent events (j) is positively correlated to the orders of magnitude of increase in the probability of failure of a system compared to the assessment without considering dependency on organizational factors. Conversely, the order of the relevant dependent failure (w) is negatively correlated to the order of magnitude of

the correction to account for organizational factors. An estimation of this correlation can indicate a rough correction for a value of probability of failure.

8.4 Human Reliability Analysis (HRA)

The primary goals of HRA are achieved by its three principal functions: human error identification, human error quantification, and human error reduction (Kirwan 1994). The human error quantification is required as input for QRA. Specific HRA techniques are reviewed by Reason (1990a) and Hollnagel (1998).

Human Reliability Assessment is acknowledged as a difficult task (Kirwan 1994):

> *...Human behaviour is intrinsically complicated and difficult to predict accurately. HRA is therefore conceptually a rather ambitious approach, particularly since it deals with the already-complex subject of human error in the additionally complex setting of large-scale systems. HRA must therefore not be used complacently, and cannot afford to be shallow in its approach to assessment. Complex systems often require correspondingly complex assessment procedures.*

The original focus of HRA was purely on quantification of human error probabilities (HEP). These probabilities were defined as number of errors occurred over number of opportunities for errors, and original effort was focused on collection of data to determine these values. Once basic probabilities of error were obtained, FTA and ETA were used to calculate a probability of a specific failure caused by human error.

The original method to introduce some context-related factors (environmental conditions, working conditions, stress, etc.) was through performance shaping factors (PSF). PSF are used as coefficients that multiply HEP in order to account for these effects.

After this initial approach to HRA, the emphasis shifted to the understanding of the causes of errors. The identification of potential system failure modes,

originally assumed a trivial task, also became a major focus of efforts (especially after large-consequence unexpected accidents occurred). Hollnagel (1998) proposes a "second generation" HRA methodology following this tendency.

8.5 Quantitative Approaches for Incorporation of Organizational Factors

Kirwan (1994) proposes three ways for dealing with organizational factors, in relation to their influence on the reliability of complex systems.

1. Developing inherently safe industrial cultures
2. Assessing organizational effects in the risk levels and altering PSA predictions accordingly
3. Setting definite organizational boundaries for risk assessment so that the deterioration of safety culture will be signaled by the PSA rather than assessed directly

All these strategies are good at first sight, and could be pursued more or less simultaneously. However, the scope and consequences of each one should be carefully reviewed.

Strategy (2) is still an active field of research. Part II of this work deals with this approach. Strategies (1) and (3) are fundamental while this research is in progress. Safety culture of organizations should be improved and maintained as good as possible, and the limitations of QRA should be acknowledged. The CANL model, as used in Part I, can qualitatively assess the characteristics of the organization with regards to safety, as part of these strategies.

A variation of strategy (1), that is "enforcing safety culture" is described for the nuclear energy industry in section 2.6.1, as applied by the U.S. Nuclear Regulatory Commission.

Strategy (3) basically means that limits of the validity of QRA results should be carefully considered. A difference in three orders of magnitude in terms of

accident frequency has been reported between physically similar industrial plants where the only difference was the organizational culture (Kirwan 1994). The numbers resulting from QRA, then, may not reflect accurately what it might be expected to if they cannot incorporate sensitivity to organizational factors.

A criterion to assess the validity of QRA results could be based on evaluations of the organization with the CANL model. If there were grounds to suspect that a platform or plant may have any organizational influence that alter the assumptions of the QRA/HRA methodology used, the results should not be considered as an absolute or accurate measure of the probability of system failure.

Strategy (3) also implies that ALARP principle (probability of failure is as low as reasonably practicable and further improvement is not cost-effective for a given risk reduction) and risk evaluations can not be calculated when organizational factors may become significant.

Both calculations require accurate absolute values of probability of failure. The use of such tools for decision making can be only justified in this case when a methodology based on approach (2) is developed and proven. In any case, QRA would still be very useful to identify physical system modifications to improve overall reliability, using its results as relative rather than absolute values.

Chapter 9 reviews four probabilistic formulations that were developed as an attempt to include organizational effects in quantitative results.

9. ORGANIZATIONAL FACTORS IN EXISTING FORMULATIONS

9.1 Introduction

The following sections include the review of four of the formulations proposed for the introduction of organizational factors into quantitative probabilistic assessments (QRA, PSA or PRA). A generic formulation based on a set of mutually exclusive organizational factors proposed by Bea (1994, 1995b, 1997) is discussed. The approach based on the "omega factor" (Goldfeiz and Mosleh 1995, 1996, Mosleh *et al* 1997) is commented. The Work Process Analysis Model (WPAM) (Davoudian *et al* 1994a, 1994b) is reviewed and its probabilistic formulation assessed. The "simple set of equations" proposed in the SAM approach (Paté-Cornell and Murphy 1996) and a similar one by Moore and Bea (1993a, 1993b) are reviewed. Finally, proposed models for the influence of management on human actions (Murphy and Paté-Cornell 1996) are reviewed.

9.2 Probabilistic Formulation – Mutually Exclusive Assumptions

9.2.1 Probabilistic Formulation

Bea (1994, 1995b, 1997) proposes a probabilistic formulation conditional on mutually exclusive human and organizational errors. Four structure quality attributes are defined as serviceability, safety, durability and compatibility (Bea 1994). The event of system failure is then the union of each set representing the event of insufficient quality of each attribute fi:

$$f = \cup fi \tag{9-1}$$

The two main category factors identified are Environments (E) and Human Errors (O), the former due to "inherent" randomness and the later influenced by

human errors. The probability of failure of anyone of the quality attributes is defined by Bea (1994) as:

$$Pfi = Pfi_E / O \cdot P[O] + Pfi_E / \overline{O} \cdot P[\overline{O}] + Pfi_O \cdot P[O] \qquad (9\text{-}2)$$

where

$P[\overline{O}]$ = probability of no human error $1 - P[O]$

Pfi_E / O = probability of failure of attribute i due to inherent randomness, conditional on the occurrence of human error

Pfi_O = probability of failure of attribute i due to human error

The failure is further classified according to life cycle phases and specific steps are defined within each phase. Human errors are classified in eight types (communications, slips, violations, ignorance, planning & preparation, selection & training, limitations & impairment, and mistakes). These are assumed as mutually exclusive and collectively exhaustive categories. The probability of failure of any attribute due to human error (the human error and one phase and step within that phase are implied to simplify the notation) is then proposed as (Bea 1994):

$$Pfi = \sum_j \{(Pfi / O_j) \cdot P[O_j]\} \qquad (9\text{-}3)$$

The categories of human errors are influenced by four types of contributing influences or error producing factors (Bea 1994): organizations (Oe), hardware (He), procedures (Pe) and environment (Ee). The probability of one type of human error is then proposed as:

$$P[O_j] = P[O_j / Oe_j]P[Oe_j] + P[O_j / He_j]P[He_j] + \\ + P[O_j / Pe_j]P[Pe_j] + P[O_j / Ee_j]P[Ee_j] \qquad (9\text{-}4)$$

Organizational errors are classified in eight types (communications, planning and preparations, culture, organization, violations, monitoring, ignorance, and mistakes).

These are also considered mutually exclusive and collectively exhaustive categories. The probability of organizational errors is then assumed as (Bea 1994):

$$P[Oe_j] = \sum_n P[Oe_{j,n}] \tag{9-5}$$

where $P[Oe_{j,n}]$ is the probability of a category j human error due to each category of organizational error n.

9.2.2 Discussion

This probabilistic formulation is based on very detailed and structured classifications. However, it implies several simplifications, in particular, the assumption that the categories within these classifications are mutually exclusive.

When the rare event approximation is applied to the union of dependent events that are not mutually exclusive, the probability could be overestimated. However, it should be recognized that failures cannot usually be attributed to only one cause. Therefore, multiple causality should be incorporated into the expressions. For example, equation (9-2) would underestimate the probability of failure if it does not consider the probability of a failure due to both human and inherent causes acting simultaneously. That is, it is not only possible that human errors increase the probability of otherwise "inherent" failure rates (like in the proposed term Pfi_E/O), but also system failures can be caused by human errors and physical component failures acting simultaneously. Equation 11-1 proposes an alternative formulation.

The widespread assumption of mutually exclusive categories has an impact on the result of calculations when the theorem of total probability is applied (equations 9-3 and 9-4). It can be argued that they are collectively exhaustive, but its categories are not mutually exclusive, as assumed. In particular, the probability of simultaneous realizations of several categories of a classification (e.g. human errors O_j) may be very small. However, the probability of failure due to them acting simultaneously may be orders of magnitude higher than the one due to one single category. This observation applies to equations (9-3) to (9-5).

9.3 Probabilistic Formulation - Omega Factor

9.3.1 Probabilistic Formulation of the Omega Factor

A model for assessing the influence of organizational factors on reliability is proposed for the explicit inclusion of organizational factors in PSA of nuclear power plants (Goldfeiz and Mosleh 1995, 1996, Mosleh *et al* 1997). A simple model for the representation of the structural and behavioral aspects of organization was developed. Factors directly influencing the quality of plant personnel in their interaction with hardware are identified, while their relationships with the elements of the organization model are considered. Influence diagrams are used to quantify the measures of influence of organizational factors.

The model proposed by these authors relates management and organizational factors to equipment unavailability and operator error probability, in order to assess an overall risk measure. The example given (Goldfeiz and Mosleh 1995) assumes that, following an initiating event, two subsystems A and B are needed to be activated successfully in order to avoid the system failure. Then,

$$\Phi_S = \Phi(I) \cdot P(\overline{A}) \cdot P(\overline{B} / \overline{A}) \tag{9-6}$$

where $\Phi(I)$ is the frequency of the occurrence of the initiating event I, $P(\overline{A})$ is the probability of failure of A, and $P(\overline{B} / \overline{A})$ is the probability of failure of B given the failure of A. The probability of failure of component A is proposed as:

$$P(\overline{A}) = Q_A = f_A \cdot \tau_A + q_A + \lambda_A \cdot t_A \tag{9-7}$$

where λ_A is the failure rate during operation and t_A is the component mission time, q_A is the probability that the component cannot be started upon demand, and f_A is the frequency of maintenance and τ_A the duration of maintenance or time to restore. The example follows assuming

$$Q_A = \lambda_A \cdot t_A \tag{9-8}$$

for simplicity of presentation of main concepts. Therefore, under the assumption that both failures are independent,

$$Q^{(I)} = Q_A \cdot Q_B = (\lambda_A \cdot t_A) \cdot (\lambda_B \cdot t_B) \tag{9-9}$$

However, if they are dependent, the probability of failure is typically greater:

$$Q^{(D)} = Q_A \cdot Q_{B/A} > Q^{(I)} \tag{9-10}$$

The difference with traditional common cause failure is pointed out; the dependence does not cause different components to fail simultaneously, but to have a different probability of failure. That is to say "components fail (conditionally) independently but at a higher rate compared with the case of a 'good' organization" (Amendola 1989b, Goldfeiz and Mosleh 1995, Mosleh *et al* 1997).

Causes that synchronize failures of multiple components so that failures occur simultaneously or within a short period are defined as common cause failure (Goldfeiz and Mosleh 1995). In this case, the failure of a second component given the failure of the first one is certain, so that the probability of failure is represented by:

$$Q^{(D)} = Q_A \cdot Q_B + Q_{AB} \tag{9-11}$$

where Q_A and Q_B are the independent probability of failure, and Q_{AB} is the probability of (simultaneous) failure of A and B due to a common cause.

When a single underlying cause increases the probability of failure of several components, but components still fail at randomly distributed times, the following expression is proposed (Goldfeiz and Mosleh 1995):

$$Q^{*} = Q^{*}_{A} \cdot Q^{*}_{B} > Q^{(I)} \tag{9-12}$$

It is proposed that organizational factors are influences common to all components and human actions modeled in a PSA (Goldfeiz and Mosleh 1995, 1996, Mosleh *et al* 1997). As such, they have a common-cause type effect, and function as a source of dependence relating different component failures and human errors. It is

proposed that the most likely form of dependence is through increase or decrease of failure probabilities of different components. Thus, the second model, represented by equation (9-12), is applied (Goldfeiz and Mosleh 1995).

The parametric model for incorporating the influence of organizational factors is based on a definition of failure rates that includes the increased probability of failure of a component described above:

$$\lambda_{Total} = \lambda_I + \lambda_O \tag{9-13}$$

where λ_I is the inherent failure rate and λ_O is the rate of failure due to organizational factors. A parameter ω is defined as follows:

$$\omega = \frac{\lambda_O}{\lambda_I} \tag{9-14}$$

so that

$$\lambda_{Total} = \lambda_I + \omega \cdot \lambda_I = \lambda_I \cdot (1 + \omega) \tag{9-15}$$

The inherent portion (λ_I) represent the rate related to the failure mechanisms that are beyond the control or influence of the organization. The added parameter λ_O represents the increase of the failure rate above that "expected" value. This assumes that for a perfect organization $\lambda_O = 0$ and $\omega = 0$. The model further assumes that "different components typically have different failure rates but they may share the same organizational factor ω " (Goldfeiz and Mosleh 1995, 1996, Mosleh *et al* 1997).

9.3.2 Determination of Organizational Influence

The method is based in a modelization of organizational influences through a hierarchical network in the form of an influence diagram. The model is proposed to include both structural (positions, etc.) and behavioral (responsibilities, etc.) aspects of the organization. It is required to include implicit and explicit relationships among elements within sub-organizations and across them. A schematic representation

proposed for an organization includes: factors that affect management behavior, managers, supervisors, personnel, teams/ programs/ processes, characteristics/ attributes, and product/ function/ objective. Each element of the model is assigned a set of possible states of values. "At the end of the quantification process we obtain a parameter P which is the degree (or probability) that the worker's performance is adversely affected by the organizational factors" (Goldfeiz and Mosleh 1995). A simple equation is proposed to relate this generic parameter of the organization P (now interpreted as a probability of failure) to the organizational factor ω for routine maintenance activities.

It is acknowledged by the authors that "several aspects of the representation and quantification of influence diagrams in this particular application involve significant subjectivity and ambiguity". Moreover, "the model of a big organization can be a quite complex network of nodes and links" (Goldfeiz and Mosleh 1995).

9.3.3 Discussion

The basic formulation of the omega factor is not thoroughly justified. There are no apparent grounds to assume that different components, with different "inherent" failure rates, should have the same organizational factor ω as derived here. An increase is expected, but a generic unbounded factor for a whole organization –as the one derived here– has yet to be proven realistic.

However, the weakest aspect of this formulation relies in the determination of the omega factor through a generic influence diagram intended to represent the organization. The approach is recognized by the authors to have drawbacks. While the proposed network can become very complex, actual relationships among elements seem hard to be identified with the precision required. It is also mentioned that "it may only be necessary to model a few significant influences" (Goldfeiz and Mosleh 1995), thus eliminating *a priori* some influences. Moreover, the approach for the construction of the network seems heavily focused on formal relationships, disregarding the very important informal networks. The underlying rational actor model assumes that the influence is mainly from "top" (managers) to "bottom"

(operators). Thus, the model as presented does not account for feedback from the operators or frontline managers to decision-makers (which are a key to understand the distortion of information loop).

Finally, the proposed implementation of the influence diagram to represent the organization does not provide a procedure to develop an overall check of its results. Deficiencies in the modelization may not be recognized after the IDA. It seems that an extensive analytical procedure with elements of high uncertainty may create the illusion of an objective assessment.

9.4 Probabilistic Formulation - Work Process Analysis Model (WPAM)

9.4.1 Introduction

The Work Process Analysis Model (WPAM) is a complete approach for the incorporation of organizational factors into the Probabilistic Safety Assessment (PSA) of nuclear power plants (NPP). The implementation requires two broad stages, a qualitative analysis (WPAM-I) and its posterior quantification (WPAM-II). It is declared to be aimed at "capturing the common-cause effect of organizational factors on NPP safety" (Davoudian *et al* 1994a) and it is constructed upon the NPP work processes.

9.4.2 WPAM Probabilistic Formulation

The probabilistic formulation of WPAM-II is based on the following equation:

$$f_{MCS} = f_{IE} \cdot \prod_{i=1}^{n} p_i \qquad (9\text{-}16)$$

where

f_{MCS} = the core damage frequency contributed by a minimal cut set (MCS),

f_{IE} = the initiating event frequency,

p_i = the probabilities of basic events, allowing for the influence of organizational factors,

n = the number of basic events in a minimal cut set.

The influence of organizational factors is included in p_i by considering the organizational factors that affect the previous events in a recalculation of the probability of each basic event.

In order to perform the analysis a limited number of MCSs is selected by a screening method described by Davoudian *et al* (1994b). The screening method is based on the calculation of a compound rating coefficient between pairs of events in the MCS. The rating coefficient between two events (R_{ab}) result from the multiplication of four partial coefficients determined by the evaluator (with values between 0.0 and 1.0), which take into account the work process, candidate parameter group, working unit, and component type and failure mode ($R_{WP,ab}$, $R_{CPG,ab}$, $R_{WU,ab}$, $R_{ID,ab}$, respectively). This procedure determines that events characterized by two different work processes are considered as independent. Candidate Parameter Group (CPG) is defined by Davoudian *et al* (1994a) as a group of parameters whose numerical values might change due to organizational factors.

The example presented (Davoudian *et al* 1994b) shows that these p_i are recalculated probabilities based on the organizational factors common to previous events and scaled as conditional probabilities found in the literature. The potential common-cause organizational factor of the initiating event (*IE*) and the basic events (*i*) is not included in the analysis. There is no consideration for the organizational factors that may affect the *IE*, or the ones that may affect the first basic event (p_1) or any other event independently. The increase in the probability of failure is only based on a common-cause type effect between two events.

The analytical example provided (Davoudian *et al* 1994b) corresponds to a MCS with two basic events, so that:

$$f_{MCS} = f_{IE} \cdot p_1 \cdot p_{2/1} \tag{9-17}$$

This formulation and the method described imply that for several basic events,

$$f_{MCS} = f_{IE} \cdot p_1 \cdot p_{2/1} \cdot p_{3/X_3} \cdot \cdots \cdot p_{n/X_n} \tag{9-18}$$

where any p_{n/X_n} is calculated based on X_n, which is determined as follows:

$$p_{n/X_n} = \max(p_{n/1}, p_{n/2}, p_{n/3}, \cdots, p_{n/n-1}) \tag{9-19}$$

For the particular case of the second basic event, the only possibility is $p_{2/1}$, but for the subsequent terms, the largest pairwise conditional probability p_{n/X_n} is adopted, as shown in (9-19).

Therefore, when a MCS is composed of several basic events, the dependence is still obtained from the relationship between pairs of events. The method implies that the modification of the conditional probability of failure of a component *n* is the same if calculated based on the previous event with highest dependence, than if calculated considering all the previous ones:

$$p_1 \cdot p_{2/1} \cdot p_{3/X_3} \cdot p_{4/X_4} \cdot \cdots \cdot p_{n/X_n} = p_1 \cdot p_{2/1} \cdot p_{3/2\text{-}1} \cdot p_{4/3\text{-}2\text{-}1} \cdot \cdots \cdot p_{n/(n-1)\text{-}(n-2)\text{-}\ldots\text{-}1} \tag{9-20}$$

This assumption can be considered "on the unsafe side", since the probability of a local failure when "several" other dependent failures occurred would tend to approach to 1.0.

For example, given the manual deactivation of the fire control system and the explosion that destroyed the control room at Piper Alpha (which, in turn, killed the OIM and control room operators), the probability of failure to restore the fire control system –and the following probabilities of failure to control the escalation in any other way– increased dramatically. For minimal cut sets of many basic events, some of the ultimate events may have conditional probabilities that are closer to complete dependence when several other failures have occurred.

The value of $p_{2/1}$ is determined by defining a Success Likelihood Index ($SLI_{2/1}$). A rating of each organizational factor for the plant and the weight of each organizational factor on every task of the event considered are evaluated for the determination of $SLI_{2/1}$.

$$SLI_{2/1} = \sum_{j} \left(R_j \cdot W_{2/1,j} \right) \tag{9-21}$$

The ratings (R_j) may be determined by different measurement procedures. They represent the performance of a plant on each of the organizational factors assumed relevant to safety and are determined for each working unit that interacts with plant equipment (Instrumentation and Control, Operations, Maintenance-Mechanical and Maintenance-Electrical). The weights Wj are obtained from experts who perform pairwise comparisons of the influence of organizational factors in each task, which are processed by a computer interactive Analytical Hierarchy Process in order to obtain the overall order.

The analytical hierarchy process method used to rank organizational factors assumes that they are mutually exclusive. Each event is characterized by only one CPG. The relative weights of all organizational factors considered are defined for CPG by integrating all the tasks of the work process that defines the basic event. The effective weight used in the calculation of equation (9-21) is:

$$W_{2/1,j} = \frac{W_{1j} \cdot W_{2j}}{\sum_j (W_{1j} \cdot W_{2j})} \tag{9-22}$$

This expression represents a dependence between the two events (1 and 2) that is in fact limited to the CPG of the tasks involved in the work process that defines each event. The effective weight is higher for a given organizational factor when both processes have a high weight for that organizational factor. For MCSs with more basic events, all combinations of effective weights are calculated, and the larger value is adopted for the calculation of the Success Likelihood Index ($SLI_{m/k}$, in general for a dependent probability p_m desired). The maximum dependence considered in the method is, therefore, only calculated between two events.

The actual probability is then calculated by

$$\log(p_{2/1}) = a \cdot SLI_{2/1} + b \tag{9-23}$$

where the constants are determined from these two equations with two unknowns:

$$\log(p_2) = a \cdot (SLI_{2/1} = 5) + b \tag{9-24a}$$

$$\log(p_u) = a \cdot (SLI_{2/1} = 1) + b \tag{9-24b}$$

The "anchor points" are p_2, which is the independent probability to which the best possible $SLI_{2/1}$ ranking is assigned, and p_u, which is a value assumed to represent the maximum dependent probability expected between events. The Success Likelihood Index ($SLI_{2/1}$=1) would correspond to the worst organizational performance for all organizational factors considered and complete dependency between CPGs. As a general rule, it is mentioned that a value of 0.5 could be used if events involve similar activities and 0.1 if they involve different activities. For traditional HRA methods (Gertman and Blackman 1994), 0.5 corresponds to the conditional probability between two low probability events, when there it is high dependence between them. The 0.1 value corresponds to about half way between moderate and low dependence (0.14 and 0.05 respectively). As mentioned before, this criterion may be "on the unsafe side". The determination of these two anchor

points is somewhat subjective, and does have an influence on the final $SLI_{2/1}$ value obtained.

9.4.3 Discussion

The numerical sample case analyzed (Davoudian *et al* 1994) shows a substantial increase in the probability of system failure of one MCS (f_{MCS}) due to the consideration of statistical dependencies. The increase is of about two orders of magnitude for only two dependent probabilities modified. It can be assumed that for MCSs with many basic events the increase should be more significant compared to the one calculated as statistically independent events.

The authors propose three methods to evaluate the impact of the increase of this MCSs on the overall core damage (system failure) frequency. The core damage frequency is more than doubled, after the evaluation of the dependent probabilities in the numerical sample case. The simplified methods tentatively proposed provide estimations for the overall core damage based on the analysis of only one of the failure paths. Given the complexity and non-linearity of the system, the lack of adequate knowledge of its behavior, and the still rudimentary method of evaluation, such further simplifications can only provide an uncertain estimation.

The weight of different organizational factors in different MCSs does not need to follow similar patterns, especially for the extensive, detailed and overlapping classification used. However, some kind of similarity is assumed in the methods proposed. The definition of the set of organizational factors is still an unresolved problem, even after many years of studies. The method assumes that the set is mutually exclusive (and collectively exhaustive) but no present classification fulfills those requirements. This assumption may increase the calculated probability of system failure in an unquantified amount.

9.4.4 Concluding Remarks and Recommendations

WPAM is expected to bring the probability of system failure (especially due to one failure path) closer to a realistic value. The order of magnitude of the overall

result is likely to be more accurate (and definitely more conservative) than the one calculated with independent probabilities of basic events.

This information can be valuable to assess the susceptibility of components and subsystems to organizational factors. It is also of outstanding value when the ALARA criterion ("as low as reasonably achievable"; or ALARP: "as low as reasonably practicable" for offshore) is used. Since ALARA/ALARP is based on an absolute value of probability of failure, a correction of this value may change its demonstration. However, it is not proven that this method can result in accurate absolute estimations (it does not consider effects that might increase the probability of system failure if considered). Thus, ALARP principle should not be applied based on it as a justification for not providing safety improvements. On the other hand, it could be used to show that a previous reliability evaluation that did not consider organizational factors does not actually fulfill the ALARP requirements.

The organizational factors used in extended classifications are "tokens" rather than "types". Four "types" of organizational factors can be derived from the application of the CANL model to the assessment of reliability in technological systems. All those types are –in turn– expressions of systemic imbalance. This broad understanding of systemic response within the organization can be tried as a way to simplify WPAM, without loosing accuracy.

However, the method is recommended (Davoudian *et al* 1994b) for use in assessments that are here considered outside of its range of applicability, such as sensitivity analyses of management policies and decisions.

Sensitivity analyses are done based on gross simplifications. There are no explicit justifications for the assumptions used in the sensitivity analyses. There seems to be no grounds to recommend that the resulting ranking of organizational factors or any other conclusion of such analyses can be used to "guide the direction of organizational improvements" (Davoudian *et al* 1994b). This use of WAPM-II can be misleading and counterproductive.

Moreover, management decisions should not be considered in the narrow scope of detailed (and yet under research) classifications of organizational factors. The detection of low organizational performance should trigger a process of global change of attitude that cannot be reduced to a training program or a study to improve formalization of work. A top manager should not be induced to believe that he can present the problem to an area manager (the one responsible for one organizational factor) and forget about the issue.

The idea that some organizational factors have more impact on risk is not only difficult to defend based on the present analytical tools but is also an inappropriate message to deliver to the top management. It may even become part of a "distortion of information" loop. The message should be that when the Reliability State of the Organization is not good, a general change of attitude is required to alter patterns that produce negative outcomes. The new attitude should influence all decisions.

9.5 Probabilistic Formulation - SAM and Accident Framework Model

9.5.1 Introduction

Paté-Cornell and Murphy (1996) use a "simple set of equations" similar to one developed earlier for the analytical approach of SAM (System-Action-Management). Moore and Bea (1993a, 1993b) use a set of equations based on the same structure for the Accident Framework Model. Both expressions are very similar, but they are used based on different interpretations of management and organizational factors.

9.5.2 SAM Probabilistic Formulation

Paté-Cornell and Murphy (1996) describe this formulation as follows. Considering just the physical system, the probability of system failure (F) is the sum

over the initiating events (IE_i) of the system failure probability conditional on that initiating event, times the probability of the initiating event:

$$p(F) = \sum_i \left\{ p(F / IE_i) \cdot p(IE_i) \right\} \tag{9-25}$$

Where each $p(F / IE_i) \cdot p(IE_i)$ is equivalent to the probability of system failure due to one MCS (f_{MCS}, in equation 9-16).

Both the probabilities of initiating events and the probabilities of system failure conditional on the initiating events are proposed by Paté-Cornell and Murphy (1996) to be influenced by decisions and actions (DA_j) of individuals within the system:

$$p(F) = \sum_j \sum_i \left\{ p(F / IE_i, DA_j) \cdot p(IE_i / DA_j) \cdot p(DA_j) \right\} \tag{9-26}$$

The conditional probability $p(F / IE_i, DA_j)$ is assumed to incorporate the probability conditional on DA_j for all the events along the failure path (all the basic events of each MCS).

Paté-Cornell and Murphy (1996) further propose that to assess the probability of relevant decisions and actions, they should be considered conditioned on "the relevant set of management factors", which are called M_k. The general probabilistic formulation proposed is therefore:

$$p(F) = \sum_j \sum_i \left\{ p(F / IE_i, DA_j) \cdot p(IE_i / DA_j) \cdot p(DA_j / M_k) \right\} \tag{9-27}$$

The authors explain that this model assumes that management factors affect the physical system only through human decisions and actions. They acknowledge that it is difficult to model the link between the so-called management factors (M_k) and the decisions and actions (DA_j) they induce (Paté-Cornell and Murphy 1996). This relationship is revised in section 9.6.

9.5.3 Generic Discussion of the SAM Approach

Paté-Cornell and Murphy (1996) propose that, while management may induce or fail to prevent dangerous individual behaviors, it can use some "control knobs" purposefully to reduce risk. They state that the management factors (M_k) represent these control knobs. Moreover, they further state (Paté-Cornell and Murphy 1996):

> *These control knobs may influence the state of the individual (fatigue, inexperience, poor training, etc), or they may affect the decision environment (e.g., though incentives, information, and procedures). This model allows comparisons of different risk management strategies involving tradeoffs between risk reduction and other dimensions (cost, productivity, profit, environmental effects, etc.).*

The interpretations that are proposed for this model by its authors might have a far-reaching negative impact. The image of "control knobs" seems at least misleading. An organization is not like a TV set that responds linearly to a control knob, but it is rather like a complex organism that responds in a non-linear and adaptive way to most impulses. Under the CANL model, decisions and actions by individuals tend to be shaped by reinforcing patterns of systemic behaviors, rather than by rational decisions and written objectives and policies elaborated by the top management. Moreover, the so-called "decision-makers" are usually strongly influenced by the system, too. The use of a rational actor model to justify the probabilistic formulation is not adequate to represent actual systemic behaviors within an organization.

Conversely, the CANL model approach is supported by many of the insightful observations presented by the authors in the same paper. Under the subheading "4. Common Threads and Casual Observations" they state (Paté-Cornell and Murphy 1996):

> 4.3 "Most of the time they [operators] simply react to their work environment, the incentives system to which they are subjected, and the information available to them". That is to say, they respond "in context"

with the system. These conditions and responses are not linearly related to the so-called "control knobs", but can be explained by the CANL model.

4.5 "The problem is that their [people's, operators'] goals and their risk attitude do not match those of the organization.... This discrepancy is often the result of management problems where policies (inadvertently) encourage undesirable behavior, or fail to screen out individuals who are more risk-prone than the organization". Again, the relationship among M_ks and AD_js is very complex and not linear at all. However, the CANL model can provide a good description of overall existing patterns.

4.6 "General policies seem to receive lower priority than specific directives". The rational actor model would allow for this inconsistency. However, the CANL model not only can explain its existence, but can also consider its contribution to the evaluation of the organizational performance.

4.7 "Management is often unaware of the 'shadow price' of the constraints that they set".

4.8 "Informal rewards seem at least as important as formal ones".

4.9 "Organizations seem to have difficulty in communicating the importance of safety".

4.10 "Informal organizational structure may be as important as formal channels". The CANL model assesses organizational behaviors as they effectively exist, independently of their "formal" or "informal" characteristics.

4.16 "People tend to ignore information that conflicts with their beliefs and wishes". This typical behavior is usually shaped by systemic imbalance, as described by "distortion of information" and "shift of the burden of

the proof". This observation would imply that the rational actor model should not be applied.

Given all these observations –which are consistent with the CANL model– it is not surprising that "the most difficult step is often the explicit quantification of the link between management factors and the actors decisions and actions" (Paté-Cornell and Murphy (1996). It is proposed here, then, that what conditions actions and decisions of individuals (both managers and operators) is a state of the organizational system, which can be defined through the CANL approach.

Faced with a complex system that is analyzed by simple linear tools, it is again suggested here that these tools should not be used to compare "tradeoffs" among management strategies. Furthermore, by creating the illusion of an objective analytical assessment, the use of these tools may induce dangerous states of distortion of information.

9.5.4 Accident Framework Model Probabilistic Formulation

Moore and Bea (1993a) propose a "general descriptive model of humans as components of man-machine systems". This approach is based on the statements as: "a fully descriptive model of the dynamic nature of human performance is not necessary for PRA modeling" and " "it is impossible to fully describe all aspects of human characteristics and behavior". Three phases are proposed for the implementation of this model (Moore and Bea 1993a):

- a preliminary QRA to identify the key subsystems or elements of the systems' reliability,
- an analysis process to identify the potential problems for each subsystem and their probabilities, and
- an analysis of the organizational procedures and incentives to determine their influence on the probability of basic errors.

As a basis for the last phase, the root causes behind system failures are represented in a hierarchical form. Basic events, such as component failures and

operator errors, are affected by decisions at a "Decisions and Actions Level", which in turn are influenced by organizational policy, procedures and culture at the "Organizational Level". The probabilistic model includes the determination of the set of possible initiating events (in_i) and final states of the system ($fist_m$). The probability of loss of components (platform, vessel, revenue, life, etc.) or, in general, system failure (F) can be then represented by (Moore and Bea 1993a, 1993b):

$$p(F) = \sum_i \sum_m \{p(F / fist_m) \cdot p(fist_m / in_i) \cdot p(in_i)\} \qquad (9\text{-}28)$$

The model is expanded to include relevant decisions and actions affecting the system at different stages during the lifetime of the platform (A_n). These are assumed to constitute an exhaustive and mutually exclusive set. The decisions and actions are then examined from the front-line operating crew level through the top-level management:

$$p(F) = \sum_i \sum_m \sum_n \{p(F / fist_m, A_n) \cdot p(fist_m / in_i, A_n) \cdot p(in_i / A_n) \cdot p(A_n)\} \qquad (9\text{-}29)$$

The effects of organizational procedures and policies on operational risks are determined through examining the probabilities of actions and decisions conditional on relevant organizational factors (O_h). The resulting expression proposed is:

$$p(F) = \sum_i \sum_m \sum_n \{p(F / fist_m, A_n) \cdot p(fist_m / in_i, A_n) \cdot p(in_i / A_n) \cdot p(A_n / O_h)\} \qquad (9\text{-}30)$$

Influence diagrams are used to represent the relationships among elements of the system, and to guide the application of the probabilistic formulation described.

9.5.5 Discussion

It is important to note that management decisions are, in fact, inputs to a complex, non-linear, organic system. Moreover, managers are "part" of the organizational system they "manage", thus also subject to its conditioning. Again, the assumption of a hierarchy of root causes with top-level decisions rigorously followed by specific decisions and actions is a misleading model.

The decisions and actions may be too many and too varied, due to its "token" nature. The assumption that A_n can constitute a collectively exhaustive and mutually exclusive set is almost impossible to sustain rigorously. By not considering the probability of system failure due to several organizational factors, the overall probability may be underestimated. Conversely, an expression conditional only on the organizational factors may prove more elegant and accurate.

9.6 Proposed Models for the Influence of Management on Human Actions

9.6.1 Introduction

Murphy and Paté-Cornell (1996) present four models for the evaluation of the link among the "management factors" and human actions. These models are required for the implementation of the SAM Framework. Three models attempt to represent the actor's intention, while one is intended to reflect the actual execution. Even if intention and execution are consecutive steps, the authors propose that these models could be used alternatively, so when an intention model is used, execution is automatically assumed as intended. Conversely, when the execution model is used, the intention is assumed correct.

In all cases, the authors propose to model the probabilities of decisions and actions by organization members, based on alternative scenarios defined by the management "control knobs" (Paté-Cornell and Murphy 1996). Management decisions, therefore, are excluded from the analysis. This analysis assumes that management decisions are represented by the rational actor model.

9.6.2 Rational Actor Model

The rational actor concept proposes that individuals make decisions based on their own rational best interest by maximizing expected utility. According to this model, decisions are determined by four factors: (1) the set of alternatives

considered, (2) the information available (subjective probabilities) about outcomes associated with alternatives, (3) consequences to the "actor" resulting from combinations of alternatives and outcomes, and (4) the preferences of the "actor". The "actor" is any individual within the organization who's decision is being modeled.

Murphy and Paté-Cornell (1996) propose that "by characterizing its own information about these factors, management can make reasonable predictions of an actor's behavior". Furthermore, they propose that management can also influence these factors in order to achieve the desired results. Some control is achieved, then, by "changing the problem that the actor implicitly solves" (Murphy and Paté-Cornell 1996).

Murphy and Paté-Cornell (1996) mention four strategies to influence decisions: (1) incentives, so that individual consequences are aligned with organizational outcomes, (2) resources, so that alternatives that are considered not appropriate become unfeasible, (3) information, so as to improve subjective estimations, and (4) change of preferences through socialization.

The Rational Actor model has been questioned based on cognitive limitations of people, the actual processes for selection and analysis of alternatives, and the influence of other context limitations. Besides these criticisms, in this case evaluators are assumed capable of identifying the alternatives that the "actors" would evaluate, their available information to estimate probabilities, their knowledge about the consequences, and their preferences. All these tasks should be performed for a complex organizational system, for many individuals, within complex formal arrangements (organizational charts) and subject to even more complex and dynamic informal networks.

Moreover, in order to reflect accident sequences the actual low probability events that determine system failures should be considered. System failures arise from combinations of *a priori* low-probability human errors and component failures.

Unless the context is adequately modeled, probability estimations would not be representative.

A major challenge that is not explicitly addressed by Murphy and Paté-Cornell (1996) is that this model should be usually fed with conflicting inputs. That is, management decisions aimed at improving safety usually have a negative impact in productivity. Conversely, management decisions aimed at profitability have widespread and usually unexpected influences on safety. Therefore, complementary decisions aimed at the attenuation of negative effects are common.

Given the uncertainty in the model, the proposition of reduction or resources to turn certain unwanted behaviors unfeasible may be dangerous. This strategy may also unwillingly reduce the potential for recovery under emergency conditions.

9.6.3 Bounded Rationality Model

The bounded rationality approach was developed in reaction to the rational actor model. It states that alternatives are not known in advance, so that the process of generating them has significant influence in the actual selection. When an alternative that satisfies the goals is found, usually the search ends without further analysis. Besides, this approach assumes that only one criterion is used at a time for the analysis of each alternative.

This approach does not provide an explicit quantitative model, so Murphy and Paté-Cornell (1996) propose one based on the sequence of alternatives analyzed. They propose that management can affect this process of decision by making certain alternatives more familiar (so that they would be analyzed first) and by inducing the use of a convenient criterion.

The probabilistic formulation for this approach is rather simplistic, and does not include explicitly the criterion that tends to be used first (it is only conditional on the sequence of alternatives). Any attempt to introduce this type of model should not neglect the criterion of selection, which is a very difficult task considering that safety and productivity and usual and conflicting ones.

9.6.4 Rule-Based Model

This model is based on Rasmussen's concept of rule-based behaviors. The "actor" uses a catalogue of pre-established rules that specifies the action appropriate for each circumstance. The "actor" does not consider alternatives explicitly. This model is proposed to be applicable in crisis conditions due to "threat rigidity", or lack of knowledge based decisions due to psychological pressures. However, the applicability of this model to accident sequences is not apparent.

The modelization is based on the identification of the situation and the rule base. It is proposed that management can affect "actor's" decisions by modifying these two conditions.

9.6.5 Execution Model

The execution model is aimed at the representation of the implementation of a given intention. It is based on the probability of error given the "actor's" ability and the task demand. Types of actor are defined based on their capabilities. Probability of error vs. task demand curves are used. It is proposed that management can improve the result of the execution by reducing task demands or increasing "actor's" abilities.

The curves that represent the relationship between task demand and probability of error are continuous. That is to say, this model assumes that for any increase in the demand there it is a continuous and finite increase in the probability of error. This assumption implies a mathematically convenient but unreal representation of human response.

9.6.6 Managers and the Rational Actor Model

The analysis assumes that managers would use this method to evaluate all alternatives and choose the one that maximizes expected utility... It assumes that managers act following the rational actor model. However, managers are subject to organizational factors such as distortion of information, shift of the burden of the

proof, time pressures and conflicts between safety and productivity. This omission by itself may alter the overall results significantly.

To explain this statement, the following probabilistic formulation is presented to assess the decision of a top-level manager:

$$P[D_j] = P[I_j] \cdot P[R_j / I_j] \cdot P[U_j / R_j] \cdot P[K_j / U_j] \cdot P[D_j / K_j] \qquad (9\text{-}31)$$

This expression proposes that the probability of a given decision $P[D_j]$ can be calculated as the multiplication among a sequence of conditional probabilities. It equals the probability that the written information is available in a document $P[I_j]$, and that given that it is documented it is read $P[R_j / I_j]$, and given that it is read that it is fully understood $P[U_j / R_j]$, and given that it is understood that the appropriate course of action is identified $P[K_j / U_j]$, and given that the best decision has been identified that it is finally taken $P[D_j / K_j]$. Of course, most of these terms make no sense in the rational actor model. However, given certain organizational factors of the real world, some of them might become surprisingly close to zero.

9.6.7 Discussion

The models proposed to represent human actions within the organization imply a high degree of uncertainty due to numerous simplifications. Under these conditions, it seems rather arbitrary to assume that the influence of management decisions on human actions can be assessed in complex organizations.

All models imply the identification of alternatives *a priori*. Evaluators are required to provide comprehensive alternatives for numerous, often unexpected, circumstances. The degree of detail required for these models seems difficult to be achieved in complex organizations, especially when a poor safety culture exists.

Influences on human actions are not only provided by management decisions. In fact, they only produce and indirect impact, after these decisions are "filtered" or "digested" by the organizational system. The assumption that management decisions

alter directly human performance can lead to significant errors in the estimation of low probability events.

In complex organizations, human actions (including management decisions) are influenced by actions and decisions of many "actors", by patterns of behavior, by time and economic pressures, by assumptions and quality of information. This analytical attempt fails to model these influences.

When the Reliability State of an Organization is bad, the decision models proposed by Murphy and Paté-Cornell (1996) do not hold. It is clear that they are not valid when an organization has a "myopic approach to safety" (Paté-Cornell 1995). The CANL model, on the other hand, is able to indicate when this happens.

The resulting model of decision-making should be based on the context given by organizational factors. Shift of the burden of the proof, distortion of information, productivity vs. safety imbalance, and time pressures create the conditions for a different type of decision-making process; one that does occur in the real world. Here the trite warning arises again: "it is the resulting discrepancies between the way in which the world is believed to be, and the way it really is, which contain the seeds of disaster" (Turner 1978).

10. RELIABILITY STATE OF AN ORGANIZATION

10.1 Introduction

In Part I, an understanding of organizational behaviors in technological systems was presented. Reliability assessment methods were reviewed in Chapter 9 with this approach in mind. It is concluded that probabilities of events (in particular local failures or basic events of a minimal cut set) can be expressed as dependent on an organizational state. This Reliability State of an Organization can be used as an indicator, in the wording used by Reason (1990a, 1990b).

Reason (1990a, 1990b) asks for the need to "establish an *a priori* set of indicators relating the system morbidity and then to demonstrate the causal connections between these indicators and the accident liability across a wide range of complex systems and in a variety of accident conditions". The system morbidity is the probability of system failure. The organizational factor types and the root organizational factors are proposed to identify the Reliability State of an Organization as a system indicator. This chapter defines this indicator and proposes a way to determine it, based on the CANL model.

10.2 Definition of the Reliability State of an Organization

The CANL approach is applied to identify the behavioral patterns that lead to reduction in reliability. There are many, complex and interrelated ways in which decisions and actions reinforced by systemic patterns alter the probability of system failure. All the deterministic paths based on a reductionist approach can not be fully identified, but probabilistic patterns can be shown with the CANL model.

The Reliability State of an Organization is the measure of the Root Organizational Factor through specific Organizational Factor Types. Any measure

scale adopted (for example a 1 to 5 scale) would be based in the interpretation of reinforced patterns of systemic behavior and their influence on reliability.

The Organizational Root Factor is defined by the way information and resources tend to flow within the organization. Outcomes that reduce system reliability and significantly increase the probabilities of local failures tend to emerge due to systemic imbalance. This is an observation based on the application of the CANL model.

The main identified types of organizational factors are either related to the treatment of information or resources allocation. One organizational factor is the "distortion of information". The distortion of information loop (Figure 3-4) shows patterns of decisions and actions reinforced by the organization that tend to increase the probability of failure. The other factors refer to the allocation of resources. The conflict between safety and productivity is usually identified as a factor that affects the reliability of a system. Patterns of behavior that induce an imbalance between these objectives can be identified and presented based on the CANL approach. The "shift of the burden of the proof" is closely related to the previous factor, but it is also present beyond this conflict. Both factors reflect a tendency in the assignment of resources such as personnel, equipment, infrastructure, and safety systems. Time pressure is the last type of organizational factor that reflects the way time tends to be assigned and the timeframe expected to produce results.

The Reliability State of an Organization is a generic measure. It is intended to assess general tendencies. It reflects non-deterministic patterns that tend to persist in time while disruptions do not occur. The organizational system, however, usually presents several particular alternative ways (tokens) to affect reliability. Reason (1990a) implies that human error tokens can become too many to be identified in an exhaustive list, here it is proposed that organizational factor tokens are too many and interrelated to analyze in detail. Classifications of organizational factors have attempted this path. The Reliability State and the four types described are a simple measure to represent the state of a complex and dynamic organizational system.

10.3 Determination of the Reliability State of an Organization

The Reliability State of an Organization can be determined in terms of a CANL model. A tentative procedure is proposed based on the methodology for assessment described in Chapter 6 and the concepts developed through Chapters 3 to 5. The four types of organizational factors are useful as a guideline to evaluate this indicator.

The tentative scale of 5 categories ranges from a best level 5 to a worst level 1. Level 5 would possess most of the qualities described for high reliability organizations, which have been proposed as representatives of an ideal condition (e.g. Roberts 1993, Roberts and Bea 1995). Level 1 could be assimilated, for example, to the conditions that caused the demand of organizational restructuring imposed to the operating company of the Millstone NPP by the Nuclear Regulatory Commission (NRC 1997).

This scale is proposed for an evaluation of the Reliability State of an Organization, based on a qualitative assessment of the four Organizational Factor Types, as determined after a system evaluation using the CANL model. The categories are described as follows:

Level 5 - Excellent: The loop diagrams reflect only loops that reinforce safety concerns.

- There it is no evidence of imbalance between productivity and safety, since safety is always declared and acted out as the overriding priority.
- There is no evidence of distortion of information, both formal and informal networks are well established and produce accurate and timely feedback among all areas of the organization.
- The burden of the proof for all kinds of decisions is actually placed as assumed or indicated in policies of the organization or external regulation.

- There is no evidence of significant time pressures and none of the members of the organization rate it as a concern.

Level 4 - Good: The loop diagrams reflect mixed behaviors, but the ones that reinforce unsafe actions and decisions are relatively weak. Some (but not all) of the following occur:

- There is some evidence of imbalance between productivity and safety, even if safety priorities are formally set.
- There is weak evidence of distortion of information, but formal networks and procedures are established to produce information feedback.
- The burden of the proof is clearly indicated in policies of the organization or external regulation, but may not be applied always in a strict way.
- There is some evidence of significant time pressures, but it is not felt strongly by any member of the organization.

Level 3 - Mediocre: The loop diagrams reflect mixed behaviors. Some behavioral patterns that reinforce unsafe actions and decisions are significant. More than two of the previous patterns occur and either one of the following:

- There it is evidence of imbalance between productivity and safety, and safety priorities are not well set.
- There is evidence of distortion of information, and formal networks and procedures are not well established to produce information feedback.
- The burden of the proof is not clearly indicated in policies of the organization or external regulation, and a pattern of unsafe shift away from the one implied in regulations can be observed.
- There is evidence of significant time pressures during certain periods, and it is felt strongly by some of the members of the organization.

Level 2 - Bad: The loop diagrams reflect consistent unsafe behaviors. All behavioral patterns reinforce unsafe actions and decisions at least in some degree. More than two of the previous patterns occur and either one of the following:

- There is strong evidence of imbalance between productivity and safety

- There is strong evidence of distortion of information.
- The burden of the proof is consistently shifted from the one implied in external regulations (if they exist).
- There is strong evidence of significant time pressures, and it is felt as a usual condition by some of the members of the organization.

Level 1 - Dangerous: The loop diagrams reflect consistent unsafe behaviors. All behavioral patterns reinforce unsafe actions and decisions at least in some degree. More than two of the previous patterns occur and aggravating conditions occur, such as threats, frequent violations, etc.

10.4 Updating of the Reliability State of an Organization

The updating of the Reliability State of an Organization can be performed through regular audits. It is acknowledged that this state may change in time, especially after new management policies are implemented (thus increasing the level, if successful) or due to inaction when unsafe tendencies are present (the effect called "degradation").

It is considered that the probabilities used in quantitative formulations are the best interpretation of the analysts, and not an absolute measure. Therefore, the values adopted can be updated, as more information becomes available. However, the general characteristics of the system must remain constant for this update to be valid.

The system is in permanent evolution, human and physical components and interconnections change continuously with time. A rigorous Bayesian update can only be performed if characteristics do not change (so that an inherent probability remains). In this case, probabilities conditional on the organizational Reliability State of the system (or the particular Organizational Factor Types) can be updated only if the Reliability State remains constant. Safety audits can be performed to assess the variability of the Organizational Factor Types, whenever more data on probabilities is collected. The use of this scaling for the Reliability State of the system would

allow for a criterion to justify Bayesian update of probabilities when the Reliability State remains constant.

11. QUANTITATIVE PROBABILISTIC FORMULATION

11.1 Preliminary Definitions

Probability of failure is the statistical likelihood that an element of a system will not perform as intended. Either human beings (as members of an organizational subsystem) or physical components (elements of physical subsystems), can fail to produce the input required by the technological system to perform as intended. Each one of those failures has at least local influence.

System failure is a condition by which the whole system suffers significant damage or loss of capability. It is a global failure, which is produced by a combination of local failures.

The concepts of latent and active failure are used throughout this work. Latent failures are those whose adverse consequences may lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defenses (as an analogy to latent errors, Reason 1990a). Active failures can be either physical component failures or human errors, but they always start a sequence that can lead to a system failure. Latent failures imply a reduction in performance or unavailability that does not directly initiate a failure sequence, and is not sufficient to lead to a system failure. However, latent failures are significant contributing causes for further failures and, therefore, for system failures. Latent failures, therefore, increase the probability of system failure given an initiating event.

The usual and expected mode of operation of a technological system requires that it corrects and avoids local failures, and –by all means– system failures are avoided. This normal operational mode can be described as a "failure damping mode" (Bella 1998a). When latent failures, local failures and/or component malfunctioning persists in time, a condition may be reached by which *a priori* local failures can become active failures leading to system failures. This condition, which

results from a non-linear flip in system response, is described as "failure amplification mode" (Bella 1998a).

Human error is an action or decision that does not produce the intended or expected input to the system. Chapter 2 reviews definitions and classifications of human errors available in the literature. Dougherty (1997) points at the distinction between the stochastic and uncertain characteristic of the components of human failure production. He concludes that human reliability is "stochastic in both ways that give rise to the need for probability models". Intrinsic variability is found in the initial conditions (even if the parameters of this random function depend on organizational factors) and, whether the human response is proposed as random or deterministic by different authors, the actual process is still random.

Organizational factors are states that influence the probability of local failures (both human errors and indirectly component failures). Several classifications of organizational factors are available which refer to specific ways organizational outcomes may affect system performance. Paraphrasing Reason (1990), these classifications are lists of "tokens". In this work, a more general classification is proposed, which attempts to represent "types" rather than tokens. The types of organizational factors proposed are: safety vs. productivity imbalance, distortion of information, shift of the burden of the proof, and time pressures. Each of these types affects decisions and actions of individuals (thus the probability of human errors and, indirectly, the probability of failure of physical components) through different paths that are represented by tokens.

All these factors have a common origin in a systemic imbalance that alters the flow of information and resources in the organization. Systemic imbalance is an emergent outcome of patterns of reinforced behaviors within organizations. The degree of imbalance represents an organizational state. Therefore, systemic imbalance is identified as the Organizational Root Factor, since all organizational factors can be traced back to this root cause.

The Reliability State of an Organization is a condition that can be assessed through the degree of systemic imbalance, or a measure of the Organizational Factor Types. By assessing the Reliability State of an Organization, probabilities of local failures can be adjusted. Probabilities of local failure can be defined and calculated conditional on the Reliability State of the system. The assessment of this organizational state can also provide a measure for the efficiency of the safety management system as a barrier for potential error solicitors, following Reason's (1990a) terminology.

11.2 Statistical Dependencies and Simultaneous Contributing Factors

11.2.1 Dependent Events

The statistical dependency among the probability of failure of components of a technological system is a basic characteristic of most complex system. Its consideration in the probabilistic approach is of fundamental importance. In general, due to availability of data and lack of deep knowledge of complex systems, independence of events used to be assumed. This assumption affects the estimation of the probability of simultaneous events or consecutive events in a failure path.

Correlation may be produced by common cause mechanisms and unexpected interactions between components. Correlation of human errors in a specific organizational context can be expected. Davoudian *et al* (1994b) consider it in a narrow sense. All individuals, each in their own way, are affected by similar organizational influences that shape personal behaviors in similar ways. Unsafe actions or decisions by managers or operators are not statistically independent when they are all influenced by the same organizational patterns.

In general, patterns of reinforced behaviors within organizations are spread throughout all levels and areas of an organization. Unless specific observations indicate different patterns in different departments or areas, they can be assumed

similar within a company. Moreover, the participation of personnel from different companies in one work environment does not guarantee independence of organizational influences.

11.2.2 Mutually Exclusive Events

Organizational influences are usually considered as mutually exclusive events. This assumption is wrong in general, and may affect significantly the results.

The classification proposed by Haber *et al* (1995), for example, has been used as a set of mutually exclusive dimensions. However, this classification is frequently presented in several categories or tiers, which share some common properties and are likely to occur simultaneously. Moreover, dimensions from other categories do not constitute mutually exclusive events. Not surprisingly, low probability/high consequence failures (catastrophic accidents) occur when several organizational factors exist simultaneously. This probability estimation conditional on multiple causes is usually neglected.

Human errors are also defined as mutually exclusive. However, there is no reason why an action can not be simultaneously caused by a cognitive error, impairment (such as fatigue), and an error in transmission of information; which may also be further compounded by lack of training and planning. All these are assumed as mutually exclusive by Bea (1994). The probability of such erroneous action would be orders of magnitude higher if all these errors are compounded in the same action. The same observation can be done if organizational errors are assumed.

11.3 Probability Conditional on the Reliability State of an Organization

Probabilistic formulations that include organizational factors have included the dependence between events, even if in a limited form (Davoudian *et al* 1994b). However, probabilities of local failures are not only related by common organizational factors, but also independently affected by them.

The probability of any single human error or component failure is increased when behavioral patterns sustained within the organization tend to reinforce decisions and actions that lead to a decrease in reliability. This modification is independent from the increase in the probability of failure due to a common-cause effect. As implied in formulations by Bea (1994, 1995b) and Paté-Cornell and Murphy (1996), the probability of initiating events is also increased by organizational factors.

Chapter 10 proposes a definition for the Reliability State of an Organization and a procedure for its determination. It is considered an indicator that can be evaluated periodically in order to assess the evolution of the system and update its reliability estimation. Organizational systems adapt to new inputs, so the dynamic evolution should be followed by audits based on the CANL model, and the update of the indicator. The CANL model used as a qualitative tool can also provide information to alert for unsafe tendencies.

11.4 Proposed Probabilistic Formulation for Organizational Factors

11.4.1 Introduction

The reliability of complex technological systems is dependent on the performance of the organization, as acknowledged by several authors (e.g. Bea 1994, Reason 1990a, Kirwan 1994). If models cannot "see" the characteristics of the organization, then they are missing important information.

The overall organizational characteristics provide significant information about tendencies, even when models are not able to capture the details of transient conditions. Latent failures tend to accumulate, thus increasing significantly the potential for "unexpected" combinations of local failures. It is assumed here that generic characteristics of the organization (types rather than tokens) can represent these tendencies. Patterns of behaviors within organizations tend to shape the

probabilities of failures of components, thus affecting the reliability of the technological system.

Post-mortem studies usually reveal combinations of events that were not predicted and, even after the event, are sometimes considered "almost impossible". *A priori* reliability assessments would reasonably give them a nil probability of occurrence. However, they do occur. The tokens may be impossible to list or evaluate accurately, but types can be monitored.

Human errors and physical component failures are usually due to several factors and causes. The probabilities are not always determined from a mutually exclusive, collectively exhaustive set of events or states. Correlations among events also exist, especially of the kind of multiple related failures (common cause effects). Moreover, there it is also a dependence on the state of the organization. A specific human error –even when considered independently from other local failures– will have a different probability depending on the actual patterns of behavior within the organization.

In this section, a probabilistic formulation is proposed. It is intended to underline the considerations necessary for a better approximation of the assessment to the objective reliability of a system. It is focused on the principles involved, rather than on the specific applicability of the expression.

11.4.2 Generic Probabilistic Formulation

In the case of the generic case based on the identification of inherently random component failures (E) and human related failures and errors (O) –criteria used by Bea (1994) (see 9.2)– the following expression is proposed:

$$Pfi = P\left[fi / E\bar{O}\right] \cdot P\left[\bar{O} / E\right] \cdot P[E] + P\left[fi / \bar{E}O\right] \cdot P\left[O / \bar{E}\right] \cdot P\left[\bar{E}\right] + \\ + P[fi / EO] \cdot P[O / E] \cdot P[E] \qquad (11\text{-}1)$$

where

fi = event that system fails to achieve some "i" quality attribute

$P[fi / E\bar{O}]$ = probability of system failure given component failures due only to "inherently random" causes (no human errors involved)

$P[\bar{O} / E]$ = probability of no human error given component failures due only to "inherently random" causes

$P[E]$ = probability of component failures due to "inherently random" causes

This expression accounts for multi causality of failures. Not all the terms have to be computed, since some are complements (e.g. $P[E]$ and $P[\bar{E}]$, $P[O / E]$ and $P[\bar{O} / E]$). It considers three forms of system failures, the ones only due to "inherently random" failures ($P[fi / E\bar{O}]$), as the traditional PRA methodologies initially considered; system failures due only to human errors ($P[fi / \bar{E}O]$); and system failures due to combinations of both ($P[fi / EO]$). The two last types include human errors and, therefore, organizational factors. However, this expression does not account explicitly for specific organizational factors.

11.4.3 Probabilistic Formulation for Organizational Factors

Whatever the classification adopted, organizational factors do not constitute a set of mutually exclusive attributes. For simplicity of the presentation, two factors are presented. The ultimate question is to determine the influence of organizational factors in the probability of system failure. A generic Venn diagram can be constructed as shown in Figure 11-1.

The two generic organizational states (Oe_1 and Oe_2) are not mutually exclusive. The probability of system failure (F) intersects the events of the two generic organizational states and goes beyond them (since system failures could occur even when organizational factors have no incidence). For the following analysis, only the system failure related to the organizational factors (f) will be

considered, and the sets will be renamed, so that they become mutually exclusive (Figure 11-2).

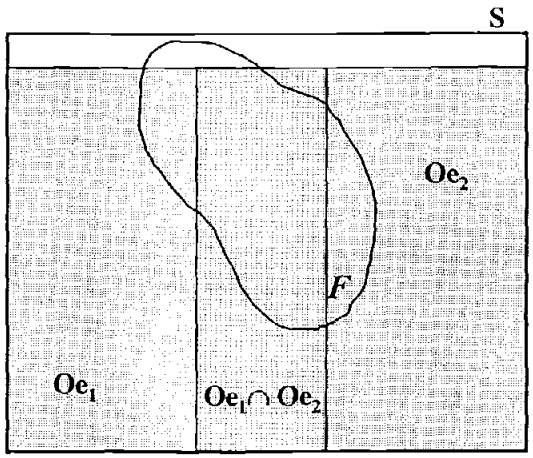


Figure 11-1
Venn diagram of probability of system failure and the relative influence of two generic organizational states.

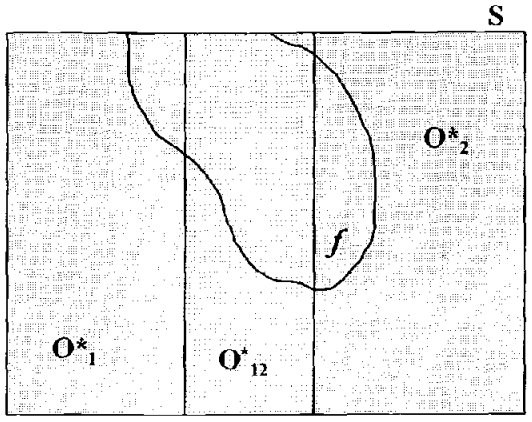


Figure 11-2
Venn diagram of probability of system failure conditional to two generic organizational influences but three artificially mutually exclusive sets.

The application of the theorem of total probability results in the following expression:

$$Pf = P[f/O_1^*] \cdot P[O_1^*] + P[f/O_2^*] \cdot P[O_2^*] + P[f/O_{12}^*] \cdot P[O_{12}^*] \quad (11\text{-}2)$$

The probability of system failure given only one organizational factor ($P[f/O_1^*]$ or $P[f/O_2^*]$) is relatively small, and the probability of occurrence of only one organizational factor ($P[O_1^*]$ or $P[O_2^*]$) can be assumed also small. Thus, the probability resulting from the first two terms can be usually assumed small, even if the probability of having one of these organizational factors increases. These are usually considered in some of the formulations that include organizational factors, even if $P[Oe_1]$ or $P[Oe_2]$ may be stated.

The probability of system failure due to several organizational factors (only two in this example, ($P[f/O_{12}^*]$) is much higher than the individual ones. Common cause mechanisms and independent increase of component failures due to the organizational factor produce a significant and non-linear increase. Conversely, the probability of having several organizational factors present ($P[O_{12}^*]$) is usually very small. However, this last probability can increase by several orders of magnitude when unbalanced patterns of organizational behavior reinforce unsafe actions and decisions. That is, $P[O_{12}^*]$ increases significantly when the organization has a poor Reliability State, where the number of latent failures is multiplied. This reasoning applies in the same way to many organizational factors as well, but the expressions get longer, and the probability of system failure given "all conditions against safety" may tend to a very large number (even close to 1.0).

Safety audits, in general, can identify the existence of reinforcing behavioral patterns that affect reliability or organizational factors. For any particular assessment, only one term needs to be calculated, given the organizational factor types detected.

Even if this formulation were not to be used for calculations, it describes a fundamental concept.

11.4.4 Formulation for Minimal Cut Sets

Within a formal PRA procedure, Minimal Cut Sets are determined. In this case, the previous formulation is adapted and the Reliability State of an Organization is incorporated such that:

$$p(f) = \sum_i p(f / IE_i, OF) \qquad (11\text{-}3)$$

where

f = event of system failure

IE_i = initiating event of each minimal cut set

OF = Reliability State of the Organization, determined as described in Chapter 10

The summation is theoretically over all MCSs, where both the dependence on the Reliability State and its common-cause effect are considered.

This formulation is not intended to be readily applicable, but to show the characteristics a formulation should have. Final users, the so-called "decision makers", tend to assume that the results of PRA provide an accurate measure for the probability of failure. In order to satisfy that assumption, the underlying probabilistic formulation must consider the elements described in this approach.

11.5 The "Other" Category

An inherent limitation of PRA is that all significant accident sequences must be identified. "No current PSA would include in its scenarios the events at Chernobyl or Peach Bottom" (Wu *et al* 1991). A category of initiating events identified as "other" was proposed, but "offers little practical help" (Wu *et al* 1991). One approach to incorporate this "other" category of initiating events into PRA would be to "determine a generic distribution of management quality versus occurrence

frequency of these events based on information obtained from industrial experience" (Wu *et al* 1991). The CANL model has the potential to serve this purpose.

Wu *et al* (1991) further propose:

> *For nuclear power plants with high quality of management, the occurrence frequency of the "other" events would be expressed by a distribution with low mean value with small uncertainty. The mean value for this expression would be relatively small compared with those for other anticipated transients and could be ignored. However, for plants with low management quality, more investigation is required on this class of initiating events.*

This proposal by Wu *et al* (1991) could constitute the justification for the omission of the "other" category of initiating events for organizations with good or excellent Reliability State.

Going a step beyond, the application of penalties by regulatory agencies of high-risk industries could also be justified. For example, an operating company may have its operating license suspended if the Reliability State is bad and it is not able to show that it has sufficient reliability through a methodology that fully incorporates the effects of organizational factors. This proposed regulatory policy would place the burden of the proof in a way that reduces risks. It is based on the recommendations by Bella (1997b) for the placement of the burden of the proof in the evaluation of projects with potential environmental impacts.

11.6 Incorporation into Quantitative Analyses

The forms of probabilistic formulation that include statistical dependence among events, common-cause effects (multiple related failures) and dependence on organizational factors could be used in QRA/HRA. The Minimal Cut set formulation can be used readily in PRA, while the more generic ones are suitable for some of the HRA approaches.

However, this incorporation does not guarantee that the intrinsic limitations of QRA/HRA methodologies have been eliminated. The methods would still be based on the evaluation of large numbers of events and MCSs. Only the development of new analytical methods designed to handle non-linear dynamics of complex human-physical systems could reduce, in theory, this uncertainty.

The determination of the Reliability State, needed to implement equation (11-3), is described in Chapter 10, but the specific relationship between the probability of human error or component failure is not defined. It is proposed that a generic relationship can be developed to increase the probabilities of those local failures or basic events by accounting for organizational factors. Procedures aimed at capturing detailed relationships (such as those based on influence diagrams) are considered too vulnerable to the complexities of actual personal and social relationships that define organizational influences.

The structure of WPAM could be modified to account for multiple dependence and independent condition on the Reliability State of the organization. It would still have the limitation that it only explicitly accounts for work processes, but further improvements could also be expected in this direction.

The CANL model has the potential to serve for evaluating the Reliability State of an Organization as an indicator of the probability of "other" initiating events, following Wu *et al* (1991). The relationship between the "others" category and the Reliability State of an Organization may lead to regulatory policies that place the burden of the proof on the operating companies when their Reliability State is not good enough.

The formulation proposed based on the CANL model and the ones analyzed in Chapter 9 are compared in Table 11-1. The embryonic formulation based on the CANL model is compared to others that have been developed with the aim of applicability in mind. Checkmarks indicate phenomena that are explicitly considered and question marks are shown when there seems to be potential for incorporation into the formulation.

Table 11-1
Comparison among probabilistic formulations

	Not Mutually Exclusive Organizational Factors	Common Cause Effect	Conditional on Organizational Factors	Multiple Causality
CANL model	✓	✓	✓	✓
WPAM	no	✓	no	?
SAM	no	?	✓	?
Omega Factor	?	✓	?	?
Mutually Exclusive	no	?	✓	no

The CANL model formulation can be used as a framework for the evaluation of the applicability of other probabilistic formulations, thus assisting in the formalization of engineering judgement.

11.7 Suitable and Sufficient QRA

The ALARP demonstration requires that "the duty holder should implement the measure unless it can be shown that the measure is not reasonably practicable" (Schofield 1998).

The burden of the proof is established by the UK law, and must be borne by the operator. In this case, a systemic shift of the burden of the proof (the regulator needing to prove that a safety measure is reasonably practicable) would be illegal. The UK offshore safety regulations require the "use of suitable and sufficient QRA for the demonstration that risks caused by certain hazards (those from fire, explosion, heat, smoke, toxic gas and fumes) are ALARP" (Schofield 1998).

Unless a new method that fully incorporates Organizational Factors is developed, or a good or excellent Reliability State can be shown in a particular platform at a given time, this legal requirement could not be fulfilled.

11.8 Preliminary Guidelines

It is proposed here that the Reliability State of an Organization can be used as an indicator to guide the use of quantitative methods and to suggest management and regulatory decisions..

When the Reliability State of the Organization is Excellent (level 5), the influence of organizational factors may not be significant. Even if the burden of the proof should be borne by the operator of hazardous systems, present methods of evaluation of reliability may be sufficient. The organizational factors implied by these methods may correspond to this state.

For a Reliability State of level 3 (Mediocre), organizational factors already influence reliability of the system. Any reliability assessment, either quantitative or qualitative, should include these factors explicitly. If any of the phenomena described in Chapter 11 is not accounted for in a quantitative method, it must be justified that they do not significantly alter the calculated value for the system. Quantitative results should not be used for risk calculations or demonstrations of the ALARP principle, unless they can be verified by alternative methods.

No available methodology can evaluate quantitatively and accurately the reliability for a level 1 condition (Dangerous). Regulatory decisions such as the one of NRC for the Millstone NPP on 1996 –shutdown until a fundamental reorganization is performed– are recommended. In these circumstances, the organizational system obviously needs a strong disruption to regain a state of minimum reliability.

At this stage of this research, specific guidelines for intermediate states are not proposed. However, any organization that is assessed to be below level 4 should immediately take large scale measures (not expensive programs, but widespread change of attitude) to improve its Reliability State.

12. CONCLUDING REMARKS – PART II

Organizational factors define states that influence the probability of local failures (both human errors and, indirectly, component failures). The types of organizational factors proposed are: safety vs. productivity imbalance, distortion of information, shift of the burden of the proof, and time pressures. Each of these types affects decisions and actions of individuals (and, indirectly, the probability of failure of physical components) through different paths. Post-mortem studies usually reveal combinations of events that were not evaluated or expected. *A priori* reliability assessments would reasonably give them a nil probability of occurrence. However, they do occur. The tokens may be impossible to list, but types can be monitored.

Organizational Factor Types have a common origin in systemic imbalance, which is an emergent outcome of patterns of reinforced behaviors within organizations. The degree of imbalance represents an organizational state. The overall systemic imbalance is, then, an Organizational Root Factor. The Reliability State of an Organization was defined based on these concepts and recommendations for its assessment were proposed.

This state, also called "safety culture" is of fundamental importance. It reflects pervasive patterns of behavior. It can be expected that given a poor Reliability State of an Organization, quantitative studies that reflect a bad safety performance would tend to be "dampened below disruptive levels", so deemed useless. The detection of an unsafe culture can be done by qualitative methods, as the one described on Chapters 6 and 10, based on the CANL model.

The approach also allows for the evaluation of quantitative methodologies. The assessment of the Reliability State of an Organization would allow for the adjustment of probabilities of local failures. Probabilities of local failure can be defined and calculated conditional on the state of the system.

Unsafe actions or decisions by managers or operators are not statistically independent when they are all influenced by the same organizational patterns. It is

stressed that managers are also influenced by organizational factors. Moreover, organizational factors are not mutually exclusive conditions in any of the classifications available, as usually considered. This assumption may affect significantly the results. Not surprisingly, low probability/high consequence system failures occur when several organizational factors exist simultaneously.

The probability of any single human error or component failure is increased when behavioral patterns sustained within the organization tend to reinforce decisions and actions that lead to a decrease in reliability. This modification is independent from the increase in the probability of failure due to common-cause effects.

Limits of the validity of QRA results should be carefully considered. A difference of several orders of magnitude can be caused by lack or insufficient assessment of organizational factors. The numbers resulting from QRA, then, may not reflect accurately what it might be expected to. A criterion to assess the validity of QRA results could be based on evaluations of the organization with the CANL model. If there were grounds to suspect that a plant or platform may have any organizational influence that alter the assumptions of the QRA/HRA methodology used, the results should not be considered as an absolute or accurate measure of the probability of system failure. This should also lead to the placement of the burden of the proof in order to reduce the risk. That is, the operator should prove that, through the full incorporation of organizational factors, a high enough absolute value of reliability is achieved.

When QRA cannot be justified to include organizational factors accurately, the ALARP principle should not be applied and absolute values of risk should not be calculated. The use of such tools for decision making can be only justified when a methodology for the calculation of system reliability based on the incorporation of organizational factors is developed and proven.

The probabilistic formulation should include the consideration for statistical dependence among events, common-cause effects (multiple related failures) and

dependence on organizational factors, in order to be used in analytical methods. However, this incorporation does not guarantee that the intrinsic limitations of fault-event tree analyses have been eliminated.

The determination of the Reliability State, needed to implement the equation proposed, was described. A specific relationship between this Reliability State and each probability of human error or component failure is not evaluated. It is proposed that a generic relationship can be developed to recalculate the probabilities of those local failures or basic events by accounting for organizational factors. Procedures aimed at capturing detailed relationships are considered too vulnerable to the complexities of actual personal and social relationships that define organizational influences, and therefore not recommended.

The proposed formulation is not intended to be readily applicable, but to show the characteristics that an acceptable methodology should have. Final users – "decision makers"– tend to assume that the results of QRA provide an accurate measure for the probability of failure. In order to satisfy that assumption, the underlying probabilistic formulation must consider the elements described in this approach.

As general preliminary guidelines, if an organization is assessed to correspond to a Reliability State of level 3 (Mediocre) organizational factors should be thoroughly incorporated into QRA. Level 1 (Dangerous) states should not be allowed to maintain operation given the extremely low reliability of the organization. For levels below 4 (Good), immediate actions should be taken to improve the safety culture or Reliability State of the Organization.

BIBLIOGRAPHY

Amendola, A (1989a) "Classification of Multiple Related Failures", in "Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment", A. Amendola (Ed.), Kluwer Academic Publishers, Dordrecht, Netherlands.

Amendola, A (Ed.) (1989b) "Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment", Kluwer Academic Publishers, Dordrecht, Netherlands.

Ang, A. and W. Tang (1975) "Probability Concepts in Engineering Planning and Design, Vol. I: Basic Principles", John Wiley & Sons, Inc, New York, NY.

Ang, A. and W. Tang (1984) "Probability Concepts in Engineering Planning and Design, Vol. II: Decision, Risk and Reliability", John Wiley & Sons, Inc, New York, NY.

Apostolakis, G., D. Okrent, O. Grusky, J. S. Wu, R. Adams, K. Davoudian, Y. Xiong (1993) "Inclusion of Organizational Factors into Probabilistic Safety Assessments of Nuclear Power Plants", IEEE

Argyris, C. and D. A. Schön (1978) "Organizational Learning: A Theory of Action Perspective", Addison-Wesley Publishing Company.

Barrell, A. C. (1992) "Control of Major Hazards Offshore – Implementing Lord Cullen's Recommendations" in "Major Hazards Onshore and Offshore", Institution of Chemical Engineers, Rugby, UK.

Basra G. and B. Kirwan (1998) "Collection of Offshore Human Error Probability Data", Reliability Engineering and System Safety 61:77-93.

Bea, R. G. (1994) "The Role of Human Error in Design, Construction and Reliability of Marine Structures", Ship Structure Committee, SSC-378.

Bea, R. G. (1995a) "Evaluation of Human and Organizational Factors in Design of Marine Structures: Approaches and Applications", Offshore, Mechanical and Arctic Engineering Conference 1995, Vol. II, 523-534.

Bea, R. G. (1995b) "Quality, Reliability Human and Organizational Factors in Design of Marine Structures", Offshore, Mechanical and Arctic Engineering Conference 1995, Vol. II, 499-512.

Bea, R. G. (1996) "Qualitative and Qualitative Risk Analysis – The Safety of Offshore Platforms", Offshore Technology Conference, OTC8037, 79-91.

Bea, R. G., R. Holdsworth and C. Smith (1997a) "Human and Organizational Factors in the Safety of Offshore Platforms", in "Proceedings of the 1996 International Workshop on Human Factors in Offshore Operations", R. G. Bea, R. D. Holdsworth and C. Smith, Eds, American Bureau of Shipping, New York, NY.

Bea, R. G., R. Holdsworth and C. Smith, Editors (1997b) "1996 International Workshop on Human Factors in Offshore Operations", American Bureau of Shipping, New York, NY.

Bea, R. G. (1997) "Human and Organizational Errors in Reliability of Offshore Structures", Transactions of ASME 119:46-52.

Bea, R. G. (1998a) "Structure Engineering Design Errors: Prevention, Detection, Correction" Journal of Structural Engineering, May.

Bea, R. G. (1998b) "Human and Organizational Factors: Engineering Operating Safety into Offshore Structures", Reliability Engineering and System Safety 61:109-126

Bella, D. A. (1987) "Organizations and Systemic Distortion of Information", Journal of Professional Issues in Engineering, ASCE, 113:360-370.

Bella, D. A. (1996) "The pressures of Organizations and the Responsibilities of University Professors", BioScience 46 (10) 772-778.

Bella, D. A. (1997a) "Organized Complexity in Human Affairs: The Tobacco Industry", Journal of Business Ethics 16:977-999

Bella, D. A. (1997b) "Organizational Systems and the Burden of Proof", in "Pacific Salmon and Their Ecosystem – Status and Future Options", D. J. Stouder (Ed.), Chapman & Hall, New York, NY.

Bella, D. A. (1998a) "Technology, Population and Global Climate Change", Civil Construction and Environmental Engineering Department, Oregon State University, Corvallis, Oregon (unpublished report).

Bella, D. A. (1998b) "Technology and Environmental Systems", Civil Construction and Environmental Engineering Department, Oregon State University, Corvallis, Oregon (unpublished report).

Bella, D. A. (1998c) personal communication, Spring, 1998.

Bignell, V. and J. Fortune (1984) "Understanding Systems Failures", Manchester University Press, Manchester, UK.

Blockey, D. I. (1980) "The Nature of Structural Design and Safety", Ellis Horwood Ltd, Chichester, U.K.

Boniface, D. E. and R. G. Bea (1996) "Assessing the Risk of and Countermeasures for Human and Organizational Error", SNAME Transactions 104:157-177

Collins, M. P., F. J. Vecchio, R. G. Selby, and P. R. Gupta (1997) "The Failure of an Offshore Platform", Concrete International: Design and Construction 19 (8) 28-35

Contini, S. (1989) "Dependent Failure Modelling by Fault Tree Technique", in "Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment", A. Amendola (Ed.), Kluwer Academic Publishers, Dordrecht, Netherlands.

Davoudian, K., J-S. Wu and G. Apostolakis (1994a) "Incorporating Organizational Factors into Risk Assessment Trough the Analysis of Work Processes", Reliability Engineering and System Safety 45:85-105

Davoudian, K., J-S. Wu and G. Apostolakis (1994b) "The Work Processes Analysis Model (WPAM)", Reliability Engineering and System Safety 45:107-125

Dougherty, E. M. (1997) "Is Human Failure a Stochastic Process?", Reliability Engineering and System Safety 55:209-215

Embrach, C. S. (1992) "Offshore Accidents Case Studies" Offshore, Mechanical and Arctic Engineering Conference 1992, Vol. II, 441-448.

Embrey, D. E. (1992) "Incorporating Management and Organisational Factors into Probabilistic Safety Assessment", Reliability Engineering and System Safety 38:199-208

Gertman, D. I. And H. S. Blackman (1994) "Human Reliability and Safety Analysis Data Book", John Wiley & Sons, Inc., New York, NY.

Goldfeiz, E. B. and A. Mosleh (1995) "An Approach for Inclusion of Organizational factors into Probabilistic Safety Assessment", in "Proceedings of the Topical Meeting on Computer-Based Human Support Systems: Technology, Methods and Future", ANS.

Goldfeiz, E. B. and A. Mosleh (1996) "A Methodology for Explicit Inclusion of Organizational Factors in Probabilistic Safety Assessment", Probabilistic Safety Assessment and Management 2:916-921

Gordon, R. P. E. (1998) "The Contribution of Human Factors to Accidents in the Offshore Oil Industry", Reliability Engineering and System Safety 61:95-108

Gottfired, P (1996) "Knowledge vs. Understanding", IEEE Transactions on Reliability 45 (3) 355.

Gusdmestand, O. T. and R. Gordon (1997) "The Role of Human and Organizational Factors (HOF) in the Fabrication, Installation and Modification (FIM) Phases of Offshore Facilities", in "1996 International Workshop on Human Factors in Offshore Operations", R. G. Bea, R. D. Holdsworth and C. Smith (Eds), American Bureau of Shipping, New York, NY.

Haber, S. B., D. A. Shurberg, R. Jacobs, and D. Hofman (1995) "Safety Culture Management: The Importance of Organizational Factors", Atomic Energy Commission USA, International Topical Meeting Safety Culture In Nuclear Installations, Vienna, April 1995.

Hirschhorn, L. (1993) "Hierarchy versus Bureaucracy: The case of a Nuclear Reactor", in "New Challenges to Understanding Organizations", K. H. Roberts, Macmillan Publishing Company, New York, NY.

Hollnagel, Erik (1993) "Human Reliability Analysis, Context and Control", Academic Press Ltd., London, UK.

Hollnagel, Erik (1998) "Cognitive Reliability and Error Analysis Method", Elsevier Science Ltd, Oxford, UK.

Hokstad, P., K. Oien and R. Reintsen (1998) "Recommendations on the Use of Expert Judgement in Safety and Reliability Engineering Studies. Two Offshore Case Studies", Reliability Engineering and System Safety 61:65-76.

Hurst, N. W., L. J. Bellamy, T. A. Geyer and J. A. Astley (1990) "Organisational, Management and Human Factors in Quantified Risk Assessment: A Theoretical and Empirical Basis for Modification of Risk Estimates", in "Safety and Reliability in the 90s – Will Past Experience or Prediction Meet our Needs?", Walter M. H. and R. F. Cox (Eds.), Elsevier Applied Science, London, UK.

IAEA, (1988) "Basic Safety Principles for Nuclear Power Plants", International Nuclear Safety Advisory Group report, 75-INSAG-3, International Atomic Energy Agency, Vienna, Austria.

IAEA, (1991) "Safety Culture", International Nuclear Safety Advisory Group report, 75-INSAG-4, International Atomic Energy Agency, Vienna, Austria.

Jacobs, R. and S. Haber (1994) "Organizational Processes and Nuclear Power Plant Safety", Reliability Engineering and System Safety 45:75-83.

Jakobsen, B (1992) "The Loss of the Sleipner A Platform", Proceedings of the Second International Offshore and Polar Engineering Conference, San Francisco, USA, 14-19 June 1992

Johnson, R. E. and H. P. Cojeen (1985) "An Investigation into the Loss of the Mobile Offshore Drilling Unit Ocean Ranger", Marine Technology 22 (2) 109-125.

Kirwan, B. (1994) "A Guide to Practical Human Reliability Assessment", Taylor & Francis Ltd, London, UK.

La Porte, T. R. and P. M. Consolini (1991) "Working in Practice but not in Theory: Theoretical Challenges in High Reliability Organizations", Journal of Public Administration Research and Theory 1 (1) 19-48.

Morone, J. G. and E. J. Woodhouse (1986) "Averting Catastrophe: Strategies for Regulating Risk Technologies", University of California Press, Berkeley and Los Angeles.

Moore, W. H. and R. G. Bea (1993a) "Management of Human Error in Operations of Marine Systems", Report No. HOE-93-1, Final Joint Industry Project Report, Dept. of Naval Arch. and Offshore Engineering Univ. of Cal. at Berkeley, December.

Moore, W. H. and R. G. Bea (1993b) "Human and Organizational Error in Operations of Marine Systems: Occidental Piper Alpha", Offshore, Mechanical and Arctic Engineering Conference 1993, Vol. II, 21-29.

Mosleh, A., E. B. Goldfeiz and S. Shen (1997) "The ω-Factor Approach for Modeling the Influence of Organizational Factors in Probability Safety Assessment", IEEE Sixth Annual Human Factors Meeting.

Murphy, D. M. and M. E. Paté-Cornell (1996) "The SAM Framework: Modeling the Effects of Management Factors on Human Behavior in Risk Analysis", Risk Analysis 16 (4) 501-515.

NRC (1996) "Notice of Violation and Proposed Imposition of a Civil Penalty" Notification by the Executive Director of Operations of NRC, June 4. (http://www.nrc.gov/OE/rpr/ea96059.htm)

NRC (1997) "Notice of Violation and Proposed Imposition of Civil Penalties" Notification by the Executive Director of Operations of NRC, December 10. (http://www.nrc.gov/OE/rpr/ea96034.htm)

National Transportation Safety Board (1983) "Capsizing and Sinking of the U.S. Mobile Drilling Unit Ocean Ranger off the East Coast of Canada 166 Nautical Miles East of Saint John's Newfoundland February 15, 1982" National Transportation Safety Board Marine Accident Report, Washington D.C., February.

Norman, D. A. (1988) "The Psychology of Everyday Things", Basic Books, Inc., New York, NY.

Offshore (1992) "Tests Suggest Likely Event Sequence in Sinking of Seipner A Base", Offshore 52 (8):48-51

Oliver, M. R. and J. Q. Smith (Eds.) (1990) "Influence Diagrams, Belief Nets and Decision Analysis", Wiley & Sons, New York, NY.

Paté-Cornell, E. (1995) "Managing Fire Risk Onboard Offshore Platforms: Lessons from Piper Alpha and Probabilistic Assessment of Risk Reduction Measures", Fire Technology 31(2):99-119.

Paté-Cornell, M. E. and D. M. Murphy (1996) "Human and Management Factors in Probabilistic Risk Analysis: The SAM Approach and Observations from Recent Applications", Reliability Engineering and System Safety 53:115-126

Peet, W. and R. Ryan (1998) "Risk management in a Network Operation – Understanding Complex Systems", in "Owning the Future – Integrated Risk Management in Practice", Elms, D. (Ed.) Centre for Advanced Engineering, Christchurch, New Zealand.

Perrow, C. (1984) "Normal Accidents, Living with High-Risk Technologies", Basic Books, Inc., New York, NY.

Pugsley, A. (1973) "The Prediction of Proneness to Structural Accidents", The Structural Engineer 6 (51) 195-196.

Rasmussen, J. (1986) "Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering", Elsevier Science Publishing Co., New York, NY.

Rasmussen, J. (1987a) "The Definition of Human Error and a Taxonomy for Technical System Design", in "New Technology and Human Error", J. Rasmussen, K. Duncan and J. Leplat, Editors, John Wiley & Sons, Ltd., Chichester, U.K.

Rasmussen, J. (1987b) "Cognitive Control and Human Error Mechanisms", in "New Technology and Human Error", J. Rasmussen, K. Duncan and J. Leplat, Editors, John Wiley & Sons, Ltd., Chichester, U.K.

Reason, J. (1987) "Generic Error Modeling System (GEMS): A Cognitive Framework for Locating Common Human Error Forms", in "New Technology and Human Error", J. Rasmussen, K. Duncan and J. Leplat (Eds.), John Wiley & Sons.

Reason, J. (1990a) "Human Error", Cambridge University Press, Cambridge, UK.

Reason, J. (1990b) "The Contribution of Latent Human Failures to the Breakdown of Complex Systems", Philosophical Transactions of the Royal Society, London, UK.

Roberts, K. H. (1993) "New Challenges to Understanding Organizations", Macmillan Publishing Company, New York.

Roberts, K. H. and R. G. Bea (1995) "Organizational Factors in the Quality and Reliability of Marine Systems", Offshore, Mechanical and Arctic Engineering Conference 1995, Vol. II, 479-485.

Rochlin, G. I. (1993) "Defining 'High Reliability' Organizations in Practice: A Taxonomic Prologue", in "New Challenges to Understanding Organizations", K. H. Roberts, Macmillan Publishing Company, New York, NY.

Rochlin, G. I., T. R. La Porte and K. H. Roberts (1987) "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea", Naval War College Review, Autumn 1987: 76-90.

Routledge, G. L. (1991) "A Paradigmatic Framework for Flight Safety", A PhD Thesis submitted to Oregon State University.

Sagan, Scott D. (1993) "The Limits of Safety, Organizations, Accidents and Nuclear Weapons", Princeton University Press, Princeton, NJ.

Schofield, S. (1998) "Offshore QRA and the ALARP Principle" Reliability Engineering and System Safety 61: 31-37.

Schulman, P. R. (1993) "The Analysis of High Reliability Organizations: A Comparative Framework", in "New Challenges to Understanding Organizations", K. H. Roberts, Macmillan Publishing Company, New York, NY.

Stephens, K. G. (1998) "Using Risk Methodology to Avoid Failure", in "Owning the Future – Integrated Risk Management in Practice", Elms, D. (Ed.) Centre for Advanced Engineering, Christchurch, New Zealand.

Tombs, S. (1990) "Piper Alpha – A Case Study in Distorted Communication", in "Piper Alpha- Lessons for a Life-Cycle Safety Management", Institution of Chemical Engineers, Rugby, UK.

Torroja, E. (1960) "Razón y Ser de los Tipos Estructurales" (Fundamentals of Structural Types), Editorial del Instituto Eduardo Torroja, Madrid, Spain (In Spanish).

Tuli, R. W., J-S. Wu and G. E. Apostolakis (1995) "Expanding Root Cause Analysis to Include Organizational Factors and Work Processes", Atomic Energy Commission USA, International Topical Meeting Safety Culture In Nuclear Installations, Vienna, April 1995.

Tuli, R. W., G. E. Apostolakis and J-S. Wu (1996) "Identifying Organizational Deficiencies Through Root-Cause Analysis", Nuclear Technology 16:334-358.

Turner, B. A. (1978) "Man-Made Disasters", Wykeham Publications, London, U. K.

Vinnem, J. A. (1998) "Evaluation of Methodology for QRA in Offshore Operations", Reliability Engineering and System Safety 61: 39-52.

Visser, R. C. (1992) "Offshore Platform Accidents: Their Effect on Regulations and Industry Standards", Offshore, Mechanical and Arctic Engineering Conference 1992, Vol. II, 97-102

Weick, K. E. (1990) "The Vulnerable System: An Analysis of the Tenerife Air Disaster", in "New Challenges to Understanding Organizations", K. H. Roberts, Macmillan Publishing Company, New York, NY.

Whalley, s. and D. Lihou (1988) "Management Factors and System Safety", Proceedings of the Safety and Reliability Society Symposium SARSS'88, B. E. Sayers (Ed.), Elsevier Applied Science, London, UK.

Wildavsky, A. (1988) "Searching for Safety", Social Philosophy and Policy Center, Transaction Publishers, New Brunswick.

Wu, J. S., G. E. Apostolakis and D. Okrent (1991) "On the Inclusion of Organizational and Managerial Influences in Probabilistic Safety Assessments of Nuclear Power Plants", in "The Analysis, Communications, and Perception of Risk", Garwick, B. J. and W. C. Gekler (Eds.), Plennum Press, New York, NY.

APPENDIX

SURVEY ON THE DESIGN ERROR OF SLEIPNER A

1. Introduction

A series of informal surveys were performed among Civil Engineering students at Oregon State University. The aim was to provide independent information about the general reaction the reinforcement design of the Sleipner A tricell may bring up to a structural engineer. This only reinforcement detail was assessed to be the cause of a major failure (Collins *et al* 1997). The surveys are limited in scope, but they may provide this generic reaction.

Two surveys were performed. A limited one took place among students who already had taken a concrete design course (CE481/581 Concrete Design - Civil, Construction and Environmental Engineering Department, Oregon State University). A survey comprising a large number of students was also performed among the ones taking such course at the time, during their second week of classes after a conceptual and intuitive introduction to concrete reinforcement. Both groups of students were presented similar questionnaires. The two groups are labeled post-CE481 and pre-CE481, respectively. Questionnaires were distributed to 15 students in the post-CE481 group and 51 students of the pre-CE481.

2. Questionnaire

Questionnaires used are presented as Figure A-1 to A-3. A one-page questionnaire was used for post-CE481 students and an additional question was used for the students taking the course.

In both cases, students were presented a basic questionnaire. They were shown a detail of the reinforcement at the tricell and were asked to answer the following questions:

- *Is there anything in this design that calls your attention? Please explain*
- *Please, indicate on the figure how you would guess this element may fail, if loaded until failure. In other words, draw where you expect to see cracks when overloaded.*

There was no further explanation about the context of the question. They were informed that they would get it after their response. The post-CE481 group was asked to return their responses during the following week (Figure A-1). The pre-CE481 group was given approximately 10 minutes to respond (Figure A-2).

After responding the questionnaire, pre-CE481 students were presented the following additional question (Figure A-3):

> *Imagine now that you are working for a large company. You get this reinforcement design (which is part of a large structure) and a computer output—which implies that this is not a critical point and that the indicated reinforcement seems to be well dimensioned. After your specific work (final dimensioning, for example), this detail will go directly to the construction site. What would you do?*

3. Results

3.1 Post-CE481 Basic Questionnaire

This group had a very low percentage of responses. Only 4 out of 15 students returned an answered questionnaire. From these four responses, one was accurate, one approximately right and two were wrong. One of the wrong answers corresponded to a student who had taken a concrete design course several years ago at another University.

3.2 Post-CE481 Basic Questionnaire

All the 51 students responded this questionnaire. Twelve (23.5%) correctly identified the problem, showing some understanding of the behavior of the T-bar, indicating cracks approximately right or indicating the need of additional reinforcement at the tricell with some clear understanding of the structural behavior. The remaining responses included different characteristics that were classified in 5

categories. Thirteen responses (25.5%) mentioned the critical area, but failed to demonstrate a good understanding of the structural behavior or demanded more reinforcement in the area but did not provide a good justification. Ten responses (19.6%) contained a misunderstanding of the drawing (they assumed that reinforcement was not symmetric, even if this was pointed out). Eleven (21.6%) provided other explanations that can be considered wrong. Three (5.9%) did not provide a sufficient response. Four responses (7.8%) indicated that there was nothing apparently wrong in the detail presented.

Table A-1
Summary of Responses for pre-CE481 Basic Questionnaire

	Number of Responses	Percentage Over 51
Error accurately identified and reasonable justification provided	12	23.5%
Error identified, but not justified correctly	13	25.5%
Confusion with drawing	10	19.6%
Other problem wrongly identified	11	21.6%
No error or deficiency identified	4	7.8%
Insufficient response	3	5.9%
Total	53	103.9%

The total number of responses was 51, but some were included in more than one category

3.3 Post-CE481 Additional Question

The additional question was responded by all the 51 students of this group. Twenty-one responses (41.2%) included the further analysis, revision and/or redesign of the detail and 19 (37.3%) mentioned that a hand calculation would be performed to check the computer model. Fifteen responses (29.4%) included the consultation with more experienced co-workers; and 18 (35.3%) included the information to supervisor or the consultation with original designer. Twenty-one

answers (41.2%) mentioned two or more of the above. Eight responses (15.7%) specifically added that they would not send the plans to the construction site if they had doubts about its safety. Six responses (11.8%) implied the submission of the plans with no further dues. Among them, one indicated that the legal value of the model output in a legal court would be checked, one stated that no further analysis would be performed if supervisor instructed to submit the plans, and one asked if the question was "technical or ethical".

4. Conclusions

The survey of the post-CE481 group is considered of no value for any conclusion. The response was too low. This was probably due to the lack of demand for a response and/or lack of commitment by the students.

The pre-CE481 group can provide statistically meaningful information. Almost 25% identified something wrong with the short T-head bar, and showed cracks approximately right. In general, about 50% (23.5% + 25.5%) identified the area as a critical one. It must be stressed that these are "second-week" students of concrete design.

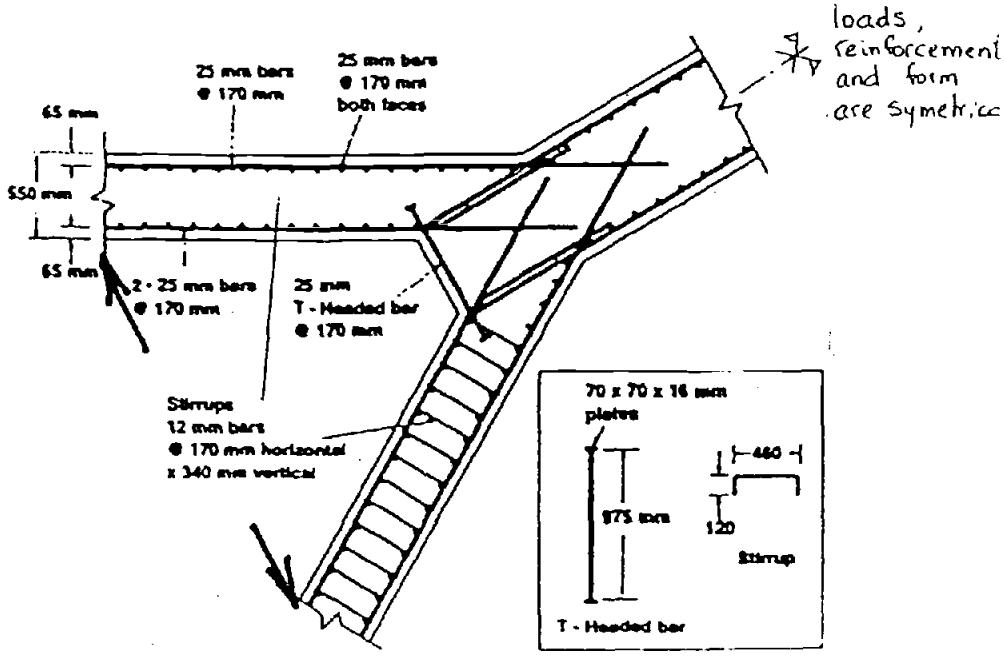
Almost 90% of these students mentioned either that they would perform hand calculations to roughly verify model results, revise the design, consult with more experienced co-workers or raise their concerns to their supervisors if they had doubts. More than 40% mentioned two or more of the above. Close to 20% indicated specifically that they would not send the plans to the construction site if they had doubts about its safety. Their good attitude seems the result from their education. They do not have professional work experience.

After responding to the questionnaires, they had a presentation with the explanation of the survey, the case study for this research, and the consequences of the failure. They were presented with the hypothesis that the raise of safety concerns within the design team could have avoided the collapse.

These questions are intended to be answered by students with background in concrete structures design. Please, do not respond if you don't feel you have this background.
This is not a test but, please, answer individually. Your responses may be used to complement research as part of my Masters thesis. I will explain the reason for this survey in a brief presentation in class.
I will be available for any question at biondie@ucs.orst.edu , 7-6891 or Graf 302.
Thank you for your cooperation.

Esteban L. Biondi

Please, look carefully at the reinforcement detail of the figure.
Two arrows indicate roughly the predominant loading.



1) Is there anything in this design that calls your attention? Please explain

.....

.....

.....

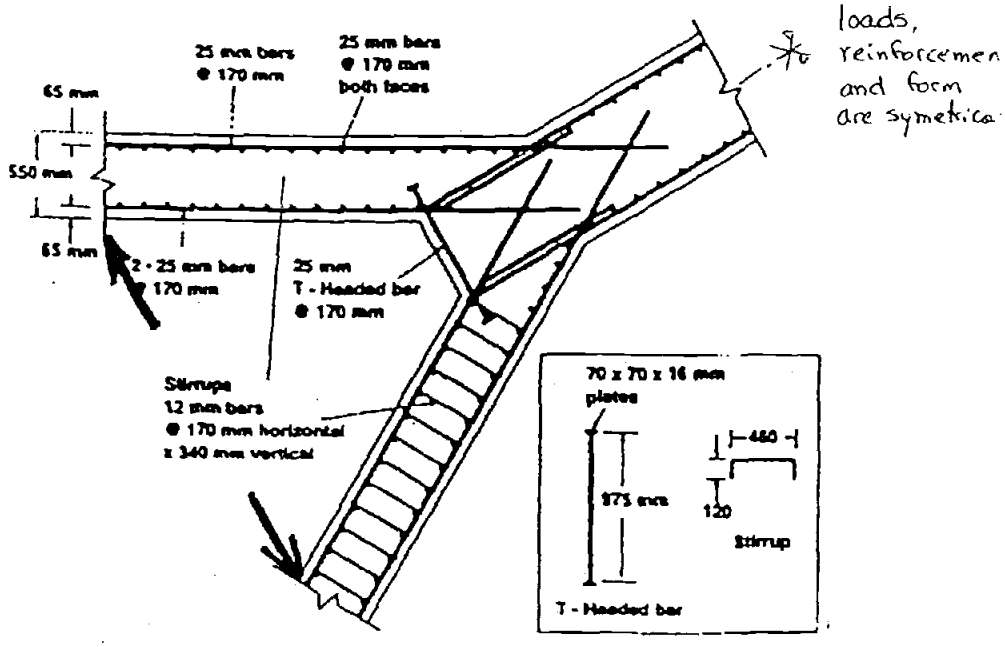
2) Please, indicate on the figure how you would guess this element may fail, if loaded until failure. In other words, draw where you expect to see cracks when overloaded.
3) Where did you take your basic course on concrete design? .....

Figure A-1
Basic Questionnaire for post-CE481 group

This is not a test but, please, answer individually. Your responses may be used to complement research as part of my Masters thesis. I will explain the reason for this survey in a brief presentation in class.
Thank you for your cooperation.

Esteban L. Biondi

Please, look carefully at the reinforcement detail of the figure.
Two arrows indicate roughly the predominant loading.



1) Is there anything in this design that calls your attention? Please explain

.....

.....

.....

.....

2) Please, indicate on the figure how you would guess this element may fail, if loaded until failure. In other words, draw where you expect to see cracks when overloaded

Figure A-2
Basic Questionnaire for pre-CE481 group

3) Imagine now that you are working for a large company. You get this reinforcement design (which is part of a large structure) and a computer output—which implies that this is not a critical point and that the indicated reinforcement seems to be well dimensioned. After your specific work (final dimensioning, for example), this detail will go directly to the construction site.
What would you do?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Figure A-3
Additional Question for pre-CE481 group