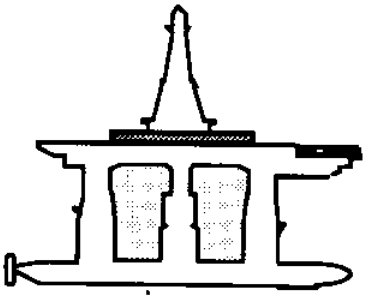
MANAGEMENT OF HUMAN ERROR IN OPERATIONS OF MARINE SYSTEMS



A Post-Mortem Analysis of the Piper Alpha Accident: Technical and Organizational Factors

by

M. Elisabeth Paté-Cornell

Report No. HOE-92-2
September, 1992

Department of Naval Architecture & Offshore Engineering
University of California, Berkeley

A POST-MORTEM ANALYSIS OF THE PIPER ALPHA ACCIDENT:

TECHNICAL AND ORGANIZATIONAL FACTORS

by M. Elisabeth Paté-Cornell
Professor of Industrial Engineering and Engineering Management
Stanford University

Research Report to the Joint Industry Project:
Management of Human Error in Operations of Marine Systems
Department of Naval Architecture and Offshore Engineering,
University of California, Berkeley

September, 1992

TABLE OF CONTENTS

FIGURES

PREFACE

This report concerns the accident that occurred in July 1988 on the platform Piper Alpha, owned and operated by Occidental Petroleum in the British sector of the North Sea oil field. The analysis of the system and of the organization presented here therefore applies primarily to Occidental-Aberdeen and to the Department of Energy of the United Kingdom which, at the time, was the relevant regulatory body. There is a wide range of practices among operators and among regulators. These practices may vary from place to place and from time to time.

Most of the information used in this study is based on the Petrie Report (1988), the Cullen Report (1990), the proceedings of the 1991 conference on Offshore Operations Post Piper Alpha, and on the prophetic book by Carson: The Other Price of Britain's Oil (1982). Other sources of information included conversations with knowledgable sources including Professor Robert Bea (the director of this project) at the University of California at Berkeley. The opinions expressed here, however, are those of the author, based on experience that includes similar problems in different service and product industries. They concern primarily Piper Alpha and may not apply to the rest of the oil industry, in the United States or elsewhere. Individual oil companies willing to draw a lesson from this tragic experience will thus have to decide for themselves whether or not they face similar situations. In many cases, only they have the relevant information.

Elisabeth Paté-Cornell
September, 1992

SUMMARY

In this report, the accident that occurred on the platform Piper Alpha in the North Sea on July 6, 1988, is analyzed both from a technical and an organizational point of view. The risk analysis framework is used to provide a systematic way of identifying (1) the accident sequence (failure mode) whose basic events include technical failures and human errors, (2) the decisions and actions that led to (or increased the probability of) the basic events, and (3) the organizational factors that influenced these decisions and actions. These organizational factors involved flaws in the design guidelines and design practices, in the management of the trade-off between productivity and safety, in the management of the personnel on board, and in the process by which financial pressures are applied on the production sector (i.e., the oil companies' definition of profit centers) which can result in deficiencies in inspection and maintenance operations.

One objective of this study is to derive from this analysis of the Piper Alpha accident a set of risk reduction measures, both technical and organizational, and an analytical approach to the assessment of their benefits. A general risk analysis model is presented with extensions to include the root causes of the basic events of the failure scenarios. An illustration is provided for the destruction by fire of the emergency water pumps. Fault tree analysis and a Markov model are proposed to compute the probability of failure of that system, and to identify how the probabilities involved can be decreased by different organizational and technical measures.

A POST-MORTEM ANALYSIS OF THE PIPER ALPHA ACCIDENT: TECHNICAL AND ORGANIZATIONAL FACTORS

M. Elisabeth Paté-Cornell

September, 1992

---

1. ACCIDENT AND ENQUIRIES

The offshore platform Piper Alpha, which was located in the British sector of the North Sea oil field and operated by Occidental Petroleum, was engulfed in a catastrophic fire on July 6, 1988 (Lord Cullen, 1990; Petrie, 1988). Piper Alpha received and sent to the shore the oil and gas production of a group of platforms (see Figure 1). The disaster caused the death of 165 men (out of 226) on board the platform itself, and 2 men on board a rescue vessel.

The accident chain started with a process disturbance, followed by a flange leak that caused a vapor release. Several explosions followed and severed a petroleum line causing a pool fire. That fire impinged on a gas riser from another platform, which fueled an extremely intense fire under the deck of Piper Alpha. The layout of the topside allowed the fire to propagate quickly from production modules to critical centers, and to destroy the control room and the radio room in the early stages of the accident (Figure 2). Electric power generation, public address, general alarm, emergency shutdown, and fire detection and protection systems also failed shortly after the first explosions. The superintendent of the platform (Offshore Installation Manager or OIM) panicked, was ineffective almost from the beginning, and died during the accident. Evacuation was not ordered, and even if it had been, could not have been fully carried out given the location of the living quarters, the layout of the topside, and the ineffectiveness of the safety equipment. Most of the evacuation routes were blocked and the life boats, all in the same location, were in most cases, inaccessible. The firefighting equipment on board

could not be operated because the diesel pumps, which had been put on manual mode and were inacessible and seem to have been damaged from the beginning. Fire boats were at hand, but waited for orders to fight the fire. When the master of one of the vessels on-site decided to assume the role of on-scene-commander (OSC), his fire-fighting monitors did not function properly. Piper Alpha was eventually lost in a sequence of structural failures. Over and above the tragic loss of life, the financial damage was in excess of three billion U.S. dollars (Bea, 1991).

The object of the enquiries that follow such a disaster is to understand what happened so as to prevent its replication. What complicates a post-mortem analysis is that the blame can be allocated in different ways according to the perspective of the investigator. The causes of the Piper Alpha disaster can be seen as a set of technical failures (due, for example to, insufficient redundancies in critical systems), or as an operator error during maintenance operations (i.e., a failure to tag the space of a safety valve replaced by a blind flange during maintenance operations) or as a fundamental problem of design (e.g., a layout that did not isolate sufficiently production modules from living quarters and command and control functions).

It can also be argued that the accident was caused by management and, for example, by the decision to dismiss warnings that a severe, prolonged fire could cause a catastrophe (Cullen 1990)[1]. In effect, the organizations that influenced operations on Piper Alpha included not only Occidental Petroleum that operated it, but also the oil industry at large and the U.K. government authorities which, at that time, had often adopted a hands-off attitude for economic and political reasons (Carson, 1982).

All of these factors contributed to the accident, with a hierarchy of causalities among them. As with many disasters, what ended up in a sequence of technical failures and human errors started mostly as a management problem (Perrow, 1984). There are therefore two ways to seek improvements given the lessons of Piper Alpha: to implement mostly technical remedies (e.g., better blast protection), or to promote better management practices (e.g., improvement of maintenance operations, or reduction of the production level when some systems or some backups are down). Such measures

can either be adopted voluntarily by the industry or imposed by regulatory authorities. Obviously, in a comprehensive approach, both engineering and managerial improvements must be considered. Both types of measures, however, are also costly in the short term. Engineering modifications often call for redundancies and decouplings that require additional equipment and/or space. Organizational modifications may increase safety at the cost of an occasional reduction of the platform production level.

Learning from the Piper Alpha accident thus requires understanding: (1) the effects of technical and organizational deficiencies on the occurrence of the chain of events in the accident of July 6, 1988, (2) the dependencies among technical and organizational failures, and (3) the costs and the benefits of risk reduction measures. The Piper Alpha Technical Investigation Report (Petrie, 1988) and the Public Enquiry into the Piper Alpha Disaster (Cullen, 1990) are important sources of factual information. They set the background of the accident, establish the sequences of relevant events and causalities among them, and make recommendations for the future. It is not the goal of either study, however, to structure in an analytical framework the causal links among events, decisions, and organizational factors that eventually led to the disaster, or to assess their relative contributions to the occurrence and the consequences of the accident.

Another important source of information is the study by Carson, a specialist of criminology, of the oil and gas production operations in the Bristish sector of the North Sea (The Other Price Of Britain's Oil, 1982). Written before the Piper Alpha accident, this book describes the political, economic, and regulatory climate in which the petroleum companies operated at the time in that region of the world, and its effects on safety.

The objective of this study is to provide an analytical framework to capture relations of causality between the different elements (technical, managerial, and organizational) of the Piper Alpha accident, starting from the basic human errors and component failures. The ultimate goal is to organize a "defense-in-depth" against platform accidents and to set priorities among safety measures. Some of the basic management issues include production pressures (rooted in financial goals and constraints), deficiencies in

personnel management, inappropriate inspection and maintenance procedures (e.g., the permit-to-work system), flaws in the design guidelines, and numerous modifications of the platforms' network, apparently without sufficient feedback to understand their effects on the system's safety.

The scope of this report includes first, the identification of the failure mode corresponding to the Piper Alpha accident scenario, of the decisions and actions that led to these events, and of the organizational factors that promoted these decisions and actions. This analysis points to a set of possible risk reduction measures (both technical and organizational) of which a few are then identified. Coarse estimates of the overall safety benefits of these measures can be obtained as a function of their reduction of the probability of the basic events of the different failure modes. A general risk analysis model (extended to link basic events to organizational factors) is presented here to that effect, and a more specific formulation is developed for a simplified system of emergency water pumps. No numerical computation is carried out at this stage.

2. THE RISK ANALYSIS FRAMEWORK FOR POST-MORTEM ANALYSIS

2.1 A three-step approach to technical and organizational factors

A post-mortem analysis is not a risk analysis since there is no uncertainty about the outcome: a specific accident scenario (failure path) occurred[2]. However, the risk analysis *framework* (i.e., the risk analysis *model structure*), extended to include some organizational factors, is used here to address sequentially the following questions:

1. What are the technical and human elements (basic events) of the main accident sequence? including: initiating event(s), component failures, operator errors, the final states of the system's components[3], and the consequences of the accident. This scenario can be identified as one of the failure modes in a general risk analysis model. If this model is described by an event tree, the accident sequence can be described as one "path" in this tree.

2. For each of the primary elements of this accident sequence, what are the decisions that have been made and the actions that have been taken (prior to the

accident in the different phases of design, construction, and operation of the platform, or during the accident itself) that influenced the probabilities of the basic events and the severity of their consequences?

3. For each of these decisions and actions, what are the organizational factors that have contributed to their occurrences and their consequences?

The use of this framework for risk management decisions then involves:

a. Identification of possible risk reduction measures that decrease the probabilities of the basic failures and events, either directly, or because they influence the decisions and actions that can cause these basic failures.

b. Estimation of the costs and the benefits of these measures, which may require either a partial risk analysis for those that affect a limited number of specific scenarios, or a complete risk analysis for those that reduce the probabilities of events common to many failure modes.

A description of this hierarchy of accident contributors is presented in Figure 3. In further sections and in Figure 3, the notations are the following:

BASIC EVENTS:

The basic events of the Piper Alpha accident have been labelled E_i, from i=1("process disturbance") to i=46 ("loss of the platform")

DECISIONS AND ACTIONS:

For each basic event E_i, a set of decisions and actions have been identified and labelled A_{ij} (e.g., for E_1, from j=1: "Production in Phase 1", to j=5: "design of the trip signals"). Each decision and action is related to the phase of the platform's life when it occured (DES: design, CONST: construction, OP: operation, and specifically, OPM: maintenance during operation).

ORGANIZATIONAL AND MANAGERIAL FACTORS:

Decisions and actions in each phase are then linked to different organizational and managerial factors (O_k). The sets {E_i's} and {A_{ij}} therefore provide a systematic tree (or matrix) structure for linking events, failures, errors, and decisions. After regrouping the

A_{ij}'s by platform life phase, the set of organizational factors $\{O_k\}$ provide the next level of linkage between failures and management.

2.2 Learning for risk management. Defense-in-depth

The objective of this approach is not primarily to identify the "culprits" in order to allocate the blame *a posteriori*, but rather to learn from the event and to identify the most cost-effective remedial measures. This perspective avoids the classic (and often sterile) debate: "it was a mostly a technical failure (just add redundancies and everything will be fine)"; "it was an operator error (those are unpredictable; so it is not our fault)"; "it was, in fact, a management failure (don't blame us; it is their fault)". It is often all three: most accident sequences do involve some technical failures (here, of a blind flange in module C) that were promoted or directly caused by some human decision or error (here, the failure of a maintenance crew to tell the night shift operators that a pressure relief valve had been removed from a condensate injection pump). But one reason why the fire turned into a tragedy is that couplings permitted by the design guidelines allowed it to spread unchecked to critical facilities and to block the evacuation routes. These human errors are often (but not always) promoted, if not directly caused, by management and its overall philosophy (Paté-Corn- 1990). For example, in the U.S., requirements for backups are quite specific for production equipment (API-RP23), much less specific for safety equipment, and inexistent for the composition of the crew[4]. As it is shown further, different aspects of the management structure, procedures, and culture at all stages of the platform life influenced the probability of the events that occurred during the Piper Alpha accident.

It has been shown that more than 90% of the failure probability of jacket-type offshore platforms involves at least some human errors or questionable judgments, most of which are grounded in organizational factors (Paté-Cornell and Bea, 1989). Yet, the technical characteristics of the system obviously influence the failure probability. Risk management can thus be viewed as the design of a comprehensive strategy combining technical and managerial elements, such as the design of inspection and maintenance

procedures tailored to the failure probabilities of the different parts of the system and their criticality to the overall safety (Paté-Cornell et al., 1989). The occurrence of a specific accident allows improvement of the current risk estimates for existing platforms (1) because it may reveal the possibility of scenarios that had been overlooked and (2) because it permits the probabilistic updating of the events that occurred during the accident. This updating of the risk estimates allows the decision maker to choose the most cost-effective alternatives among risk reduction measures.

2.3 The fallacy of probabilities after the fact: "freak events" versus "accidents waiting to happen"

After a catastrophe, there is often another debate regarding the prior probability of the accident: on the one hand, there are often some who claim that it was "an accident waiting to happen" (i.e., it had a very high prior probability), that warning signals were ignored, and that clearly unsafe practices were tolerated and even encouraged. On the other hand, others are quick to point out that the conjunction that led to the accident was very unlikely and that it was rational to tolerate the risk given the state of knowledge at the time. Those characterize the tragedy as "a freak event" or an unpredictable, unavoidable "human error".

The task of assessing *a posteriori* the probability of an accident that has already happened is a futile exercise except, perhaps, in the rare instances where the accident is the direct result of a specific event (or a clear chain of simple events) for which there is strong statistical evidence to support a probability of occurrence. For instance, when a flood with a known return period occurs, one can claim that it was (and remains) an event of probability X. In most accident sequences, however, the probability *a posteriori* can be made arbitrarily small depending on the level of detail that one adopts in the description of the accident. In other terms, the probability of an accident computed after the fact is determined by the way the accident is described. For example, if one specifies precisely the element that failed, the specified amount of gas released, the exact ignition source of ignition etc., the identified conjunction of events can be

attributed an extremely low probability, which can even be made lower if one specifies further details (time of the day, weather conditions etc.,) and as many factors as one may choose.

What matters, for risk management purposes, is the *class of relevant events* that led to the accident, not the fine details of the scenario. The choice of the relevant class of events is to some extent arbitrary (and part of the art of risk assessment) but determines the value of the information provided by the analysis. In the case of Piper Alpha, as it is described below, the critical classes of events are: a release of flammable material in module C, ignition, a sequence of explosions and fires leading to rupture of a riser bringing fuel at full capacity from an adjacent platform, an intense fire under the platform that could not be controlled, and the death, mostly by smoke inhalation, of a large number of people in the quarters who did not receive evacuation orders.

2.4 System complexities and failure dependencies

Complexity and couplings have sometimes been presented as the major source of failure risk in technical systems (Perrow, 1984). Piper Alpha presents examples of both. On offshore platforms, both are unavoidable to some degree: the level of decoupling that can be achieved after careful design still depends on the resources that one is willing to invest to increase the size of the topside.

Complexity *per se*, however, does not automatically reduce system safety. Risk depends on the system's configuration. Adding one element in <u>series</u> to an existing system generally increases its failure probability because the failure of this element is one more event that leads to system failure (unless the presence of this element decreases considerably the failure probability of the other components). Adding an element in <u>parallel</u> (a redundancy), however, generally *increases both complexity and safety*. The actual increase of safety depends on the level of dependency ("coupling", correlation) between the failures of the redundant elements: if they are highly positively correlated, the gain of redundancy is lower than if they are independent. It is thus advantageous to try to "decouple" to the greatest extent possible the potential failures of

different parallel subsystems, in particular when they are subjected to common causes of failure such as explosions or fires. Therefore, in general, even when there is a coupling between the parallel elements, the addition of redundancies brings some additional safety[5].

Altogether, a simpler system is generally preferable for management reasons: design errors are easier to detect, a simpler system is easier to manage and to maintain, and in an emergency, diagnosis is quicker than in a complex one. In the final analysis, the optimum level of complexity for maximum safety is the result of a trade-off between the number of redundancies, the level of coupling of these redundancies under common loads and external events, the space occupied by additional components, and the benefits of these additional elements. New communication links and computers, for instance, generally bring complexities and occupy scarce space for the benefit of the information that they provide. Only a global analysis provides an estimate of the balance.

The problem, in fact, is often *compactness* as much as *complexity*: a compact system is difficult to access, to monitor, to maintain, and the proximity of components packed in a tight space increases coupling. Technical *couplings* (or a high degree of dependency among component failures) do increase failure probabilities. Couplings are unavoidable when a large number of components have to be packed into a small area. However, the art of design for safety within space constraints is to avoid, whenever possible, several types of dependencies including:

° Correlations among the failures of redundant elements, either because the failure of one is the direct cause of failure of the other, or because the same common cause of failure (e.g., an explosion), is likely to destroy both. For example, one generally tries to physically separate as much as possible the hydraulic lines of an airplane, to disperse safety equipment, and to provide separate emergency power sources for redundant safety systems.

° Propagation of the effects of an external or internal event among elements in series (e.g., fire propagation, or domino effect in an earthquake).

° Component failures that can cause a release of chemical, energy, or other external or internal load increasing the probability of failure of other components.

° Location in the same space of fuel and possible sources of ignition (e.g electrical equipment) specially when external correlations are possible (the same event can cause simultaneous failure of the fuel container and of the electrical equipment.)

Organizational couplings are just as common a threat to safety as technical couplings. High dependencies in inspection and maintenance operations of two redundant elements increase the likelihood that the same signals of deterioration are missed or that the same short cuts are taken. More generally, the philosophy of the organization, its attitude towards safety, and the incentives that it provides for the management of the trade-off between production and safety constitute a strong source of dependencies among failures of different components and are perhaps, the most important source of couplings in the system. For example, in the case of the Piper Alpha accident, the platform experienced a double decapitation when, at the onset of the accident, it lost both its control room and the OIM function. The former was caused by technical couplings: the control room was located in the vicinity of the production modules. The latter was caused by couplings and lack of backups in the structure of the on-board organization: many safety decisions depended directly on the OIM and there was no immediate alternative authority to order the evacuation and to coordinate fire fighting operations[6].

3. IDENTIFICATION OF THE FAILURE PATH

3.1 Structure of the risk analysis model:

The structure of the risk analysis model presented in Figure 4 and Figure 5 is the basic tool for the first step of the analysis, i.e., to identify the "failure path" or accident sequence that occurred on Piper Alpha. Figure 4 represents a sequence of elements of a general risk analysis model in the form of an event tree to show the *failure path* corresponding to the accident. Figure 5 represents the accident scenario using an influence diagram format to show the *dependencies* among different classes of events.

The structure of a risk analysis model for the loss of a platform such as Piper Alpha in an accident initiated by fires and blasts involves the following elements:

INITIATING EVENTS

Explosions and equipment failures characterized by:

* location
* intensity
* amount of fuel released

Fires:

* presence (or not) of an ignition source
* severity (magnitude) of the fire as a function of the rate at which fuel and air feed the fire

INTERMEDIATE DEVELOPMENTS

Effectiveness of emergency shutdown

* Availability
* Actual performance

Destruction of key functions and key personnel:

* loss of power generation
* loss of emergency shutdown
* loss of communication functions
* loss of command and control

Performance of fire-fighting activities:

* availability
* ability to receive orders
* effectiveness

Fire propagation to other modules of the platform:

* which modules (control room, living quarters, etc)
* couplings among modules (effectiveness of fire walls and blowout panels)

* further explosions
* number of people threatened
* amount and propagation of smoke

FINAL SYSTEM STATE

* state of the different modules: no damage, smoke-filled, destroyed (measured, for instance, by a damage ratio)
* state of evacuation routes and passages
* availability and state of safety equipment
* state and effectiveness of rescue equipment

LOSSES

* number of casualties (death and injuries)
* amount of property damage (and other monetary losses, including loss of production)

For a complete probabilistic risk analysis, the system is first divided into modules, subsystems, and interfaces at an arbitrarily chosen level of disaggregation. The analysis can be structured using an event tree such as the one of Figure 4. The possible initiating events (occurrence of an initial explosion in each module) and independent events (e.g., presence of ignition sources in each module) are characterized by their probability per time unit. All subsequent events are characterized by their conditional probabilities given occurrences of events that precede them in the tree, for example: the probability distribution of the intensity of the initial explosion conditional on occurrence, of the amount of fuel released per time unit conditional on the intensity of the initial explosion, the probability of ignition given the fuel released, and the probability of propagation of a fire of given intensity from one module to another per time unit. The final result of the risk analysis is a probability distribution for the number of casualties and the amount of property damage (including loss of production)[7].

Classical fault tree and event tree methodologies, however, do not allow temporal analysis of fire propagation. Some of the conditional probabilities describing fire growth have to be computed separately using, for example, a Markov model involving the probabilities of transition from one state (fire location and severity level) to another state during each time unit (e.g., one minute). As shown further in Section 6, a Markov model with this structure can be developed for a time analysis of platform fire, capturing not only fire growth within a specific unit but also fire spreading among units. Such a model, however, requires a larger number of states to represent the different levels of fire severity in the different modules. An analysis involving the amount of released fuel and the presence of ignition sources determines the initial states, characterized by the location and intensity of the initial fire. The model specifies the subsequent states (including fires of different levels of severity in different modules) and the probabilities of state transition per time unit.

A similar model, presented here in appendix, has been developed in a previous study to allow accounting for the benefits of early fire detection and for the effectiveness of fire fighting operations in an oil refinery (Paté-Cornell, 1985). In that study, a Markov model of this type was used to assess the effects of camera monitoring in an oil refinery. The transition probabilities were allowed to vary to represent fire growth in the different fire fighting phases: first, an active growth phase (where the fire grows unchecked), second, a detection phase (the fire is detected but not yet fought) during which the fire grows at the same rate, third, fire growth during the initial fire fighting phase (reduced probabilities of propagation to other modules or of transition to increased intensity), fourth, a "controlled" growth where the transition probabilities are much smaller, and fifth, an extinguishing phase. The "very large" fire state (including the possibility of full destruction of the system) can be reached in any one of the fire growth phases including the active phase if the fire is never effectively fought[8].

The result of such a model is a probability distribution for the final losses based on the transition probabilities that describe the system and its mode of operation. Such a Markov model can be developed for a platform similar to Piper Alpha in order to assess

the benefits of alternative measures of fire risk reduction by the difference between the mean values of the final losses with and without the considered measure[9]. These measures can be characterized by new probabilities of transition among the system's states. For example, a fire detection system increases the probability of transition from active growth to detection phase, therefore reducing the time of unchecked growth. The effect of fire fighting measures aimed at decreasing the amount of fuel into the fire is to decrease the probability of transition to larger fires in the "working growth" phase. The corresponding benefits are measured by the displacement of the loss distribution towards lower values. The difference in the mean losses is one possible measure of the benefits.

3.2 The Piper Alpha failure mode and accident sequence

For Piper Alpha, it is useful to start with the identification of the basic events of the *failure mode* (i.e, the events that are necessary links in the accident sequence) to analyze to what degree they have been induced by human actions and to identify systematically the organizational roots of the accident. This *post facto* failure mode identification thus does not involve probabilities. It also excludes secondary events that may have promoted the basic events but are not part of the failure mode. The basic events of the accident sequence are labeled as indicated in section 2.1 so that they can be matched with causal decisions and organizational factors. Note that the labelling has been chosen for analytical purpose and *does not imply a chronological order.* In particular, the initiating events and the major loads (fires and explosions) have been separated from their consequences.

<u>INITIATING EVENTS (IE): MAJOR EXPLOSIONS AND FIRE LOADS</u>

The references for this section are the Cullen Report (Cull.) and the Petrie report (Pet.). Times are indicated for some events. Included in "initiating events" are not only the actual initial explosion and fire, but also the subsequent ones which initiated further component failures.

A] PRIMARY INITIATING EVENT (IE1): **First explosion**. July 6, 1988. 21:58.

E1: Process disturbance (inadvertent pressurization of a PSV) 21:45 to 21:50.

E2: Two redundant pumps inoperative in Module C: condensate pump 'B' trips. 'A' was shut down for maintenance.

E3: Failure of a blind flange assembly at the site of PSV 504 in module C.

E4: Release of condensate vapors in module C (~45 kg, filling ~25% of the module volume); failure of gas detectors and emergency shutdown.

E5: First ignition and explosion. Possible ignition sources: hot surfaces, broken light fitting, electrostatic sparks, electric motors (Cull. p.60).

E6: Almost total failure of gas detectors and fire detection/protection (deluge) systems.

E7: Partial failure of emergency shut down system (Cullen, 7.63).

E8: Failure of C/D fire wall. Failure to prevent destructive overpressure inside the module (blowout panels).

Failure of emergency systems (E6 and E7) and failure of containment function (E8) led to further explosions:

B] SECONDARY INITIATING EVENT (IE2): **Second explosion**. Propagation of fire in module B. (Almost immediately, i.e., shortly after 22:00).

E9: Rupture of B/C fire wall (single layer, 4.5 hour integrity wall).

E10: Rupture of a pipe in module B (projectile from B/C fire wall).

E11: Large crude oil leak in module B.

E12: Fire ball and deflagration in module B.

E13: Fire spreads back into module C through breach in B/C fire wall.

E14: Fire spreads to 1,200 barrels of fuel stored on deck above modules B and C.

C] TERTIARY INITIATING EVENT (IE3): **Jet fire from broken riser** (22:20)

E15: Failure of fire pumps: automatic pumps have been turned off; manual (diesel powered) pumps located in module D damaged by failure of C/D fire wall.

E16: Rupture of riser (Tartan to Piper Alpha) caused by pool fire beneath it (E5, E12, E13); "high temperature reducing the pipe steel strength to below the hoop stress induced by internal pressures" (Cull. p.133).

E17: Intense impinging jet fire under the platform.

FURTHER EFFECTS OF INITIATING EVENTS (in addition to causing other initiating events) AND FINAL SUBSYSTEMS' STATES

A] From IE1 (**consequences of first explosion**):

E18: Immediate loss of electric power.

E19: Failure of emergency lighting.

E20: Failure of the control room (no lights on mimic panels).

E21: Failure of the public address/general alarm system.

E22: Failure of the radio/telecommunication room.

E23: Loss of the OIM function, both on board and as OSC of rescue operations.

E24: Smoke prevents the Tharos helicopter from reaching the helideck.

E25: Fire and smoke envelop the North side of the platform.

E26: Casualties in A, B, C modules.

E27: Escape of some people from 68ft level to 20ft level -> some jump into the sea.

B] From IE2 (**consequences of second explosion**):

E28: Fire from modules B and C spreads to various containers ("lubricating oil drums, industrial gas bottles: oxygen, acetylene, butane "(Petrie)).

E29: Fire from modules B and C causes rupture of pipes and tanks -> growth of oil and condensate fires.

E30: Some survivors jump into the sea from 68 ft and 20 ft levels.

E31: Some people are engulfed in smoke and die in the quarters (22:33)

E32: Partial failure of Tharos fire-fighting equipment.

C] From IE3 (**consequences of the jet fire**)

E33: Rupture of the MCP-01 riser at Piper Alpha.

E34: Most people remain and are trapped in living accomodations (more survivors jump into the sea from the 20 ft and the 68 ft levels).

E35: Third violent explosion (22:52).

E36: Some survivors jump from the helideck (175ft levels).

E37: Collapse of platform at 68ft level below B module (22:50).

E38: Collapse of western crane from turret (23:15).

E39: Fourth violent explosion (23:18): rupture of Claymore gas riser.

E40: Major structural collapse in the center of the platform.

E41: Slow collapse of the north end of the platform

E42: Collapse of the pipe deck, White House, and OPG workshop (-> additional casualties).

E43: Accomodation module over-turned into the sea (AAW north end of platform) (00:45).

E44: Rescue of survivors at sea. Through out the accident, people who jump and survive are rescued by semi-submersible vessel Tharos, stand-by vessels Silver Pit and Lowland Cavalier, and supply vessel Maersk Cutter.

LOSSES

E45: Human casualties: 167 (165 men on board; 2 rescue workers).

E46: Loss of the platform; damage in excess of three billion U.S. dollars.

4. DECISIONS AND ACTIONS SPECIFIC TO PIPER ALPHA

4.1 Identification of human factors linked to the basic events of the Piper Alpha accident:

The object of this section is to identify the decisions and actions specific to Piper Alpha that led to each of the basic events (the next task being to look for organizational roots beyond the Piper Alpha case). Some of these decisions are clear errors; others are judgments that may have been acceptable at the time when they were made but

proved catastrophic in conjunction with other events, some of which could have been anticipated. As indicated in Section 2, decisions and actions are noted Aij (corresponding basic event Ei) and labelled according to the phase where they occured: design (DES), construction (CONST), operation (OP) and more specifically, maintenance (OPM).

E1: Process disturbance around 21:45

E1 which triggered a sequence of compressor trips and gas alarms is the result of a system overload and operators' confusion that can be linked to:

A 1.1: Production in the Phase 1 mode (OP)

A 1.2: Physical and managerial interdependencies in the Piper Alpha-Tartan-Claymore-MCP-01 network (DES; CONST)

A 1.3: Decision to promote personnel to critical positions on a temporary basis (OP)

A 1.4: Missed signals (OP)

A 1.5: Insufficient redundancies in the design of trip signals (DES)

Phase 1 production had rarely occurred in the past on Piper Alpha. It occurred because the gas driers essential to Phase 2 operations had been shut down and isolated for routine maintenance (Petrie, 4.2.1.3). Phase 1 operations resulted in high pressures in the system (650 psi instead of the normal 250 psi in Phase 2 (Pet. 4.2.4.2)) which was much more likely to strain the equipment than the regular production mode. Distributed decision making within the platform network (Piper Alpha, Tartan, Claymore, and MCP-01) compounded the problem of managing high-pressure operations with only remote control (at best). There was therefore a conjunction of a *high level of physical coupling* among the platforms and a *low level of management/organizational coordination* (Cullen). The network had apparently grown in an un-preplanned manner as the system was developed and constructed over time to accomodate new needs, production parameters, and regulatory requirements (e.g., the gas conservation project). These changes were jointly decided by corporate and local management, sometimes

under regulatory constraints (e.g., addition of the gas conservation module). The mode of operation evolved in the first years towards higher levels of production, with a peak of about 320,000 barrels per day in 1979. These changes have also involved, at times, higher pressures and higher density of equipement on the deck, perhaps without sufficient checking that the system could safely accomodate the load increment.

High pressures can cause problems of varying severity with warning signals such as vibrations, roaring flares, small leaks etc. These symptoms require immediate attention, detection and diagnosis capabilities, and therefore experienced operators (Pet. 8.1.2). Unfortunately, this experience was probably not available. First, there had not been much opportunity to learn about Phase 1 operations. Second, the problem was compounded by the temporary promotion of a certain number of employees to positions above their regular level of responsibility, a regular practice on Piper Alpha. On the night of the accident, the production team consisted of five operators (which is the minimum number of persons who can operate the plant) and the members of the production management team had all been promoted one level above their normal position (Pet.8.1.5) and therefore had less experience than the old-timers who managed operations in normal time. A sequence of signals were not given sufficient attention (for example, the fact that the south west flare was roaring and larger than normal) and "the control room operator did not check which heads were detecting gas prior to the explosion" (Petrie, 5.14.1). Furthermore, in Phase 1, there was insufficient redundancy in the signals of alarm, i.e., one single trip signal (Pet.10.1.4) .

E2: Failure of both condensate injection pumps in module C:

A 2.1: Apparently improper maintenance of both pumps A and B (OPM)

A 2.2: Decision to remove PSV 504 in pump A and to replace it by a blind flange (OPM)

A 2.3: Failure of the maintenance crew to inform the night shift that pump A was out and that the PSV was missing (-> operator error in trying to restart pump A) (OPM)

Both pumps A and B had been maintained shortly before the accident. It seems however, that only minimum work was performed; what was clearly broken was fixed; the rest does not appear to have been thoroughly checked (Pet.8.3.3.14). The decision to remove a pressure safety valve in pump A for maintenance is consistent with the view that there was one redundancy (B) and that it was sufficient to continue operations.

Then, a serious failure of communication occurred between the day crew and the night shift; the night crew who had not been informed that PSV 504 had been removed, tried to restart pump A (Pet.8.3.2.12). This failure can be traced back to the work permit system (Cullen, Chapter 11) and is discussed further in Section 5.

E3: Failure of the blind flange assembly at the site of PSV504

A 3.1: Error in fitting of the blind flange (OPM)

A 3.2: No inspection of the assembly work (OPM)

The blind flange was not leak tight. The assembly can be made "finger tight", "hand tight" or can be "flogged up". Experts concluded that only a "finger tight" assembly could experience a leak of this magnitude (Cullen, p. 102). Furthermore, there was no inspection of the work, and an error in fitting, if it happened, could not have been detected and fixed.

E4: Undetected release of condensate vapors in Module C

A 4.1: Problems with the warning systems for gas release (DES; CONST)

A 4.2: Failure to fix the warning system after it issued false warnings (OPM)

A 4.3: Poor design of the monitoring panels in the control room (DES)

A 4.4: Failure of the control room operator to read and interpret the signals (OP)

About 45kg of condensate were released in module C and should have been detected before an explosion could occur; but there were two problems with the warning system for gas release: first, it issued false alerts that may have caused real ones to be ignored, and second, there were read out problems in the control room (Pet.5.14) that were due to the design of the panels, and perhaps, to the actions of the operator.

E5: First ignition

A 5.1: Possible error of detection of potential ignition source (OPM).

A 5.2: Design of control mechanisms: spark arrestors and deluge system (DES)

A 5.3: Maintenance of the deluge system (OPM)

The first ignition may have been caused by several possible sources. It is difficult, if not impossible, to completely separate fuel lines from ignition sources. Electro-static sparks are a possibility; but it could also be a broken light fitting or other anomalies that could have been detected and fixed earlier. For electric motors, spark arrestors may have prevented ignition. An effective, explosion-resistant, and properly maintained deluge system may have prevented the fire from spreading in its initial phase.

E6, E7: Failure of gas detectors, fire protection (deluge) and emergency shutdown systems

A 6-7.1: Design of the Main Control Room (location of the detector module rack) (DES)

A 6-7.2: Failure of the control room operator to check the origin of first gas alarms from the detector module rack (OP)

A 6-7.3: Design of the low-gas alarm system (DES)

A 6-7.4: Design of the gas detection system: couplings to the electric power system (DES)

A 6-7.5: No automatic fire protection upon gas detection in west half of Module C (Pet. 4.7.5.3). (DES)

A 6-7.6: Lack of redundancy in the fire pumps' location (DES; OP)

A 6-7.7: Deluge system of limited effectiveness (DES)

A 6-7.8: Failure to upgrade some safety functions to requirements of Phase 1 production mode (DES; CONST; OP)

Prior to the initial explosion, gas alarms were received in the main control room; but due to the display of the signals' origins in the detector module rack, the operator did not check where they came from. High gas alarms were received shortly after, but it had

been determined earlier that the gas detection system was issuing false alerts (Pet. 5.14); there had been "a number of apparently spurious gas alarms on C centrifugal compressor. An opportunity was being awaited to change out the gas detectors" (Cullen, 3.124). The gas detection system, in any case, did not survive the first explosion for lack of electric power, which, at the same time, caused the inoperability of the pumps and of the deluge system. The electric systems failed catastrophically: first the main generator tripped after the initial explosion; then the production emergency generator failed to start, and the UPS system and the drilling emergency generators failed shortly after (Petrie, 9.2.1). Automatic pumps having been turned off, the system could not function in places where it existed. In many areas of the platform, and in particular in critical parts of the production modules, deluge systems did not even exist. In some areas, the deluge system started and quickly failed (riser from Tartan). In module C, the fire deluge system had experienced repeated clogging and was inoperable (Cullen, p.205). Primary automatic trip functions did not exist for operation in Phase 1. The system was primarily designed to operate safely in Phase 2 at pressures of 250 psi; when operating at higher pressures, the probability of a gas leak increased and some safety features (e.g., the automatic trip mechanism) may not have been fully adapted to accomodate the pressures of Phase 1.

E8, E9: Failure of the C/D and B/C fire walls

A 8-9.1: Design of fire walls with little resistance to blast pressures (DES); no blast control panels.

Fire walls and blast walls have different characteristics and blast walls may cause other problems by creating projectiles if and when they finally break. However, fire and blast containment systems on board Piper Alpha were generally insufficient (Cull.66; Pet.9.4.15). For example, the blowout (side) panels were ineffective.

E10, E11: Pipe rupture in module B and large oil leak

General problems of layout and separation:

A 10-11.1: Couplings in the design of the modules (insufficient isolation) (DES)

A 10-11.2: Couplings due to insufficient protection against fire propagation (DES)

A 10-11.3: Insufficient protection of critical equipment against blast projectiles (DES)

The propagation of the accident at this stage involves several kinds of couplings: tight space, and insufficient blast protection and fire protection. The space problem may be unavoidable in this part of the production system; it is all the more important to reinforce the fire and blast protection to prevent coupling problems.

E12, E13: Fire ball in Module B that spreads back into module C

A 12-13.1: Poor insulation against overpressures (DES)

The spreading of the fire at this point cannot yet be attributed to the malfunction of the fire fighting equipment (the succession of events was too fast) but rather to a design problem that made each module vulnerable to blasts in the others.

E14: Fire spread to fuel storage

A 14.1: Decision to store fuel above the production modules; spatial couplings (OP)

Storage of fuel above modules B and C introduced one more source of hazard that was avoidable.

E15: Failure of diesel power fire pumps

A 15.1: Poor design of the fire fighting system (DES); problems of location, redundancy, and protection of the pumps against fires and blast

A 15.2: Decision to turn off the automatic system to protect divers (OP)

Several factors contributed to the tragic loss of fire fighting capabilities. The automatic system had been turned off to protect divers from being sucked into the water inlet (there are, apparently, other ways to protect the divers). The diesel fire pumps were therefore on manual mode and were damaged in the first explosion. Even if they had been intact, they could not have been reached because the module was on fire. They

should have been located in places where they were less vulnerable to fires and blasts (and protected against them). The diesel-powered fire pumps (and the fire protection system in general) were thus poorly located and without sufficient redundancies elsewhere.

E16, E33, E39: Rupture of the risers from Tartan, then from MCP-01 and Claymore

A 16-33-39.1: No fireproofing of the riser connection (DES)

A 16-33-39.2: Vulnerability of the deluge system to blasts (DES)

The pool fire above modules B and C caused such a heat load that the riser from Tartan failed under the platform. There was no appropriate fire proofing to protect the riser, and the deluge system that could have prevented this went out. Later failures of risers from MCP-01 and Claymore were also caused by massive fire loads as the accident unfolded, and caused further explosions as production continued on these platforms.

E17: Jet fire under Piper Alpha

A 17.1: Physical linkages in the Piper-Tartan-Claymore network (DES; CONST)

A 17.2: Distributed decision making in the Piper-Tartan-Claymore network (OP)

A 17.3: Poor communication among the platforms and with the vessel Tharos (DES; OP)

A 17.4: Underestimation of the severity of the Piper situation on other platforms (OP)

A 17.5: To some extent: decision to continue production on Tartan (communication problems); insufficient procedures and enforcement of existing procedures) (DES; OP)

In this particular scenario, the decision to continue production on Tartan even though there were clear and visible signs of a severe condition on Piper (and even to increase the pressure as it was beginning to drop in order to maintain production) probably did not considerably worsen the situation on Piper Alpha given the pressures in the pipe line at the onset of the accident. The OIM on Tartan soon realized the

severity of the situation on Piper and ordered production to stop (Cull. 133). But on Claymore, the will to maintain pipeline pressure and optimism about the capabilities of containing the fire on Piper Alpha against signals to the contrary led the OIM to a severe error of judgment: the decision to continue production until an hour later followed by a fourth violent explosion at 23:18 with the rupture of the Claymore riser.

E18, E19: Immediate loss of electric power. Failure of emergency lighting

A 18-19.1: Decision to run the cable route through module D (DES)

A 18-19.2: Inadequate decoupling of the redundant power supplies (DES; OPM)

A 18-19.3: Insufficient inspection and maintenance of emergency generators (OPM)

Loss of electric power can be one of the most devastating accident initiators if there is not reliable redundancy in the system since many of the emergency features require electricity (this is true on offshore platforms as in nuclear power plants and many other engineered systems). As mentioned above, the redundant power systems all failed shortly. In this case, the cable routes were running through one of the most vulnerable of the production areas without adequate redundancy (Pet.4.3.6). Furthermore, after the main generator tripped, the emergency generator did not start. The drilling generator started, then failed. A few battery-activated systems functioned for a while. The emergency lighting functioned for a while, then failed.

E20: Loss of the control room

A 20.1: Bad location of the control room next to the production modules (DES)

A 20.2: Lack of redundancies in the control system (technical decapitation) (DES)

The location of the control room next to the production modules created failure dependencies such that an accident initiator (fire or blast) in these modules had a high probability of destroying the control room, where the accident could have been minimized by controlling the process. With loss of command and control and loss of electrical power, the system was technically decapitated. Lack of redundancies in the commands made it extremely difficult at that time to manually control the equipment.

E21: Failure of the public address system

A 21.1: Design of the public address system: insufficient redundancy for the loss of main electric power source (DES)

The public address system was entirely dependent on electricity: if there is no power, there is no sound. Couplings among the backups of the central electric power supply caused a failure of the public address system.

E22: Failure of the radio/telecom room

A 22.1: Bad location of the radio room (DES)

A 22.2: Lack of redundancies in the communication system (DES)

The location of the radio room on the east side of the platform (AAE) above the C module made it vulnerable to production accidents. Given the interdependencies among the different platforms in case of emergency, and the assumption that the OIM on Piper was to assume the role of on-scene commander (OSC) for the rescue, the loss of the radio room prevented critical exchanges of information with Tartan, Claymore, and the vessels in the vicinity (decapitation of all damage control operations).

E23: Loss of the OIM function

A 23.1: Decision to hire and promote the individual to the OIM position (OP)

A 23.2: Poor training for this kind of emergency (OP)

A 23.3: No organizational redundancy; disruption of the chain of command (OP)

Although the OIM was not killed at the onset of the accident, he panicked, appeared to be in a state of shock, and was incapable, from the beginning, of giving appropriate orders, and in particular, evacuation orders that could have saved many lives (Cull. p.163). Neither could he assume the OSC function, so that by the time the master of the Tharos decided to assume these functions and coordinate fire fighting from the fire boats, much time had been lost and the result was negligible. The OIM probably knew that the evacuation passages were blocked and that regular evacuation was impossible; he was perhaps incapable of thinking beyond procedures that could not

apply and of ordering an improvised evacuation. The technical decapitation of the system was therefore compounded by an organizational decapitation as no one took charge except the personalities that emerged as leaders under the circumstances.

E24, E25, E28, E29, E31: Fire and smoke spread throughout the platform

A 24-25-28-29-31.1: Layout decisions: insufficient physical separations (DES)

A 24-25-28-29-31.2: Equipment design decisions: insufficient fire proofing, insulation and smoke filters (DES)

A combination of lack of fire fighting capabilities and design decisions allowed the fire to propagate across modules and components, spreading to utility modules and escape routes, and the smoke to fill the living accomodations.

E32: Ineffectiveness of the Tharos in fighting the fire

A32.1: Delay in the decision of the Tharos master to take charge as OSC (OP)

A32.2: Failure of the Tharos fire fighting equipment (DES; OP)

The semi-submersible vessel Tharos was by chance in the vicinity of Piper Alpha at the time of the accident. It could have played a major role in fighting the fire and rescuing peronnel on board (by providing an external escape route), but eventually made little difference for several reasons. First, it was waiting for orders that never came from the OIM on Piper Alpha. By the time the master of the Tharos decided to take charge as OSC, it was too late to come close to Piper and the fire was too severe to be fought effectively from the outside. Second, the equipment on the Tharos malfunctioned because the fire fighting monitors were overloaded and non functional (Cullen).

E26, E30, E34, E36, E44: Casualties on board: escape and rescue of survivors

A 26-30-34-36-44.1: Poor design and planning of evacuation routes (lack of redundancies) (DES)

A 26-30-34-36-44.2: Failure of the OIM to give evacuation orders (OP)

A 26-30-34-36-44.3: No alternative official authority to incapacitated OIM (OP)

A 26-30-34-36-44.4: Individual initiatives to escape and jump off against previous information about survivability of jumping in the sea from more than 60 ft. (OP)

A 26-30-34-36-44.5: Poor training for evacuation: lack of knowledge of the platform layout and alternative escape routes (OP)

A 26-30-34-36-44.6: Failure to properly locate, install, and inspect emergency exit equipment, rafts and boats. Poor location of the life boats (and lack of redundancies when they are inaccessible) (DES; OPM)

A 26-30-34-36-44.7: Failure to inspect and maintain inflatable rafts (OPM)

A 26-30-34-36-44.8: Failure to provide, properly locate, and inspect individual protection equipment (smoke hoods, survivability suits, life jackets, etc.) (DES, OPM)

First, the location of the control centers and utility modules close to the production modules caused the immediate death of a certain number of key operators and personnel. Second, the poor location of living accomodations too close to the production modules and equipment allowed the smoke to fill the quarters and failed to provide a safe temporary refuge for the personnel. Third, the poor planning of the exits (lack of separation, redundancies and single-point passages) led to the early blockage of the planned evacuation routes and the inacessibility of the TEMPSCs (Totally enclosed, motor-propelled survival crafts). The OIM probably knew this, which may have contributed to his state of panic and his inability to function and give orders. There was chaos, no organized response, and no responsibility or authority (Cull. p.163). As in many emergency situations, leaders emerge, according to personalities, knowledge of the premises, and luck, but without planning and training in crisis response.

The personnel who followed the procedures and did not take the initiative to escape perished. The unavailability of smoke hoods in the living accomodations probably shortened the time that the personnel would have had otherwise to make escape decisions. Of those who tried, some found themselves trapped at the 68ft level and the 175 ft level, and took the risk of jumping from such heights. In some cases, they were not aware of the possibility of some passages to the 20 ft level which some drillers knew about (Cull. 158). At least one life raft could not be inflated (it had probably not

been inspected and maintained properly). Of the survivors rescued later, few were fully equiped to survive in the water and there were additional deaths by drowning that could have been avoided. (In fact, in winter time, many more would have died in the cold water.) A serious design problem was the lack of redundancies and dispersion of the life boats around the platform (Pet. 6.2) and the lack of appropriate access routes (there was a single access point). Of the 135 bodies recovered, 14 had died during escape, all others had died on board (and 2 in rescue operations).

E37, E38, E40, E41, E42, E43. Structural failures and collapse of the structure

A 37-38-40-41-42-43.1: Failure to account specifically for fire loads in the design of the structure (DES)

A 37-38-40-41-42-43.2: Decision to ignore early warning that the platform could not sustain severe fire loads for more than ten minutes (DES; OP)

Whereas jacket-type platforms are designed according to the wave loads that they may experience in their lifetime (e.g., the 100-year wave), the fire loads are not explicitly accounted for in the design of the structure itself (Gale and Bea, 1991). The slow collapse of the structure as the steel yielded under the prolonged and intense fire load may not have significantly increased the human losses, but the property damage was certainly greater than if the structure could have been saved. Occidental Petroleum management had been warned earlier that the platform could not survive prolonged exposure to a high-intensity fire. The warning, however, was ignored because the event was judged too unlikely to be taken seriously based on an error of reasoning (wrong assumption of independence in the successive failure events) (Cullen, p. 228).

4.2 Classification of the decisions and actions that contributed to the Piper Alpha accident

An accumulation of questionable decisions, gross errors, and errors of judgment of varying severity thus contributed to the Piper Alpha accident and its consequences. These decisions and actions occurred in the three phases of the lifetime of the structure:

design, construction and development over time, and operations both before and during the accident of July 6, 1988. Some were strategic decisions common to the oil industry at the time, others were more specific to operations of Piper Alpha and Occidental Petroleum; some were tactical decisions made on the spot. It is this accumulation of questionable decisions that led, in particular, to the technical and organizational decapitation of Piper Alpha at the onset of the accident.

The human errors, questionable decisions, and errors of judgment that have been identified above and contributed to the Piper Alpha accident can therefore be divided into four categories: (1) design decisions, (2) production and expansion decisions, (3) management of personnel, and (4) inspection, maintenance, and correction of detected problems. It should be noted that some of these decisions (e.g., design decisions) were considered acceptable at the time and were conform to the existing codes and the practice of the industry. It is these codes and common practices that are questioned below and need improvement.

4.2.1 Design decisions

Among the basic events of the Piper Alpha failure mode, a large number were directly influenced by design decisions that caused couplings and dependencies of three types: (1) direct linkage of component failures (i.e., public address, main electrical generators and their backups), (2) increased risk of fire propagation (e.g., from module B to module C, to control room and beyond), and (3) vulnerability of several components to the same event or load (common causes of failure, e.g., blasts). Finally, in other cases, some critical safety features, such as the life boats, had simply not received sufficient attention in the design and in maintenance operations.

°The general design of the network of platforms (Piper Alpha, Claymore, Tartan, MCPO-01) made them physically interdependent without providing sufficient management integration, both for production decisions that affected operations on other platforms, and for coherent and quick decisions in case of emergency.

°The final layout of Piper Alpha was deficient because of insufficient redundancies,

unnecessary complexity (e.g., storage of fuel on the deck), and excessive compactness. This final layout, which may not have been unusual in the industry at the time, was in part the result of un-preplanned additions of equipment. Mutual proximity produced critical spatial couplings such as: (1) no spatial separation of production modules and other modules, in particular living quarters; (2) inappropriate planning of escape routes (insufficient redundancies); (3) the life boats, life rafts, and other means of escape were grouped at one end of the platform; and (4) critical systems for emergencies (control room, radio room, electric generators, diesel pumps, etc) were so close to production modules as to be inoperative in crisis situations when they were critically needed.

° The design philosophy of emergency, protection, and safety systems was generally faulty. First, fatal failure dependencies and couplings made automatic shut down, alarm, public address, and other critical systems directly dependent on central electric power generation capability, without sufficient redundancies in this central source and reliable alternative supply for each emergency system. Furthermore, these backups were themselves coupled. Second, fire and blast protection was clearly insufficient, although protection against both is difficult to achieve (Cullen). Third, the design of fire protection systems (deluge systems, automatic response to gas alerts, etc.) implied strong couplings among failures of emergency systems (e.g., the manual and the automatic pumps). Fourth, the lack of redundancies in production equipment and safety equipment proved critical at the onset of the accident. Fifth, there were simple cases of deficiencies in the design of emergency equipment which did not work when needed: a warning system for gas leaks that produced too many false alarms and relied on readouts in the control room that proved difficult in times of crisis because of poor choice of layout, display, and color coding; or equipment such as life rafts that are not used in normal time and could not be inflated when needed.

°Finally, the platform was simply not designed for severe fire loads. Altogether, the system was capable of responding to minor fire emergencies, not to the severe fire conditions that developed during the accident. The structure itself was not designed to sustain high temperatures and direct fire loads for a long time. Safety was generally

considered on a small scale, but provisions for severe conditions such as a prolonged high-pressure gas fire were inadequate based on the assumption that they were simply too unlikely to be worth worrying about (Cull., p.228). Indeed, prevention of small and frequent accidents is, in the short run, more cost-effective. However, backing up judgments regarding rare and potentially catastrophic events generally requires serious risk analysis and cost-benefit analysis under uncertainty and clear criteria of how safe is safe enough. According to Lord Cullen "[Occidental management] adopted a superficial attitude to the assessment of the risk of major hazard" (Cullen, p. 3).

4.2.2 Production and expansion decisions

The design proposal which was presented to the United Kingdom Department of Energy in March 1974 was based on a peak production rate of 250,000 barrels of oil per day (Petrie, 3.1.6, 3.1.7); the living quarters were designed to accomodate 135 persons (Bechtel: Piper Production Platform, Project Profile). The platform was completed in 1976. It reached a peak production of about 320,000 barrels per day in 1979 (Oil and Gas Journal, 1988). By 1988, the production had declined to about 130,000 barrels of oil and 20 MMcfd of gas per day. Many modifications had been made to the platform, some of which included addition of equipement, for example, the Piper Gas Conservation project required by the U.K. government authorities, which was initiated in 1978 and commissioned in 1980: "To conserve the gas produced at Piper, which was being flared in considerable amounts as oil was being produced at rates in excess of 300,000 bpd, major modifications to the Piper platform were undertaken to retrofit gas separation processing and export facilities" (Bechtel: Piper Production Platform, Project Profile). Other modifications included the addition of a produced water facility in 1980, of supplementary living quarters, installation of oil lift pumps, etc. (Petrie, Annex B).

Although the structure itself was reinforced in 1979, the deck surface was fixed and the result of un-preplanned additions was an extremely packed space. Not only additional components were stacked, thus creating new couplings, but also, the record keeping of these additions was inadequate: it was not even clear what was on board

and where at the time of the accident (Bea, 1991). Some of these additions apparently interfered with the proper functioning of safety features: external reinforcements on module C, for example, prevented adequate functioning of the blast relief (Bea, 1991). At the end of this growth process, the situation on Piper Alpha was described by Bea (1991) as "fifteen pounds of potatoes in a five pound bag." The result was that safety features that may have been adequate in the beginning became insufficient for this new layout, with new couplings and higher risks of accident that may not have been realized (or sufficiently questioned) at the time when the additions were made. In particular, additional safety precautions should have been taken at the time of the shift to Phase 1 production in order to accomodate the greater risks due to higher pressures.

Also troublesome, although in the end probably without effect, were the decisions to continue production on the other platforms when there were clear signals that a serious accident was unfolding on Piper Alpha. On platform Tartan, at first, production was even increased to maintain line pressure before shutting down. Platform Claymore took more than one hour before responding and stopping production. The OIM on each platform was in charge of his own system. There seems to have been a lack of central command and control of the normal production process. Emergency procedures by which the Piper OIM could have communicated with the other platforms could not be activated because of loss of command authority and communication failures. However, in this case, once the accident started on Piper Alpha, even interruption of production on the other platforms would have made little or no difference since the gas was already in the line under pressure.

4.2.3 Management of personnel: hiring, screening, training, and promotion

There were not enough qualified and trained personnel on board at the time of the accident. Temporary promotions allowed fulfillment of critical functions by available people. Therefore, some less experienced (or even inexperienced) personnel, contract maintenance crews, operators, and production workers were allowed to run Piper Alpha at a time when high-level activity should have required special care, attention, and the

ability to recognize abnormal signs in order to diagnose and fix problems immediately.

The loss of the OIM function clearly led to a tragic increase in the number of casualties. The choice of personality fit to be captain of a ship is traditionally the result of a promotion process by which individuals are evaluated on the effectiveness of their actions in normal and emergency situations. As marine systems have become more sophisticated, crises are rarer, and training in crisis management becomes more crucial. Simple instructions about emergency procedures are insufficient because they may not be applicable in some circumstances. Thorough understanding and knowledge of the system (e.g., layout and passages), ability to reason under pressure and to respond to unforeseen situations are the result of appropriate screening and training. This training seems to have been inadequate in the case of Piper Alpha. Such training, however, represents an investment that assumes first that the organization recognizes the possibility of truly catastrophic situations, then that it properly estimates their probabilities.

4.2.4 Inspection and maintenance decisions

Inspection on Piper Alpha had been lacking in many areas, particularly in safety equipment. Life rafts, fire pumps, or emergency lighting do not seem to have received proper attention. Minimal response to inspection findings was apparently one of the factors that weakened redundant pumps A and B. The most critical maintenance problem was the failure of the permit-to-work system and the carelessness with which the PSV 504 was removed and replaced by a blind flange assembly without proper tagging thereby putting pump A out of service. The night shift was not informed of this situation and tried to restart this pump in which the initial leak seems to have started. The enquiry concluded that for a leak of the magnitude observed to develop, the assembly must have been only "finger tight". The assembly work was not inspected and therefore, the defect was not detected. Altogether, this maintenance failure was rooted in a history of short cuts, inexperience, and bypassed procedures (Cull., p.193-194).

5. ORGANIZATIONAL ROOTS OF DECISIONS SPECIFIC TO PIPER ALPHA

The decisions, human errors, and questionable (or bad) judgments that contributed to the Piper Alpha accident can be in turn systematically related to a certain number of organizational factors. Some of these factors are rooted in the characteristics of the oil company (culture, structure of the corporation, procedures and their rationale), others in specific features of the British oil industry and its relations to the Bristish government authorities (Carson, 1982).

Key organizational factors that are at the root of the decisions identified in the previous section are the following: (1) questionable judgement in the management of productivity versus safety, (2) flaws in the design philosophy and the design guidelines, (3) problems of personnel management, and (4) insufficient attention to maintenance and inspection. All of these involve questions of information (do the personnel have appropriate levels of knowledege? and do they receive appropriate information to take action in different cases?), incentives and rewards (what are people actually told to do? If they don't do it, what are the consequences for them? What are they actually rewarded for?), and resource constraints (time, money, and attention). As a result, problems accumulated, generated by an organizational structure that lacked redundancies, by procedures that allowed cutting corners, and by a culture that encouraged flirting with disaster[10]. Once again, the conditions described here may not have existed in July 1988 in other oil companies and may or may not exist at this time in particular oil companies.

5.1 The management of production versus safety

There is no golden rule for managing the productivity versus safety trade-off. The desirability of a particular safety measure is the result (1) of what the organization believes (and wants to know) about the effect of the feature on the system's safety, and (2) the risk attitude of the corporation. Decision analysis (e.g., Raiffa, 1968) is thus the tool best adapted to support such choices in a consistent and rational manner. The use of decision analysis relies on an explicit risk attitude. Responses from the public and the

legal system (either to hazardous conditions or to an accident) are generally meant to ensure that the risk attitude of the corporation does not clash with the values of society at large. Critical factors and potential risk management problems include the following.

5.1.1 Myopia in risk management and emphasis on small incidents

In some oil companies, the philosophy seems to be "production first" and the time horizon seems limited to the short term. These myopic views and the rarity of large accidents tend to focus attention on avoiding small (and frequent) safety problems that may disrupt production, create a visible record of incidents, and attract the attention of the insurance companies. The possibility of severe (and rare) accidents, however, is given insufficient attention because catastrophes are unlikely to occur on any particular watch. Yet, large accidents may involve multiple casualties, large sums of money, and enormous environmental costs. For example, as it will be discussed further, the design guidelines for fire protection are generally geared towards the control of minor incidents and are inadequate to protect the system from major events. If and when a large accident occurs, the tendency is to consider it a "freak event" that was unpredictable and simply should not have happened. Probabilities are sometimes used *a posteriori* to claim that the likelihood of the particular chain of events that led to a catastrophe was so small that the corporation was justified in ignoring its possibility. As discussed above, this result is often obtained by an accumulation of details in the story and by ignoring dependencies among events. When this happens, the lesson of the accident can be partially lost and the losses absorbed as "costs of doing business". The public, however, is now pressing for higher and higher punitive costs in order to make the costs of real disasters unbearable enough to force the industry to adopt a longer-term perspective. Because the costs proved so high, the Piper Alpha accident was an eye opener that simply could not be ignored.

5.1.2 A "reverse safety culture"

A safety culture is generally defined by a clear understanding of the system and its

safety features, a positive attitude towards safety measures, and an incentive system that encourages safety in operations (Weick, 1987). In an organization that rewards maximum production, operates most of the time in a rough and generally unforgiving environment, and faces a demanding world market, the culture is marked by formal and informal rewards for pushing the system to the limit of its capacity. Production increases sometimes occur with little understanding of how close one is or might be to the danger zone. When a platform operates above the level of flowrates for which it was designed, the high sustained production levels are a source of pride. The original design is modified and the system expanded, by "debottlenecking" and by adding components and links that allow still greater production levels[11].

However, pushing the envelope without disaster requires understanding the consequences. This is not the case (1) when operators, production engineers, and/or system designers are not aware of all the dependencies of a naturally complex system, (2) when under-trained and under-experienced people are allowed to run the operations, and (3) when negative experiences and stories of near-misses and incidents tend to be ignored and suppressed as they run counter to the general philosophy. The operators may not really want to know what could happen when expanding and increasing the demand and they may not want feedback from the people who have designed the system because such enquiry may bring the bad news that increasing the production level is dangerous or that the system may have to be shut down for retrofitting.

In such a cultural and economic environment, the star is thus the one who shows unflinching optimism and wins the battles of "us" (the production people) versus "them" (the safety inspectors, the government regulators, and others who tend to slow down production). At the time of the Piper Alpha accident, the system was not working at its peak of production but at a high pressure level that required additional precautions.

5.1.3 The role of government and safety regulations

Before the Piper Alpha accident, Carson (1982) had already pointed out that the

Bristish government, eager to benefit from the North Sea petroleum, had adopted a hands-off attitude compared, for example, to that of the Norwegian government where the tradition of regulation and inspection was generally much stronger. The result was a set of relatively loose and dispersed connections between the British oil industry and several regulatory authorities. The British government was very supportive of the petroleum industry for a variety of political and economic reasons, but in order to allow uninterrupted production, important safety issues may have been overlooked by inspection authorities[12]. Furthermore, in their guidelines, the approach of these governement agencies was to micromanage the specifics of design and procedures, removing, in effect, the responsibility for the resulting degree of safety from the operating oil companies as long as they complied with government specifications. This policy simplified the game for the offshore operators who succeeded if they could satisfy the "safety office". Everything being permitted unless explicitly forbidden, the emphasis was not on the actual level of safety achieved but on satisfying regulations without seriously considering the resulting risk. These regulations were often incomplete because the regulator cannot always keep up with developments and expansions in the production area. Therefore, this process could even stifle safety innovation itself.

During the Cullen investigation of the Piper Alpha accident (Cull, chap.16), this laissez-faire situation was compared to the much more stringent Norwegian approach to regulation. For cultural reasons described above, the concept of government regulation of oil and gas production has not always been welcome by a large segment of the oil industry, both in the U.K. and the U.S.[13]. Yet, it was pointed out after the Piper Alpha accident that the Norwegians had been more effective in regulating offshore safety and that, in the U.K., regulation had to change emphasis in its scope, and focus on the result (actual safety) rather than on the details (Salter in OOPPA, 1991). It was also argued that consolidating the regulatory bodies would allow the oil companies to deal with one single authority in a more consistent and effective manner. This, of course, implies that the companies themselves are willing to change their perspective, and manage both safety and production functions within more general regulatory requirements.

5.1.4 Separation versus integration of safety functions:

Among other things, the oil companies will face a problem of organizational structure: should the safety function be separated or should it be integrated into the production function? The creation of a strong safety office has often been recommended to organizations facing critical safety problems (Heimer, 1990) such as NASA after the Challenger accident. Advice in the literature varies. Many favor a strong safety function that can impose its views on production (e.g., Presidential Commission Report on the Challenger accident, 1986). Yet, experience with regulation in other industries shows that the same opposition between production and safety functions can exist inside as well as outside a corporation when it is in opposition to its regulators. Furthermore, because industries reward mostly the production stars, the safety division or office can become a convenient position to pigeon hole the less productive employees. This, in turn, further reduces the power and effectiveness of the safety function.

It seems, therefore, that separating safety and production is not the best strategy, and that safety must be an integral part of the production process. (In the same way for example, the manufacturing industry has discovered that inspection alone does not provide quality, but that quality must be the responsibility of everyone in the production line.) To that end, the incentive system has to be adapted to this goal, rewarding safety measures and punishing dangerous actions. Governments (in the U.K. as well as in the U.S.) may seek greater involvement, but the operators and the production personnel have to assume the primary responsibility for the safety of operations. The first step is to set reasonable production goals and objectives, and to allow for contingencies.

5.1.5 Economic constraints and profit centers

Making the production personnel responsible for safety requires that they receive appropriate resources, time, and margin of maneuver in production operations. Yet, the production sector of many integrated oil companies is pressured by corporate structuring of profit centers that separates production from refining operations (Bea, 1991). The profits of the oil business vary with the world price of petroleum and the

profits of production are directly linked to this external variable. In order to meet these goals, production operations have to adjust to these fluctuations. When the price of the barrel of oil decreases, the production sector tries to absorb these variations by decreasing its costs. The costs of research and the costs of non-immediate safety measures are often the first to be cut, sometimes at the expense of longer term financial results and at the risk of a disaster. Refinery operations, by constrast, enjoy a greater stability because accounting methods isolate them to some extent from the world price of the raw materials and measures their results as a function of the selling price and the volume of the demand.

This arbitrary definition of profit centers, as if they were separate entities and independent businesses, is therefore at the fundamental root of some questionable practices of cost reduction in the production sector, in areas that directly affect the safety of operations such as inspection, maintenance, and personnel management.

5.2 Flaws in the design philosophy

5.2.1 Lack of redundancies, catastrophic couplings, and risk of decapitation

In organizations that cultivate the production-first, penny-pinching philosophy and the perception that severe accidents are too rare to be seriously planned for, the view is generally held that redundancies must simply satisfy regulations and are there mainly to keep production going. As it was mentioned earlier, backup requirements are specific enough for topside operations; but for emergency and safety features, the requirements are much less specific and a philosophy of minimum compliance can be particularly disastrous. Even if the number of backups is specified, the safety gains will depend, in the end, on the robustness of the equipement and the couplings among potential failures. For instance, if the backups of the power supply are tightly coupled, the loss of electrical generation at the onset of a disaster implies that there may be no power to activate the safety features such as the automatic shut down, the public address, and the general alarm systems that are designed for these very circumstances. Finally, lack of redundancies in the life boats (and their location) implies that, if they become

inaccessible, there is no escape alternative but to jump into the sea.

Redundancies are particularly critical in the functions of command and control whose loss ("decapitation") may prevent the proper functioning of emergency equipment and procedures. It takes special attention to anticipate and explicitly address decapitation problems because the linkages that may occur under severe circumstances are not always obvious in times of normal operations. Decapitation can occur both at the technical and at the organizational level. The system must be able to function when parts of it are isolated, when centers of command and control are out, and when the formal head of the organization either is dead or has lost control of the situation.

Among the most critical subsystems are electric power production equipment and electric transmission cables, because electric power is needed to activate most of the emergency shut down, fire fighting, and evacuation operations. Therefore, power generation must be located in a "safe" (i.e., electrically unclassified) area, electric cables must be protected, and reliable alternative emergency (battery activated) power sources must be provided for each of the critical systems in case of failure of the central supply. And of course, once installed, these redundancies must be regularly inspected and maintained even if they are seldom called upon.

Proper design of safety redundancies often requires formal analysis. A probabilistic system analysis in critical situations allows rational decisions regarding the number, the site, and the level of design of the redundancies needed. An example of functional and fault tree analysis of safety features is presented in Figure 7 and Figure 8 for the design of an emergency water pumps system. The trade-off between the cost of additional redundancies and added safety should be addressed by a decision analysis based on the costs of each alternative, its effect on system safety, and the risk attitude (utility function) of the corporation.

Avoiding the risk of organizational decapitation requires that the OIM be in a relatively safe location most of the time, and that in the event of his death or incapacitation, the problem is recognized, others are informed, and an alternative chain of command is set up to operate quickly under emergency conditions. Furthermore, a

platform network has to be able to operate safely in situations of distributed decision making, especially in the case of a catastrophic fire.

An analysis of couplings requires identification (1) of direct causal relations between subsystems' failures, (2) of the external events that can constitute common causes of failure (e.g., a fire that destroys all the redundancies in the fire pumps), and (3) of the possibilities of propagation of the effects of these external events (fires and blasts). Analysis of causal relations among failures and of common causes of failures can be done using event trees and fault trees. Analysis of fire propagation requires the use of a stochastic process (e.g., a Markov model) as described in Section 6. The results for a particular class of failure modes can then be included in a general risk analysis model to check that fixing one problem does not create another one elsewhere.

5.2.2 Flaws in some of the guidelines for topside layout

The layout of the topside is generally guided by area-classification concepts whose goal is to separate the flammable vapors expected under normal production conditions from the sources of ignition, in particular, electrical equipment (W. Gale, 1991). In the U.S., areas where vapors are normally expected are classified as Division 1 where explosion-resistant equipment is required. Areas where vapors are present only under abnormal conditions are classified as Division 2 where equipment is required to be vapor-tight or non-sparking. The rest is unclassified: no vapors in ignitable concentrations are assumed to be present and there may be some ignition sources. For example, in the U.S., areas including ignition sources other than electric (such as an open flame) are unclassified, which does not mean that fire hazards do not exist there.

The objective of such guidelines is to prevent the start of a fire under normal conditions of operations and to protect the system from minor incidents. The guidelines do not require decoupling of production modules and other modules such as accomodations, the control room, or the radio/telecom room that are critical to survivability (at least there was no such requirement when Piper Alpha was constructed). For the control room, however, electrical classification determines the

design criteria: physical separation and vapor-tight separations are required (i.e., unpierced bulkhead wall) but there are no specific requirements against fires and blasts. The control room can be located anywhere, even in a process area. All that is required in its design is to bring in fresh air. Therefore, it was not inconsistent with these guidelines to locate the control room above or even within the production modules nor to put the living accomodations next to them (although, as a rule, one generally tries to separate process and accomodations with utilities in-between). Insulation for fires and blasts is costly, separation requires more space, and there is great congestion on a typical platform. It is thus easy to see why under guidelines that allow for such tight couplings, the compressor module can be placed next to (or even below) the living accomodations.

5.2.3 Later modifications and un-preplanned growth

Platform production systems generally evolve through the life of the platform. Multiple modifications are often made to the original design, for example, to increase capacity by removing bottlenecks, or to correct fundamental flaws such as an undersized pump. The increase in production capacity often increases mechanical stress in the system, the velocity and pressure of the flows, and therefore piping erosion from sand and other particles.

As in most engineering systems, problems can occur when there is insufficient feedback to the original designer to check that these modifications do not create couplings and hazards that may not be directly visible, or that the production capacity and the pressures after modification are compatible with the design characteristics and maintenance schedule. The actual criterion often appears to be trial and error: does the system seem able to sustain an increase of load? In the past, there was generally no attempt to check by analytical reasoning, before a real-life test, how these changes can affect the probabilities of external or internal accident initiators, loads, and transients for the expanded system, and its ability to respond. Also, un-preplanned growth can bring with it, for the same functions, a whole new set of complexities and weaknesses that

would not have occured if these functions had been planned for in the initial design phase. This tinkering with the system on one hand allows for imaginative innovations, but on the other hand, can prove fatal unless there is a clear understanding of the system's characteristics in its final state. One of the benefits of developing a probabilistic risk analysis model for each system at the design stage and of using it as a "living document", updated and modified as the system evolves and responds, is to be able to check the effects of successive modifications.

5.2.4 Lack of specific fire criteria in the design of the structure

Fire risk is accounted for, in the design of the topside, by trying to prevent (as described above) the co-existence of vapors and ignition sources, and by providing means of fire fighting[14]. Fire protection thus relies on fire pumps, water spray and deluge systems, resistive coatings, and steel fire-proofing. Fire loads, however, are not directly accounted for in the design of the structure (Gale and Bea, 1991) in the way wave loads are considered. There is no attempt to assess the annual probabilities of different fire loads to which the structure might be subjected and to adjust the design parameters to provide thermal robustness, i.e., inherent fire resistance. The same approach that is taken for wave loads could be used to characterize the uncertainties about the future fire loads (as a function of the system design and mode of operation) and the uncertainties about the system's capacity to sustain these loads. A decision analysis based on marginal costs of increased safety and on the risk attitude of the corporation can allow consistent treatment of the multiple loads to which the structure may be subjected. Therefore, such an analysis permits placing safety dollars where they can be most efficient at risk reduction.

Setting fire criteria, however, may be more complex than setting criteria for waves because the occurrences of fires is not a stable external environmental factor. Therefore, there is more uncertainty for a particular platform and more variability among platforms in the estimation of the future fire loads, even though there may be an abundance of statistics about platform fires in the industry as a whole.

5.3 Problems of personnel management

5.3.1 Too few people in time of high activity: temporary promotions

As it was pointed out earlier, the system of temporary promotion allowed Occidental-Aberdeen to fully utilize available personnel to replace off-duty employees, and to avoid having to bring on board higher ranking individuals. This temporary promotion system, however, did not guarantee that appropriate experience was available when needed. Furthermore, there seemed to be inadequate redundancy in human functions, especially in the supervision of the production and maintenance crews. At the time of the Piper Alpha accident, the number of people who were operating the system in Phase 1 was the minimum required and appears to have been insufficient. In many cases, operators, when overburdened by several functions, choose to attend to the most pressing problems. As with many other organizational issues, these problems are rooted in the way strategies to cut production (and personnel) costs are implemented.

5.3.2 Failure to learn

The culture of any industry that discourages internal disclosure and communication of bad news leads to ignoring small incidents and near-misses as long as they do not result in full scale accidents. In such an environment, the fact that a severe accident did not occur seems to be sufficient proof that the system works and that "an inch is as good as a mile". The possibility that several minor problems could occur at the same time does not seem to be considered. Consequently, small, isolated incidents are seldom discussed openly since they would constitute a black mark for the personnel involved. Therefore, the same problems are likely to recur elsewhere.

In fact, even when an accident does occur, appropriate measures to avoid its recurrence are not necessarily taken. The permit-to-work system, for example, had failed before, in particular on Piper Alpha in 1987, when a worker was killed in an accident in the A module (Cullen, p.197). The accident was the result of a breakdown of communications in the permit-to-work system and an error in the shift handovers. In spite of memos and warnings to other OIMs, the lesson was not learned on Piper Alpha itself.

5.4 Insufficient attention to maintenance and inspection

5.4.1 Deficiencies of the permit-to-work system

The permit-to-work system is described in great detail in the Cullen report (Chapter 11). Its deficiencies may not be in the formal procedures themselves but in their practical applications, generally because of insufficient resources (including personnel and time), training, discipline, and verification. For example, because the culture did not discourage shortcuts, multiple jobs could be performed on a single permit. Also, even in the written procedure, there is no mention of "tagging and locking off of isolation valves which have been closed or opened as part of making equipment safe to work upon" (Cull., p. 196). The communication problem that occurred on Piper Alpha seemed to be a general one: "unless he was involved himself in suspending a permit, a night-shift lead production operator would not know which permits had been suspended and accordingly what equipment had been isolated for maintenance purposes." (Cull. pp.192-193). Again, the people who performed the work did not seem to understand clearly (or to be willing to communicate) dependencies and couplings among components, and how maintenance of one affected the others. The question simply does not seem to have been addressed.

It may be that the formal procedures are too complicated for the workers who perform the job and that they consider it necessary to take short cuts to alleviate the load. If that is the case, the procedures themselves should be streamlined and simplified so as to remove the source of the problem.

5.4.2 Minimum response to inspections: safety features as extra baggage

If and when the primary concern is to maintain the flow and to reduce short-term costs, the objective is to do minimum maintenance that would interrupt production, just enough to keep producing and to set records of duration between turnarounds, when the system must be shut down for maintenance and cleaning. In this perspective, safety issues are seldom part of the picture. As pointed out earlier, the safety inspections performed by government authorities of the United Kingdom as well as corporate

personnel were generally minimal or ineffective because inspectors sometimes looked the other way in order to permit uninterrupted production[15].

In addition, the custom seems to have been minimum response to this minimum inspection. Defects were corrected where they were found but there was often no attempt to find out if the same defects existed elsewhere, much less to seek to correct them. This problem was in part a problem of communication, but mostly one of priorities and incentives. Altogether, inspection and maintenance of safety features seem to have been low on the priority list, at least prior to the loss of Piper Alpha (Carson, 1982). If these features seem like extra baggage even at the design stage, they are the most likely to be neglected when resources are scarce, personnel are reduced to a minimum, and everyone's attention is focused on maintaining (or increasing) production.

6. BENEFITS OF RISK REDUCTION MEASURES

For most of the basic events of the Piper Alpha accident sequence, there are possible technical improvements; for example, addition of a redundancy, or reinforcement of a component against blasts and fires. In the same way, for many of the decisions and actions associated with these basic events, there are procedures that may decrease the probabilities of errors by forbidding certain practices, or by rewarding workers for discovering and fixing problems. Often, but not always, the costs are those of reducing or interrupting production. Finally, for many of the organizational features described above, there are modifications that may improve individual decisions and reduce the risks of failures and accidents, for example, a change in the internal accounting system or the systematic use of a risk analysis model (1) to record all changes and (2) to check their effects on the overall safety of the platform.

Many of these possible improvements can be derived directly from the description of the problem as presented in the previous sections and have been listed in the Cullen report (Cull. Recommendations). The recent Conference on Offshore Operations Post Piper Alpha (OOPPA, 1991) proposed a certain number of improvements. Technical improvements involve, for example, new materials for fire and blast protection (Hu),

safer accommodation including a temporary safe refuge (Godfrey), and better fire detection devices (Watkins). Organizational improvements include better regulation (Daneuberg and Schneider) and corporate management (Dawson). Using the decision analysis framework and a coarse estimate of the costs and benefits of each alternative, one can set priorities and choose among these measures. Most of these modifications affect several components or phases of operations; therefore, they may influence the probability of several failure modes. System analysis and risk analysis involving fault trees, event trees, and stochastic processes (e.g., Besse et al. in OOPPA91; Fitzgerald and Grant, ibid.) can help capture these dependencies. The risk analysis model, however, must be extended if one wants to include (1) decisions and actions and (2) organizational features in the assessment of the benefits of improving risk management.

6.1. The extended risk analysis model

Computation of the benefits of various risk reduction measures requires a general risk analysis model, i.e., a model linking initiating events to a probability distribution for the losses per time unit. The benefits are then calculated as the differences of the probabilities of accident scenarios (and/or by the differences of the expected values of the annual losses) with and without the proposed measures.

The probabilities of decisions and actions can be modified either directly, for example, by forbidding certain practices, or indirectly by modification of the organization, for instance, by changing the reward structure. In turn these measures thus affect the occurrences of the failure modes. Assessment of their benefits requires conditioning the basic probabilities of the risk analysis model on these decisions and actions, and if applicable, conditioning these decisions and actions on relevant characteristics of the organization.

Let $\{in_i\}$ be the set of possible initiating events (e.g., fires, blasts, wave loads, earthquakes, boat collisions), $\{fist_m\}$ the set of possible final states (characterized for instance by a Boolean vector such as [0,1,1,0,0....,1] indicating whether the different components are functioning or have failed), and $\{loss_k\}$ a partition of the set of possible

loss levels. The probability distribution $p(loss_k)$ for all k thus represents a discretization of the distribution of the annual losses. If the initiating events are described by their annual probabilities of occurrence $p(in_i)$, the risk analysis model that characterizes the annual losses can be written:

$$p(loss_k) = \sum_i \sum_m p(in_i) \times p(fist_m|in_i) \times p(loss_k|fist_m) \qquad \text{for all k.} \qquad \text{Eq.1}$$

The probabilities $p(fist_m|in_i)$ (final states conditional on initiating events) are the results of event tree and fault tree analyses that indicate which components can be affected by the considered initiating event and its further developments, and which failure mode (or accident sequence) can occur. The probability $p(loss_k|fist_m)$ is the result of the consequence model linking the human and economic losses to the final state of the system. The losses are generally represented by a vector of two elements (casualties and property damage).

To include in this model the effect of relevant decisions and actions $\{A_n\}$ requires conditioning the probabilities of Equation 1 to the elements of the set $\{A_n\}$ (Note that the A_n's can affect separately all the elements of the previous equation). The A_n's are structured so that they constitue an exhaustive, mutually exclusive set of classes of decisions or actions that affect the platform in the different phases of its lifetime. Each A_n is described by a vector whose elements represent the outcomes of these classes of decisions or actions. Equation 1 can thus be written:

$$p(loss_k) = \sum_i \sum_m \sum_n p(A_n) \times p(in_i|A_n) \times p(fist_m|in_i, A_n) \times p(loss_k|fist_m, A_n) \qquad \text{Eq.2}$$

Finally, the effects of different organizational factors $\{O_h\}$ on the risk are assessed by computing their effects on the probability of decisions and actions which, in turn, affect the probability of the possible accident sequences. The O_h's thus affect the elements of Equation 1 only to the extent that they affect the probabilities of the

corresponding A_n's. The probability of the different loss levels given a state O_h of the organization is thus:

$$p(loss_k|O_h) = \sum_i \sum_m \sum_n p(A_n|O_h) \times p(in_i|A_n) \times p(fist_m|in_i, A_n) \times p(loss_k|fist_m, A_n) \qquad \text{Eq.3}$$

The results of technical improvements (insulation, decouplings, redundancies, etc.) are measured directly in Equation 1 by their effects on the probabilities of initiating events (e.g., the corresponding decrease of the probability of fire), on the probabilities of the final system states (e.g., the decrease in the probability of fire propagation among components), and on the loss function (e.g., an increase in the probability of success of evacuation operations). The overall result is a reduction of the annual probability of different levels of losses, and therefore, of the expected value of the annual losses.

The results of organizational improvements (e.g., incentives for safety) are measured in Equations 3 by their effects on the probabilities of different actions and decision outcomes and consequently, on the overall loss levels. For example, a decision to decrease temporarily the production level because of excessive vibrations decreases the probability of pipe rupture (and therefore, of the initiating event: leak followed by fire and explosions). A decision to improve maintenance operations may decrease both the probability of an initial fire and the probability that it propagates once it starts. A decision to have on board six experienced operators instead of five relatively inexperienced ones increases the probability that an initiating incident is quickly discovered and fixed, therefore, for instance, decreases the probability of propagation to other modules if a fire occurs, and may decrease the probability of severe human losses even if several modules are destroyed.

Finally, for many of the organizational features described above, one can consider a certain number of modifications that reduce the risk of failures and accidents by reducing the probability of dangerous decisions and actions and consequently, the probability of the basic events of the failure modes. These benefits sometimes occur at the cost of reducing or interrupting production. For instance, increased inspection and

maintenance, decreased pressure in the system (therefore, reduction of the rate at which sand and other particles erode the pipes), all imply a lower production level in the short term. The effects of these organizational modifications can be measured in the model above by their modification of the probabilities of the decisions and actions that lead to the basic events of one or more failure modes. Many of these possible improvements can be derived directly from the description of the problems that led to the Piper Alpha accident and have been listed in the Cullen report (Cullen, Recommendations). Most of these modifications affect several components or phases of operations, therefore, they may influence the probabilities of several failure modes. A complete system analysis (possibly at a high level of aggregation) may be needed to capture these dependencies.

6.2 Reduction of the risk of loss of life in fires on board platforms

To illustrate the general model above, consider the problem of assessing the benefits of reducing the risk of losses in fires on board a platform by improving the system of emergency water pumps. For the initiating event in_i = "fire", further specifications are needed: (1) where it started (location noted loc_l) and (2) at what level of initial severity (noted sev_j). The analysis is then done in several steps:

* Logical analysis of the functions involved and fault tree analysis.

* Probabilistic analysis of the different failure modes for the top event: "failure of emergency pumping".

* Computation of the probability of fire start and propagation to the location of the pumps and their accesses, using a Markov model. (The final system's state is described by the vectors $fist_m$. The probability computed here is that of the $fist_m$'s in which the element corresponding to the emergency fire pumps indicates that they do not function.)

* Assessment of the benefits (risk reduction) of several types of measures (e.g., addition of a second manual redundancy, or improvement of the protection of the pumps against the effects of fires and blasts) by computing the contribution of the pumps to the overall level of losses in fires.

6.2.1 Event tree and fault tree analysis

The annual probability of the level of losses k is obtained by summing the joint probability of losses k, fire (initial location and severity), and final system states.

$$p(loss_k) = \sum_m \sum_l \sum_j p(fire) x p(loc_l|fire) \times p(sev_j|fire, loc_l) \times p(fist_m|fire, loc_l, sev_j) \times p(loss_k|fist_m)$$

fire initial state — fire propagation — final losses

Eq.4

The vectors $fist_m$ represent the possible final system states and the loss of the pumps may be one element of each $fist_m$. Therefore, a key element of the probability $p(fist_m|fire, loc_l, sev_j)$ is the probability of failure of the fire pumps. It can be analyzed by the simplified functional diagram (Henley and Kumamoto, 1981) shown in Figure 7. The function "water feed" is needed for both manual and automatic functions. The automatic pump requires electric power (i.e., that the power supply and electric cables are both functioning) and that the electric pump itself functions. The manual pump requires that an operator is available, that the access has not been blocked, and that the pump itself functions. (It is assumed here that the manual pump is a manually-started diesel pump.)

The fault tree corresponding to the top event T = "the water pumps do not function" is represented in Figure 8. Each failure event is noted by a Boolean variable X, and X is equal to 1 if the corresponding element does not function. Using the notations of Figure 7, the Boolean polynomial corresponding to this fault tree is:

$$T = W + (E + C + EP) \times (A + O + MP) \qquad \text{Eq.5}$$

Expansion of this polynomial yields the ten failure modes of the pumps:

$$T = W + ExA + CxA + EPxA + ExO + CxO + EPxO + ExMP + CxMP + EPxMP \qquad \text{Eq.6}$$

The probability of failure of the pumping function is thus:

$$p(T) = p(W) + p(E) \times p(A|E) + p(C) \times p(A|C) + p(EP) \times p(A|EP) + p(E) \times p(O|E) + p(C) \times p(O|C) + p(EP) \times p(O|EP) + p(E) \times p(MP|E) + p(C) \times p(MP|C) + p(EP) \times p(MP|EP) - \Sigma\, p(\text{two failure modes at a time}) + \Sigma\, p(\text{three failure modes}) \ldots \text{etc.} \quad \text{Eq.7}$$

Given the strong dependencies introduced by the possibility of accident initiators such as fires, the probabilities that two or more failure modes occur at the same time can be high. Therefore, in Equation 7, these terms must be explicitly computed. An example of two failure modes at a time is the conjunction: E x O x EP x A.

Fire is one of the "common causes of failure" that can affect the probabilities of all ten failure modes. The probability of losing the fire pumping function in a fire (event F) depends on the location l of the fire start and on the severity j of the initial fire. If one restricts the top event T to the loss of emergency pumping in a fire, Equation 7 becomes:

$$p(T) = p(F) \times p(T|F)$$

$$= p(F) \times \sum_{l} \sum_{j} [p(W|F, loc_l, sev_j) + p(E|F, loc_l, sev_j) \times p(A|F, E, loc_l, sev_j) + \ldots\ldots] \quad \text{Eq.8}$$

6.2.2 Markov analysis of fire development

Fault tree (and to some extent, event tree) analyses are static ones. They do not allow computation of the evolution over time of a phenomenon such as system deterioration or fire propagation. To do so requires a stochastic process analysis, the result of which provides the probabilities of the different states after t time units. Consider, for example, one particular failure mode of T: CxA, i.e., "Access routes are blocked by the fire" (therefore the manual pump cannot be started) AND "Electric cables are destroyed by the fire" (therefore, the electric pump does not work). Assume that the cables and the access routes are located in close proximity. Assume also, for simplicity of illustration, that the fire can start only in one particular location (Module 1), and in one of two levels of intensity (low intensity: severity 1; high intensity: severity 2). Finally,

assume that the fire has to reach location 2 (Module 2, close to the emergency pumps) and the higher level of intensity (severity 2), for example, to break through a fire wall before it can propagate to Module 3 where the emergency pumps are located. The probabilities of the different states of the subsystem Cables AND Access after t time units can be computed using the Markov chain described in Figure 9.

In Figure 9, C represents the state of the electric cables (C0: no damage, C1 minor damage by fire but still functioning, C2: failure due to fire) and A represents the state of the access to the manual pump (i.e., the space that must be crossed to reach the pump from other locations). In the same way: A0 means that the fire has not reached the access, A1 that the pump can still be reached but that fire and smoke are beginning to invade the space, and A2 that the pumps are inaccessible. The initial states of the cables and the access to the pumps while they are still undamaged but as the fire starts and propagates (C0-A0) have been grouped for clarity in Figure 9. The final state C2-A2 represents the failure mode CxA of the water pumps.

This Markov chain has 12 states numbered from 1 to 12 by column in Figure 9 (state 1: C0-A0, location 1, severity 1; ...; state 5: C0-A1; ...; state7: C1-A0; ...; state 12: C2-A2). It is assumed here that the fire always grows and damages the two components C and A continuously (i.e., without jumps in severity levels). Human intervention is not modeled here explicitly (see Appendix for an example of several growth rates corresponding to different phases of fire fighting). The probabilities of transition among states depend on fire fighting activities and on the availability of water (i.e., whether or not the other failure modes of the emergency pumps have occurred before CxA). Once the fire has reached Module 3 (states 5 to 12), the severity of the fire is represented only indirectly by its effects on the cables and the access to the pump.

The initial vector P(0) represents the probabilities of the initial severity levels given that a fire starts in Module 1.

$$P(0) = [p0(1), p0(2), 0, ..., 0] \qquad \text{Eq. 9}$$

Let Π be the transition matrix corresponding to this system; π_{ij} is the probability of transition from state i to state j per time unit (e.g., 1 mn). The probability that the system is in each of the 12 states after t time units is given by the vector P(t) which is the product of the initial vector P(0) and the transition matrix to the power t (Hillier and Lieberman, 1967):

$$P(t) = P(0) \times \Pi^t \qquad \text{Eq. 10}$$

The probability that the failure mode C2-A2 has occurred before t or at time t is the twelfth element of this vector P(t) noted $P_{12}(t)$. One can then obtain the probability distribution of the time to failure of the water pumps through this particular failure mode. Similar models can be developed for the other failure modes involving fire propagation.

6.2.3 Benefits of safety measures

This analysis (and similar ones for the other nine failure modes, and possibly for some conjunctions of failure modes) permits the assessment of the benefits of a certain number of measures aimed at reducing the probability that the fire pumps are unavailable in a fire. Examples of such measures include:

* Design: Isolation of the fire pumps (better layout or reinforced fire protection of the pumps area) -> Effect: to decrease the probability of transition between initial states C0-A0 and any of the other states.

* Design: Decoupling, given a fire, of the access to the manual pumps and the electric cables: -> Effect: to decrease the corresponding probabilities of transition between Ci-Aj and Ci+1-Aj+1 (e.g., C0-A0 to C1-A1).

* Operations: Procedures forbidding closing the water inlet (protection of the divers through other means): -> Effect: to decrease the probability of failure mode W.

* Operations: Human redundancy in the operation of the manual pumps (several individuals can access and operate the pumps) -> Effect: to decrease the probabilities of failure modes ExO, EPxO, and CxO which involve an operator.

* Operations: Change in the policy allowing less experienced personnel to operate

the platform: -> Effect: to decrease the probability that a fire starts, the probability that the fire, given that it starts, reaches Module 2 and Module 3 (where the emergency pumps are located), and the probability that no operator is available in the case where the automatic pumps do not function. In the model presented above for the failure mode CxA, these are the probability of fire p(F), the conditional probability $P_2(0)$ that the fire starts at a high intensity level, and the probabilities π_{ij} which characterize transition to higher damage or fire intensity states.

* Operations: Improvement of the maintenance procedure (more thorough or more frequent) that decrease the probability of leaks in pumps and valves: -> Effect: to decrease the probability of fire p(F) and the probability that the fire starts at a high level of intensity $p_2(0)$ if it does.

An overall evaluation of the benefits of measures aimed at decreasing the probability of losing water pumps in a fire must thus be done in the following way:

1. Assessment of the contribution of fires and blasts to the overall probability of platform failure.
2. Contribution of the failure of emergency pumps to the the probability of losing the platform given that a fire starts.
3. Contribution of each of the failure modes to the probability of failure of the emergency pump system.
4. Computation of the reduction of the probabilities of these failure modes as a function of the reduction of specific initial or transition probabilities such as those identified above.

Several types of improvements such as layout modifications, fire protection, and other measures aimed at decoupling the different parts of the system have multiple benefits because they reduce the probabilities of several failure modes. Improvements of the inspection and maintenance procedures allow adapting interventions to the loads and deterioration rate of each component. The choice of maintenance on schedule or on demand can be supported by a decision analysis (Paté-Cornell et al., 1987).

7. CONCLUSIONS

Many of the events that led to the Piper Alpha accident were rooted in the culture, the structure, and the procedures of Occidental Petroleum, some of which are common to large segments of the oil and gas industry and to other industries as well. At the heart of the problem was a philosophy of production first and a production situation that was inappropriate for the personnel's experience. Successive additions to the system had been made without sufficient feedback and understanding of their effects on the safety of operations. Because of the method of assessment of the internal financial results of the different segments of some integrated oil companies, it is the production part of the corporation that often finds itself under economic pressures. Measures that are then taken to save money in the short term have sometimes led to understaffed facilities and less experienced, overworked operators. Because they must attend to immediate problems, these operators are often unable to focus specifically on accident prevention, which often does not seem to have been at the forefront of the corporation's concerns in any case. For a long time, government regulations have been fought by the oil industry (fearing interference and loss of control). At the time of the Piper Alpha accident, the lack of coordination of dispersed regulatory authorities and the interests of the British government in an accelerated oil production contributed to the isufficient attention given to safety features and procedures on board the platforms. The maintenance error that eventually led to the initial leak was the result of inexperience, poor maintenance procedures, and deficient learning mechanisms.

Several kinds of improvements can be envisioned to reduce the probability of a future accident of the Piper Alpha type and of other classes of accident sharing with Piper Alpha some common technical or organizational roots. Probabilistic Risk Analysis and its extensions can be used to assess the benefits of these improvements. In general, there is a clear need for a change of some design guidelines and adoption of severe accident criteria. Technical measures that involve the design include: fire protection of the structure itself, improvement of the layout (decoupling of the modules), and improvement of fire protection of the equipment. In addition, improvement of the

inspection and maintenance procedures, personnel safety and evacuation procedures, and better coordination and communications among platforms in a network should reduce the risk locally. Yet, nothing will change fundamentally unless the oil company itself decides to promote a safety culture, to alleviate the production pressures under dangerous circumstances, and to provide consistent incentives for accident prevention.

8. FOOTNOTES

1. Occidental management had been warned by Elmslie Consultancy Services and by Mr Wottge (production engineer) that a prolonged high pressure gas fire would have grave consequences for the platform and its personnel (Cull., p.227); but it had been concluded at a subsequent meeting that "[the probability of the event] was so low that it was considered that it would not happen" (Cullen, 1990, p. 228).

2. There may be some uncertainty, however, about the details of the exact sequence. If needed, the Bayesian framework can be used to assess the probabilities of the different possibilities, i.e., their probabilities conditional on the known elements of the accident scenario.

3. The "final" state of a subsystem refers here to the state of this subsystem that determined the ultimate losses (i.e., the end of its useful life), for example, failure or no failure, rather than its chronologically final state at the bottom of the sea.

4. In the U.S., a recent report of the National Academy of Sciences recommends to the Mineral Management Services to issue guidelines regarding personnel as well as equipment.

5. This is not true, however, when the additional redundant element creates the danger of an added common cause of failure.This was the case, for example, of the auxiliary power units of the space shuttle: the addition of a third redundant element on one hand decreased the probability of unavailability of the APU system but, on the other hand, increased the probability of hydrazine release, which constituted an additional common cause of failure for other subsystems. The net result of a third redundancy was a net decrease of the system's safety (Garrick, 1988).

6. A tightly coupled organization, however, can also be a source of reliability to the extent that someone is clearly in charge, that there is a common purpose, and that supervision and feedback are available when needed (Roberts, 1990).

7. Other factors such as environmental damage and deterioration of public image are relevant to a loss estimation. Both are more difficult to quantify than the direct costs.

8. This model, however, does not include the case in which the fire dies by itself without fire fighting before full destruction of the system.

9. Such a model can become extremely large. The difficulty is in choosing a manageable model structure

and an appropriate level of aggregation given a large potential number of ignition sources, of physical components, and of fire severity levels.

10. For example, the temptation to shut down gas alarms and deluge systems. Such tendencies can be traced back to a clear definition of success as the ability to meet production and financial goals, and to the painful process of feedback by which goal reductions are considered and "negative excusers" re-assigned (Bea, 1991). At the time of the accident, a certain number of deluge nozzles were blocked in module C where such problems had occurred first in February then in May 1988 but had not been fixed yet (Cullen, p. 205).

11. The process of increasing production and "debottlenecking" the system to permit higher levels of activity starts with financial pressures from the board of directors. Goals are then set by the President or Vice-president of production, with the advice of production engineers. Finally, a sequence of tactical decisions are made regarding the technical steps needed to achieve the goals (Pet. 4.2.2). For Piper Alpha, it was mostly the production engineers and production operators close to the site (in this case, Aberdeen) who were in charge of the reservoir and equipment "debottlenecking" (Bea, 1991).

12. Carson (1982) writes of the situation in the British zone of the North Sea at the end of the seventies: "Indeed, according to the safety manager for one well-known oil company, the inspectors' approach actually created safety problems because of its cursoriness and lack of attention to the detail of more mundane issues. As a result, he contended, the incentive to improve this aspect of offshore safety was not being backed up, and a lot of the effort put into making the installation 'shipshape' appeared to be wasted." (p.241).

13. This situation is evolving in the United States, where the petroleum industry and the Coast Guard have been working together for two years on revisions of OCS regulations. There are two major reasons why industries involving hazardous products (and, in particular, the best-managed segments of these industries) end up welcoming safety regulation: one is that regulation sets standards for the least-well managed among them, where accidents are more likely and imply costs and image deterioration for the whole industry; the other is the hope that compliance with requirements will protect them legally.

14. Beyond design issues, fire safety also involves fire training, securing, and evacuation.

15. Carson (1982) discusses thirteen cases of serious safety violations of the North Sea oil industry that reached the Bristish court system and concludes: "Suffice it to say here that the evidence on prosecution once again supports the view that tolerance of violation has been institutionalized at a comparatively high level. The enforcement of safety regulations has thus far been dominated by an administrative structure which, for whatever reason, developed a distinctively low-profile approach to the application of legal sanctions against offenders" (Carson, p.251).

9. REFERENCES

Bea R. G.: Personal Communications, 1991.

Bea R. G. and W. E. Gale: "Structural Design For Fires on Offshore Platforms" Presentation to the NAOE Industrial Liaison Program Conference, University of California, Berkeley, 1990.

Carson, W. G. The Other Price of Britain's Oil: Safety and Control in the North Sea. Rutgers University Press, New Brunswick, New Jersey, 1982.

Cullen, The Hon Lord The Public Inquiery into the Piper Alpha Disaster, Vol. one and two, Report to Parliament by the Secretary of State for Energy by Command of Her Majesty, Nov. 1990.

Gale W. E. : Personal Communications, 1991.

Garrick, B. J. Quantitative Risk Assessment and the Space Program. Risk Analysis Seminar Series, Department of Industrial Engineering, Stanford, California, March, 1988.

Heimer, C. Social Structure, Psychology, and the Estimation of Risk. Annual Review of Sociology, Vol. 14, pp. 491-519, 1988.

Henley, E.J. and H. Kumamoto. Reliability Engineering and Risk Assessment. Prentice Hall Inc., Englewood Cliffs, NJ, 1981. Cambridge University Press, Cambridge, U.K., 1981.

Hillier, F. S. and G. J. Lieberman. Introduction to Operations Research, Holden-Day, 1967.

Oil and Gas Journal, "Explosion, fire heavily damage N. Sea platform, July 11, 1988.

Paté-Cornell, M. E. "Fire Risks In Oil Refineries: Economic Analysis of Camera Monitoring", Risk Analysis, Vol. 5, No. 4, pp. 277-288, 1984.

Paté-Cornell, M.E., H.L. Lee and G. Tagaras, "Warnings of Malfunctions: The Decision to Inspect and Maintain Production Processes on Schedule or on Demand," Management Science, Vol. 33, No. 10, October 1987, pp. 1277-1290.

Paté-Cornell, M. E. and R. G. Bea. "Organizational Aspects of Reliability Management: Design, Construction, and Operation of Offshore Platforms". Research Report No.

89-1, Department of Industrial Engineering and Engineering Management, Stanford University, Stanford California, 1989.

Paté-Cornell, M. E. Organizational Aspects of Engineering System Reliability: the Case of Offshore Platforms, Science, pp. 1210-1217, November 30, 1990.

Petrie, J. R.: "Piper Alpha Technical Investigation Interim Report", Department of Energy, Petroleum Engineering Division, London England, 1988.

Perrow, C. Normal Accidents, Basic Books, New York, 1984.

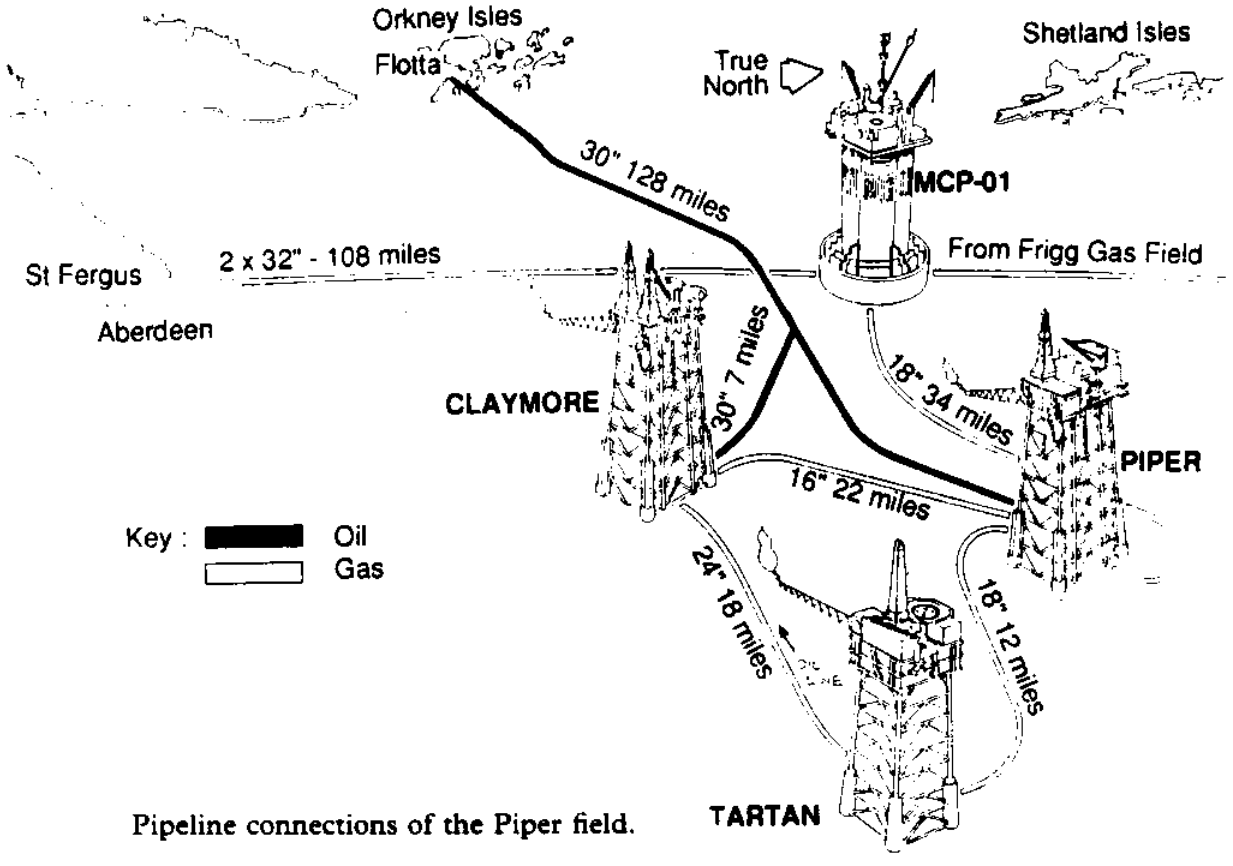
Presidential Commission on the Space Shuttle Challenger Accident. Washington D.C. June, 1986.

Raiffa, H. Decision Analysis, Addison-Wesley, 1968.

Roberts, K. H. "Some Characteristics of High-Reliability Organizations", Organization Science, Vol. 1, No. 2, pp. 1-17, 1990.

The Institute of Marine Engineers: "Offshore Operations Post Piper Alpha", Proceedings of the February 1991 Conference, London, England, 1991.

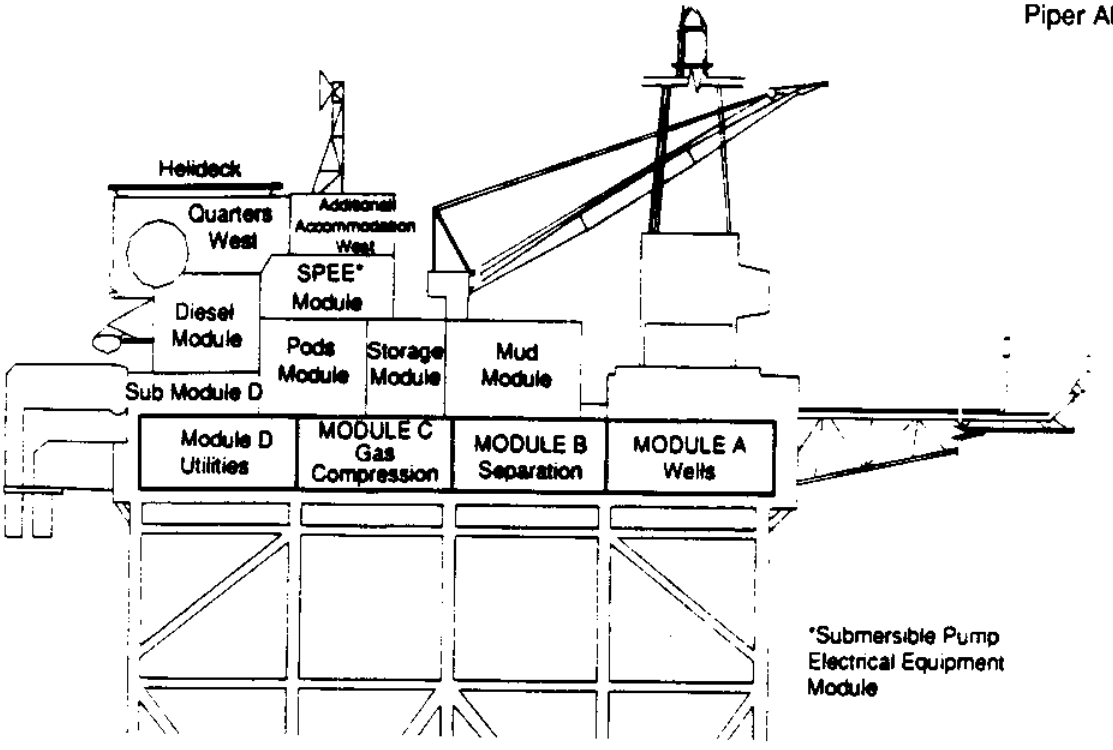
Weick, K.E. "Organizational Culture as a Source of High Reliability", California Management Review, Winter, 1987.



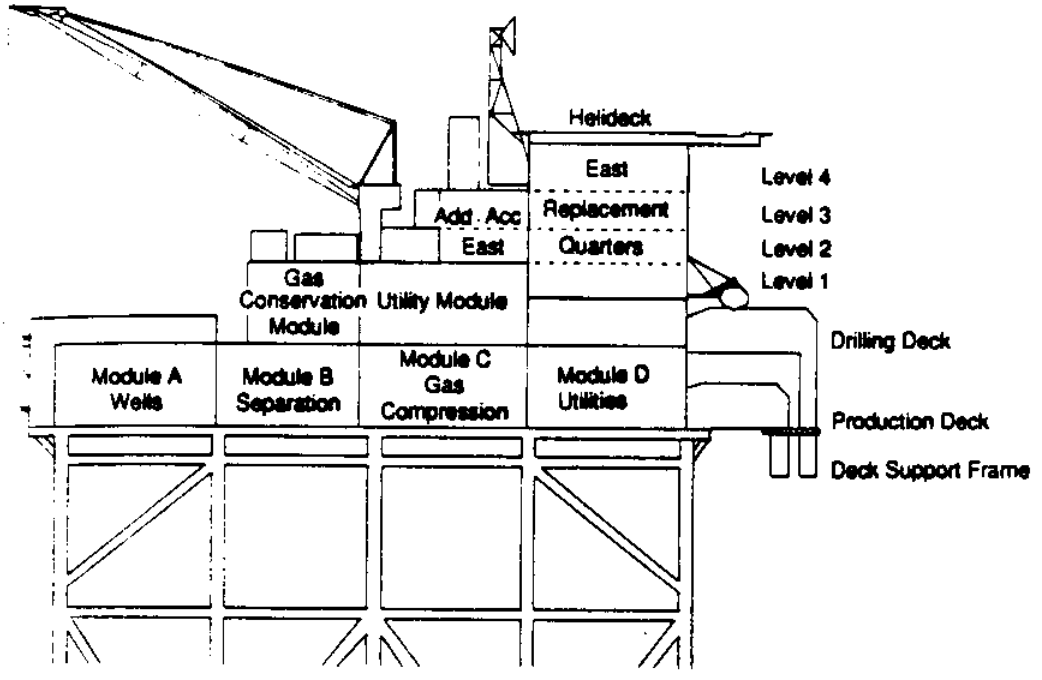
Pipeline connections of the Piper field.

Figure 1: The platform network: Piper Alpha, Claymore, Tartan, MCP-01

Source: Cullen Report, 1990



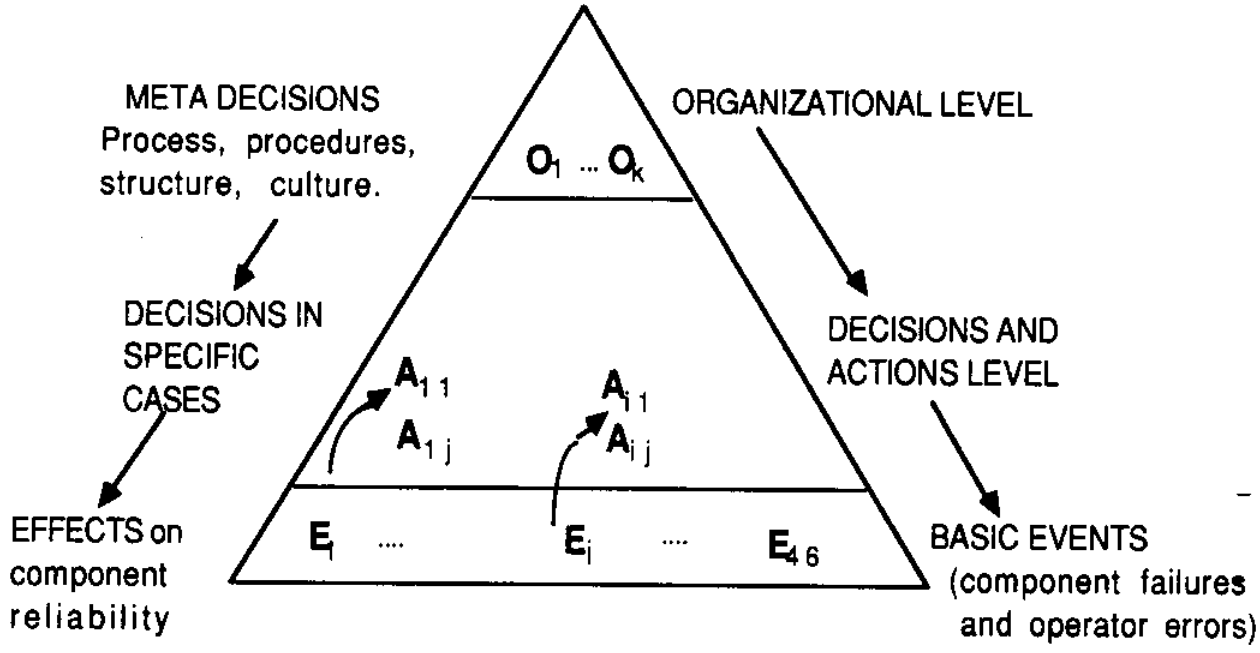
The Piper Alpha platform: west elevation (simplified).



The Piper Alpha platform: east elevation (simplified).

Figure 2: The layout of Piper Alpha

Source: Cullen Report, 1990



Legend:

E_i: basic events of the Piper Alpha accident sequence;

A_{ij}: decisions and actions that influenced the probability of event E_i;

O_k: organizational factors that influenced the A_{ij}s.

Figure 3: Hierarchy of root causes of system failures:
Management decisions, human errors, and component failures.

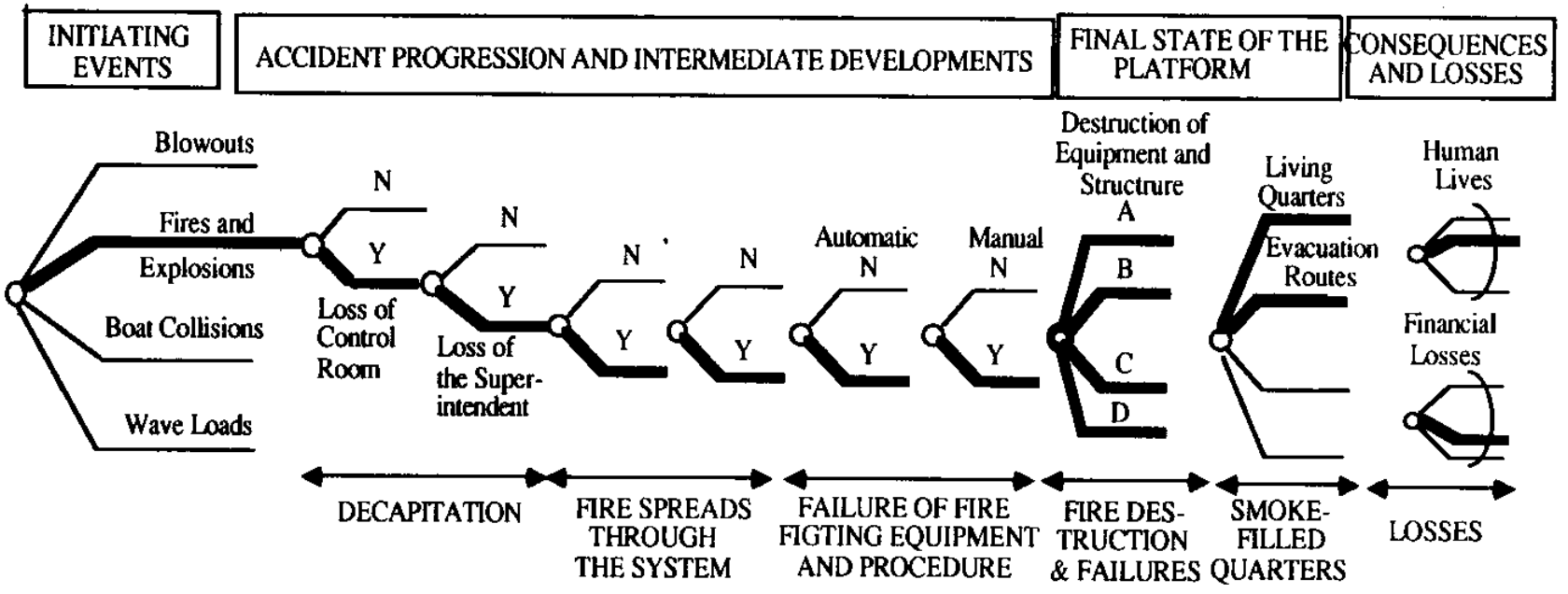


Figure 4: Structure of an event tree for a risk analysis for an offshore platform; identification of the Piper Alpha main accident sequence

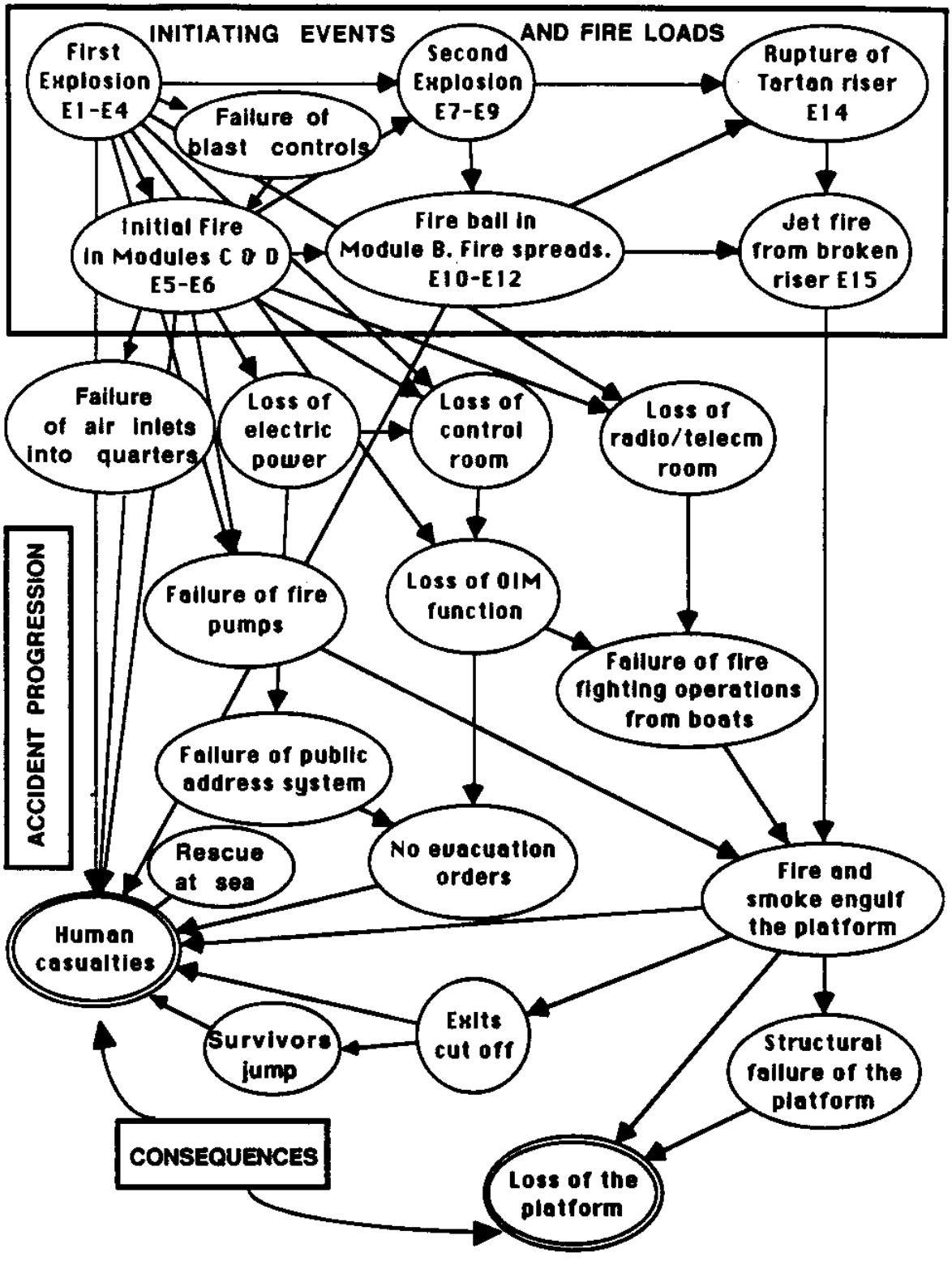


Figure 5 : Event dependencies in the Piper Alpha Accident Scenario
(Influence diagram representation)

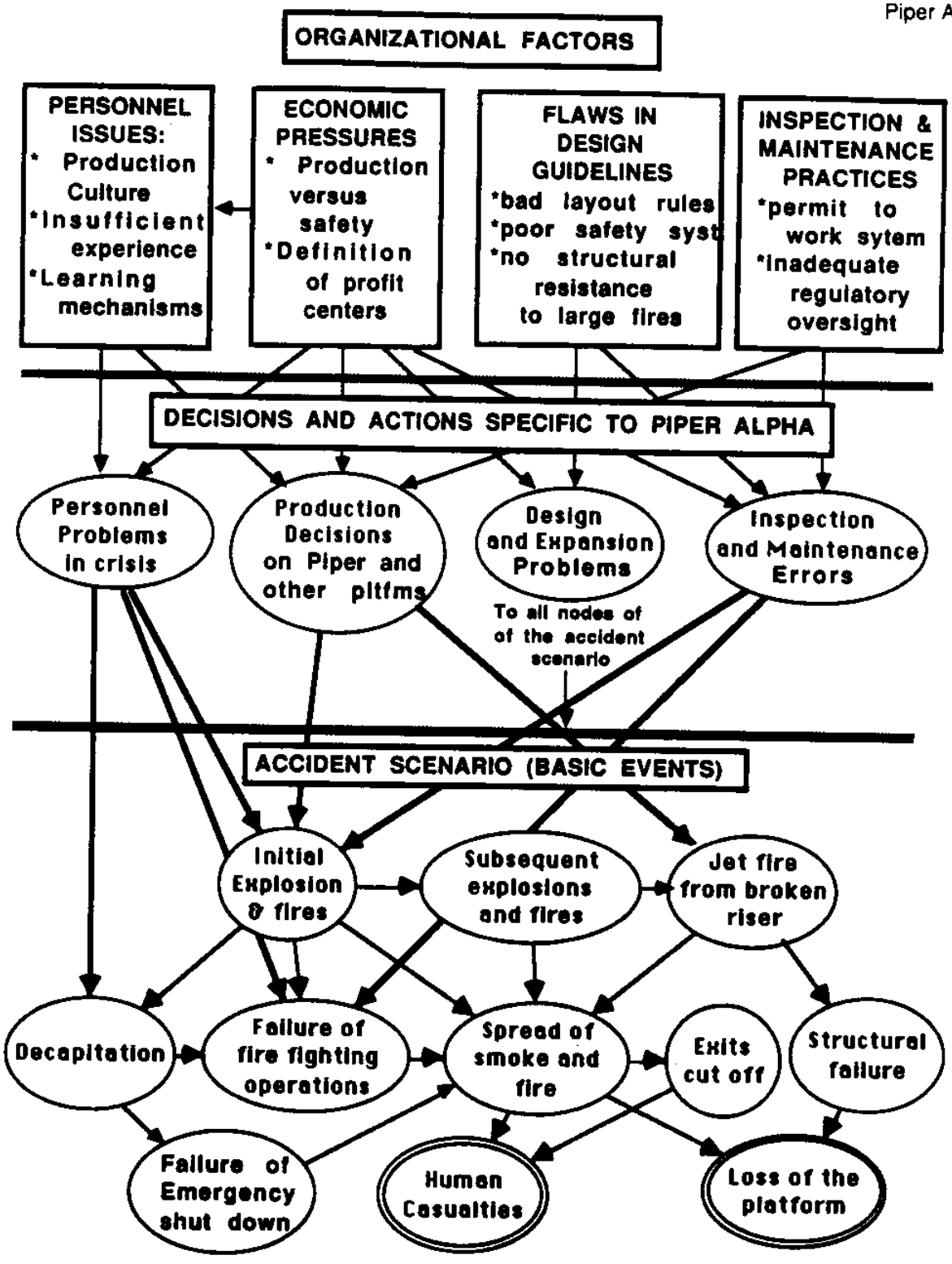
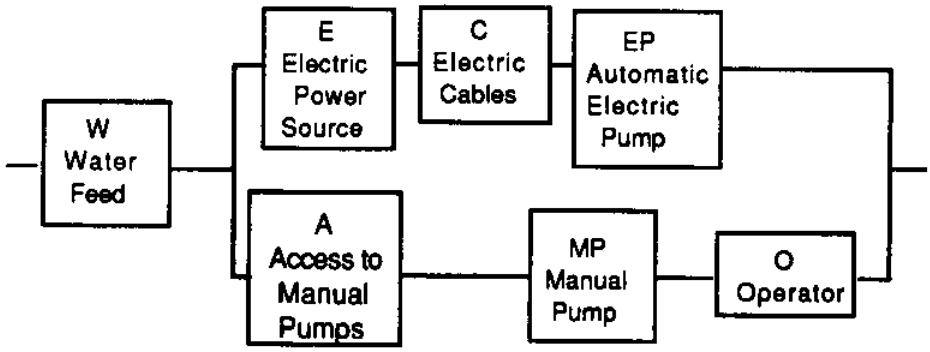


Figure 6 : Dependencies among basic events of the accident scenarios, decisions and actions specific to Piper Alpha, and organizational factors

(Influence diagram representation; the lower part is a simplified version of Figure 5)



Note: It is assumed here that the manual pump is a manually-operated diesel pump

Figure 7: Functional diagram for the emergency water pumps

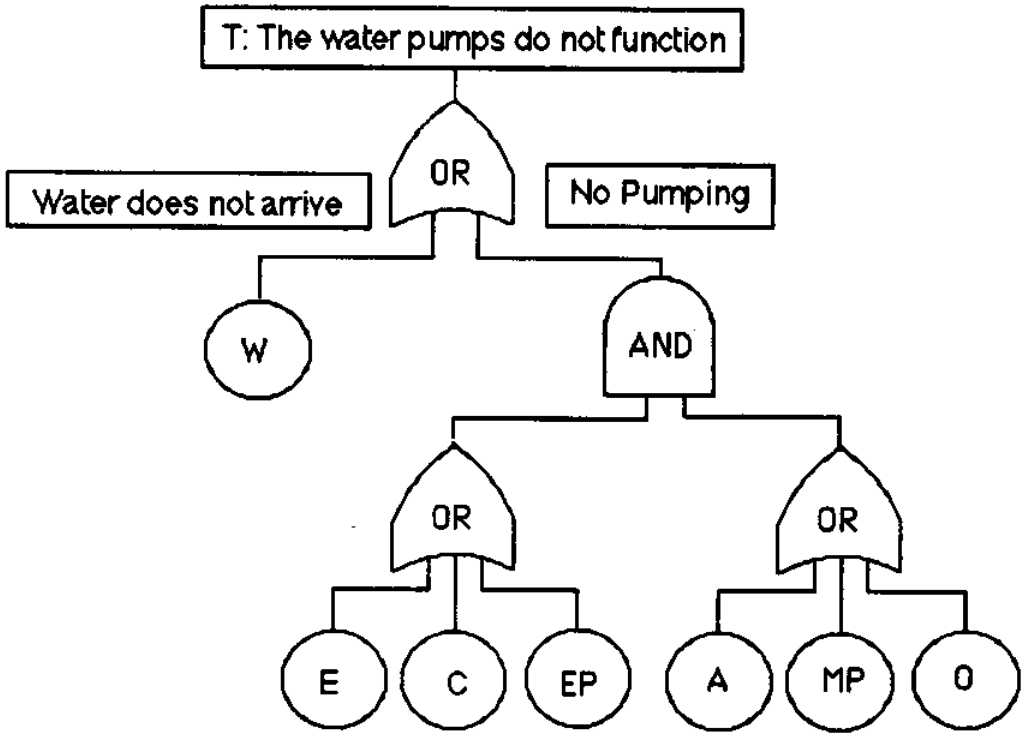
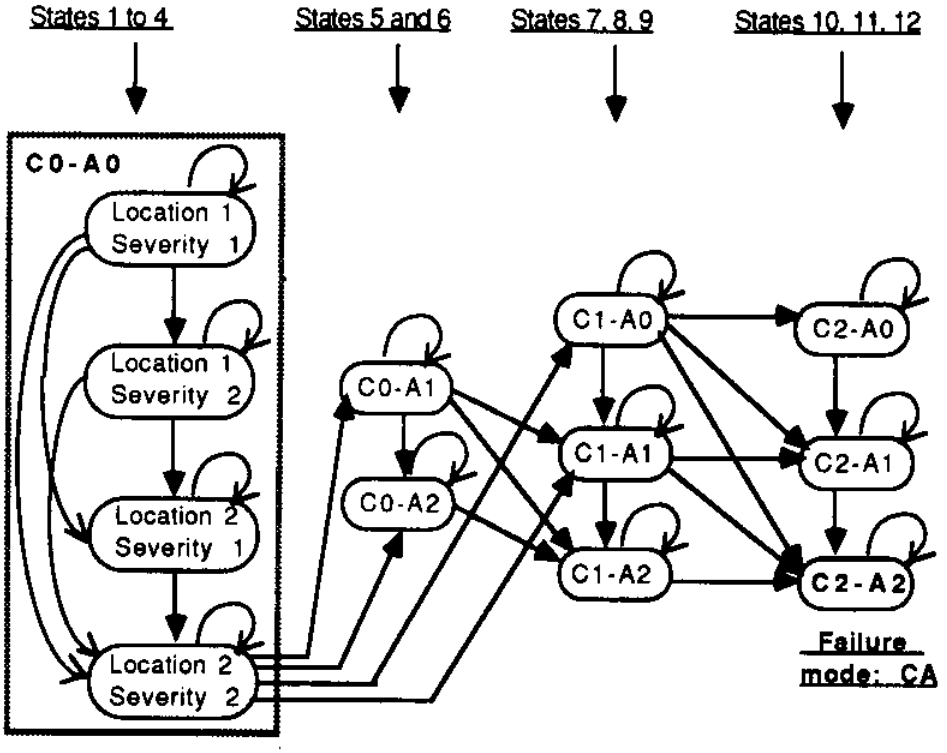


Figure 8: Fault tree for the top event "the water pumps do not function"



Legend: location i, severity j refer to the characteristics of the initial fire and of fire propagation.
Ci-Aj represent the state of the access (A) and the cables (C). Index 0: intact; index1: minor fire damage but still functioning; index 2: damaged by fire, failure state.

Figure 9: Markov diagram and transition among states for the subsystem: access to the manual pump(s) (A) and electric cables (C) feeding the electric pump(s)

10. APPENDIX

Fire risks in Oil Refineries: Economic Analysis of Camera Monitoring

M. Elisabeth Paté-Cornell

Risk Analysis, Vol. 5, No. 4, pp. 277-288.

Risk Analysis, Vol. 5, No. 4, 1985

Fire Risks in Oil Refineries: Economic Analysis of Camera Monitoring

M. Elisabeth Paté-Cornell[1]

Received July 31, 1984; revised May 10, 1985

A probabilistic method is presented to evaluate the economic value of fire monitoring by closed circuit TV camera in petroleum refineries. The proposed model is restricted to the analysis of risk reduction in an area where fires can be caused either by pump failure or by failure of valves and lines. The benefits come from reducing the time during which the fire grows undetected. Fire growth and expected values of losses are analyzed by a Markov model that includes five phases: (1) active undetected growth, (2) detection, (3) fire growth at the beginning of the firemen's intervention, (4) fire control, and (5) fire extinction. The results (e.g., the expected net present value of the investment) show that the proposed monitoring investment is attractive for an illustrative example.

KEY WORDS: Fire; risk assessment; Markov model; warning systems; cost-benefit analysis; petroleum refineries; camera monitoring.

1. INTRODUCTION

The American Petroleum Institute reported fire-related losses averaging $114 million per year for the period 1976 to 1980, with a high value of $316 million in 1980.[1,2,3,4,5] Of these losses, an average of $69 million, or 60%, occurred in oil refineries. Table I shows these results and the corresponding average loss per oil refinery.

Efforts are constantly being made to decrease this risk to life and property.[6] One method of mitigating fire losses is through early detection of fires, which reduces the risk of fire spreading. In particular, monitoring by closed circuit TV cameras (fixed or sweeping) allows the operator in the control room to immediately notify the fire department. It is often difficult, however, for the Fire Protection Staff to justify this investment because, whereas global statistics on fire losses exist, the statistical data are seldom sufficient for the particular spot in which the device is to be located.

What is proposed here is a method of *cost-benefit analysis under uncertainty* using probabilistic risk assessment of different levels of annual fire losses in a given area with and without the proposed camera. The assumption is that only financial losses occur, and the possibility of human death or injury was not considered here. As an illustration, the costs and the benefits of a closed circuit TV camera were evaluated for a chosen sensitive zone of the refinery where fires can be caused by the failure of a pump or a valve or a line. This model can be used to show the company management how such a protective investment compares with other protective and productive alternatives. The results include a present net value of cash flow, an internal rate of return, and a benefit-cost ratio corresponding to expected values of benefits and costs. It is understood that, if appropriate, other risk attitudes can be introduced by a nonlinear utility function.

[1]Associate Professor, Department of Industrial Engineering, Stanford University, Stanford, California 94305.

0272-4332/85/1200-0277$04.50/1

Table I. American Petroleum Institute's Fire Related Losses (See Refs. 1–5)

Year	Total fire losses (million $)	Refinery fire losses (million $)	Fraction of losses occurring in refineries	Number of refineries	Yearly ave. loss per oil refinery $
1980	316.0	187.8	59%	—	—
1979	111.0	79.1	71%	166	476,000
1978	34.8	20.5	59%	153	134,000
1977	64.0	40.0	62%	124	323,000
1976	45.4	17.8	39%	133	134,000

The basic method is a Markov modelling of the fire growth, detection, and extinction with and without the camera. This study is one particular application of a more general theory of warning systems.[7] The general model included the possibility of Type I and Type II errors: Type I errors correspond to a situation where the event occurs but the signal is missed, and Type II errors are false alerts. In the case of camera monitoring, however, there is virtually no possibility of false alert (Type II error). The focus here is on the consequences of Type I errors, or rather Type I *delays*. The operator in the control room may fail to notice the fire on the television screen for a certain time. The probability distribution assumed for this delay determines the extent of fire-spread, and, therefore, the additional losses due to Type I errors.

It would be prohibitively expensive to place the whole refinery under camera monitoring. The first question is, therefore, to identify places where the camera would be most effective. With the help of the personnel of Standard Oil of California and the Richmond Chevron Refinery, prime locations for fire starts were identified as follows:

- the tanks;
- the fire boxes;
- areas of concentration of pumps, valves, and lines.

It was decided to focus on the third type of location. For a given area, the problem is to evaluate, for example, a 360° sweeping camera whose field of monitoring can be reduced by blind spots. In the zone actually monitored, it is assumed that fires can be caused either by pump failure, or by failure of valves and lines. For one fire, one computes the expected value of losses under current monitoring. One then introduces the probability distribution of the annual number of fires of each of the two types occurring in the whole refinery, and the probability that, conditional on the occurrence of a fire somewhere in the refinery, it actually happens in the monitored area. This allows computation of the expected value of losses in both types of fires in the monitored area, given the present monitoring situation. This assessment is repeated, assuming monitoring by the proposed system, to obtain by difference the expected value of the annual benefits of camera monitoring for the considered spot. Figure 1 shows a block-diagram description of this procedure. The complete results include an assessment of the annualized costs of monitoring (first costs, plus costs of operations and maintenance) and various financial indicators of the investment performance.

The analysis is done using Bayesian probabilities, based both on statistics (e.g., annual fire losses in oil refineries) and on experts' judgments (e.g., probability of the detection of a fire of given size per time unit). This work is generic and is not based on the case of a specific refinery; the emphasis is on the development of the methodology rather than on the numerical results themselves. A Pascal computer code can be found in the original report[8] along with intermediate results showing the time evolution of fire losses from the beginning until extinction for the considered illustrative case.

2. MODELING OF FIRE GROWTH

State transition models of fire growth have been used in the past to model the physical spreading of fires. Ling and Williamson[9] for example, have developed a model of fire-spread in a room in which the states of the system were defined as the successive ignition of different elements and pieces of furniture.

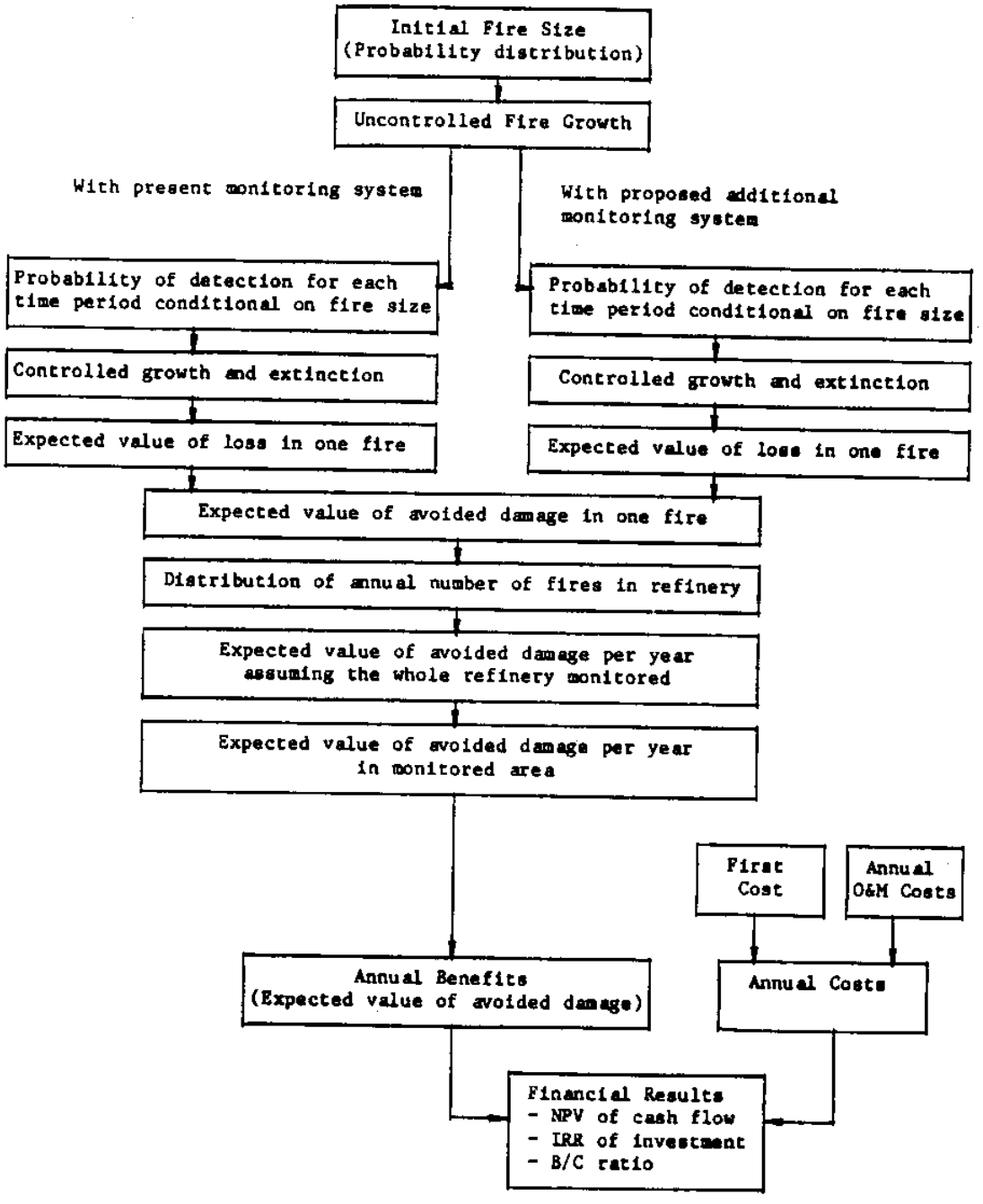


Fig. 1. Analysis of costs and expected benefits (block diagram).

In the case of fires in petroleum refineries, the same could have been done, but it would have been an extraordinarily complex task. As the results of this model are financial quantities, it appeared more direct and simple to define the system states as the amount of dollar losses in the fire at a given time.

The choice of a Markov model that relies on a given probability of transition from one fire size to a larger one gives reasonable results, although more refined growth models could be designed to account for some memory in the system. The process that was considered is the following:

- The fire starts in one of three possible sizes (dollar amount of losses).
- The fire may grow unattended and undetected for a certain number of time periods, with given probability of transition from state to state.
- The fire may be detected at each time period, with a probability that depends on its size.
- Once a fire is detected, it takes a certain (fixed) number of periods for the firemen to intervene. Initially, this delay was estimated at 2 min. Meanwhile the fire keeps growing at the same rate as an undetected fire.
- Once the firemen start fighting the fire, it still grows, but at a slower rate than before.
- At each time period, the fire may be brought under control with a probability that depends on the size that it has reached. The intensity of the controlled fire decreases, which means that the losses may still increase but at a very slow rate.
- Finally, at each period, there is a given probability that the controlled fire is extinguished (the smaller the fire, the larger the probability of extinction); the extinction states are absorbing states for the Markov model.

The system at a given time can, therefore, be in one of five phases:

- an active, undetected fire ("active" states);
- a fire that has just been detected ("detected" states);
- a still growing fire which firemen are fighting ("working" states);
- a controlled but still burning fire ("controlled" states);
- an extinguished fire ("extinction" states).

Furthermore, in each phase, the fire can be in one of the four loss ranges considered. We therefore consider a system that can be in 20 different states. At a

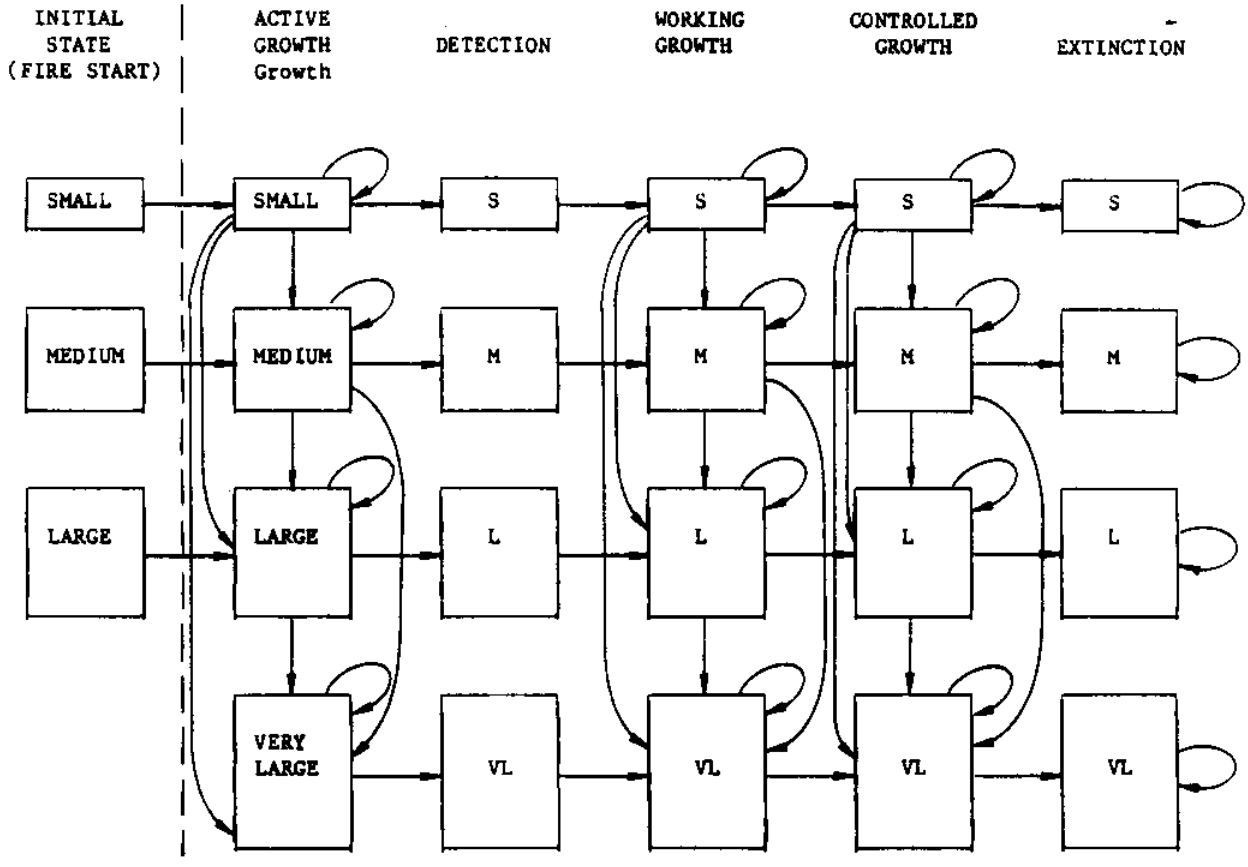


Fig. 2. Transition diagram for Markov modelling of fire growth and detection.

given time t, the system's evolution can be described by a vector of probabilities $P(t)$ that it is in one of these twenty states. This transition process is described in Fig. 2. It is assumed in this model that the fire would not extinguish itself but had to go necessarily through the five phases mentioned here. Of course, the losses associated with a given fire never decrease in further transitions.

3. COSTS AND BENEFITS OF A MONITORING CAMERA

The camera is assumed to be placed in a spot where fires can occur for two reasons: (1) failure of a pump, or (2) failure of valves and lines. The computation of costs and benefits of adding a monitoring camera is done in five steps (see Appendix 2).

First, we compute the expected benefits of camera monitoring for one pump fire. Because of earlier detection, the probability that the fire finally reaches larger sizes decreases, and the expected value of the losses is smaller with the camera than without it. The benefits of the camera in one pump fire are the expected value of this difference of losses.

Secondly, we compute the expected value of the annual loss reduction for all pump fires in the monitored area. To do this, we consider the total number of pump fires in the whole refinery, and the probability that given such a fire, it occurs in the monitored area. We then repeat these computations for valve and line fires, using corresponding data for our Markov model of growth and extinction.

Finally, we add the benefits for both types of fires and we compute the global economic results of camera monitoring: the benefit-cost ratio, the present value of the cash flow, and the internal rate of return of the investment (as if the expected value of the expected losses were sure benefits).

4. ECONOMIC EFFECT OF MONITORING DELAYS

The new camera may be useless if the operator in the control room does not immediately notice the fire when it appears on the screen, which results in a delay of firemen's intervention. After a short time, the fire is actually detected by other means of monitoring (e.g., people passing by). The benefits as computed above may therefore be overestimated.

The potential delays can be measured as a random variable K. The value of K affects the transition matrix of Appendix 1. The model described in Section 3 is run for each possible value of K. The reduction of the benefits due to these delays is then computed by comparison of loss reduction, given minimum intervention time.

This technique can generally be applied to the analysis of warning systems in which the signal cannot be missed forever (Type I error), but for a random number of periods while the background problem is still growing unnoticed (Type I delay).

5. NUMERICAL APPLICATION

The numerical example that follows is a hypothetical illustration for a very large refinery. All costs and benefits are evaluated in 1984 dollars. Fire losses and frequencies for different causes were assessed after Standard Oil documentation for a group of nine refineries for years 1979, 1980, and 1981.[10,11,12] For convenience, given the structure of the data, the global reference was therefore the potential loss reduction in this group of refineries, and the probability that given a fire occurrence in this group, it happens in the monitored area in the considered refinery. A crude assessment of the probabilities of growth and extinction was then done through conversations with the staff of the Chevron refinery in

Table II. Pump Fires' Growth, Detection, and Extinction Probabilities for the Area With and Without the New Camera

Dollar loss for each fire size	Probability of initial fire size	Undetected fire growth (transition matrix) 1	2	3	4	Detection probability without the new camera	Detection probability with the new camera	Working fire growth (transition matrix) 1	2	3	4	Probability of fire control	Controlled fire growth (transition matrix) 1	2	3	4	Probability of fire extinction
5,000	0.85	0.85	0.13	0.02	0.00	0.60	0.80	0.90	0.10	0.00	0.00	0.80	0.97	0.03	0.00	0.00	0.90
34,000	0.13	0.00	0.85	0.13	0.02	0.65	0.85	0.00	0.90	0.10	0.00	0.70	0.00	0.94	0.06	0.00	0.60
247,000	0.02	0.00	0.00	0.85	0.15	0.70	0.90	0.00	0.00	0.85	0.15	0.60	0.00	0.00	0.93	0.07	0.40
3,500,000	0.00	0.00	0.00	0.00	1.00	0.75	0.95	0.00	0.00	0.00	1.00	0.50	0.00	0.00	0.00	1.00	0.30

Table III. Expected Benefit of Monitoring All Pumps[a]

Total number of pump fires this year	Probability of this many fires[b]	Expected benefit given this many fires
1	0.0152	44,660
2	0.0303	89,320
3	0.0455	133,981
4	0.0606	178,641
5	0.0757	223,301
6	0.0909	267,961
7	0.0852	312,621
8	0.0795	357,281
9	0.0738	401,942
10	0.0681	446,602
11	0.0625	491,262
12	0.0568	535,922
13	0.0511	580,582
14	0.0454	625,243
15	0.0397	669,903
16	0.0340	714,563
17	0.0283	759,223
18	0.0226	803,883
19	0.0169	848,543
20	0.0112	893,204
21	0.0055	937,864

[a] Overall expected benefit of monitoring all pumps = $416,021.

[b] Conditional on the occurrence of a fire starting from a pump failure, we assume a probability 0.020 that it occurs in the monitored area. Thus, the annual expected savings will be $8,320.

Table V. Expected Benefit of Monitoring All Lines and Valves[a]

Total number of valve & line fires this year	Probability of this many fires[b]	Expected benefit given this many fires
1	0.0667	31,588
2	0.1333	63,175
3	0.2000	94,763
4	0.1716	126,351
5	0.1430	157,939
6	0.1144	189,526
7	0.0858	221,114
8	0.0572	252,702
9	0.0286	284,290
10	− 0.0000	315,877

[a] Overall expected benefit of monitoring all valves and lines = $136,985.

[b] Conditional on the occurrence of a fire starting either from a valve or line failure, we assume a probability 0.010 that it occurs in the monitored area. Thus, the annual expected savings will be $1,370.

Richmond, California. It was checked that the corresponding times to fire extinction were generally realistic. The basic time unit is 1 min. The response time (between detection and firemen's intervention) is originally estimated at a minimum of 2 min,then replaced by a random variable in order to check the economic effects of detection delays. Table II shows the input probability data with and without the proposed camera. Table III shows the annual distribution of the total number of pump fires in the considered group of nine refineries, and the annual benefit of monitoring the considered spot. Tables IV and V show the same inputs and results for valve and line fires.

The total annual benefit (avoided losses) of the camera is:

$$b = \$1,370 + \$8,320 = \$9,690$$

The initial cost of the camera is assumed to be $20,000, the operation and maintenance cost to be $5 per day or $1,825 per year, and the rate of discount 12%. The economic life of the camera is expected to be 10 yr. The total equivalent uniform annual cost is therefore $4,525.

The economic results are therefore: (1) Expected benefit-cost ratio: 2.14; (2) Expected net present value of the cash flow over 10 yr: $58,650 (expected payback

Table IV. Line or Valve Fires' Growth, Detection, and Extinction Probabilities for the Area With and Without the New Camera

Dollar loss for each fire size	Probability of initial fire size	Undetected fire growth (transition matrix) 1	2	3	4	Detection probability without the new camera	Detection probability with the new camera	Working fire growth (transition matrix) 1	2	3	4	Probability of fire control	Controlled fire growth (transition matrix) 1	2	3	4	Probability of fire extinction
5,000	0.93	0.85	0.13	0.02	0.00	0.40	0.80	0.90	0.10	0.00	0.00	0.80	0.99	0.01	0.00	0.00	0.90
37,000	0.07	0.00	0.75	0.25	0.00	0.45	0.85	0.00	0.81	0.19	0.00	0.70	0.00	0.90	0.10	0.00	0.60
355,000	0.00	0.00	0.00	1.00	0.00	0.50	0.90	0.00	0.00	1.00	0.00	0.60	0.00	0.00	1.00	0.00	0.40
3,500,000	0.00	0.00	0.00	0.00	1.00	0.55	0.95	0.00	0.00	0.00	1.00	0.50	0.00	0.00	0.00	1.00	0.30

period between 2 and 3 yr); (3) Internal rate of return (as if expected benefits were certain): 38%.

The economic implications of the method used and the value of the results are discussed in the next paragraph; but one can already conclude that the risk-indifferent investor who relies on expected values of costs and benefits for his investments (and *a fortiori* the risk-averse decision maker) will find the project economically attractive.

5.1. Effect of Type I Delays

The results above were computed assuming that the operator immediately notices the fire on the monitoring screen and that the firemen intervene two minutes after the fire is detected. The response time, however, can be greater. Table VI shows a probability distribution for Type I delays and the effects of these delays on the expected value of losses in one fire. These results were obtained using the models described in Appendix 2 with different values of k. When the delay exceeds 3 min for pump fires or 4 min for valve and line fires, the fire is likely to be detected by conventional means before it is noticed by the operator (the model then would show greater losses for camera monitoring than for present detection). It is, therefore, assumed here that the current means of fire detection are kept in operation after the new system is adopted.

The expected value of benefits of the new camera for the detection of pump fires is $40,500 per fire (instead of $45,000, assuming 2 min response time), because with probability 0.1, the fire will be detected by current means rather than by the proposed camera. For valve and line fires, the expected value of the benefits is $29,000, accounting for possible delays, instead of $31,600 for the 2 min response time. The expected value of the annual benefits is $8,812 (instead of $9,690), showing a 9% reduction due to potential Type I delays. The project, however, remains attractive to the risk-indifferent (and therefore to the risk-averse) decision maker.

6. CONCLUSIONS

The probabilistic method presented here allows one to perform a difficult task: the evaluation of a safety investment with uncertain returns. In the illustrative case presented here, one can show that the proposed monitoring by cameras of one specific area has a large positive net present value over the proposed economic life of the investment, a benefit-cost ratio greater than two, and an internal rate of return between 30% and 40%.

The model presented here includes the effect of Type I delays on the overall performance of the equipment. To include the effects of the system's reliability on these results, the benefits can simply be multiplied by the expected proportion of operation time; expected annual repair costs should then be added to the total annualized cost. Economic computations are done assuming that the decision maker is risk-indifferent and makes investment decisions on the basis of expected values. This is a reasonable assumption because of the relatively low range of costs and benefits considered here. If the company is risk-averse, and willing to spend greater sums to reduce large losses, the method can simply be modified by replacing loss reductions by the corresponding value of the firm's utility function.

The method itself is general and can be used with little or no modifications to assess the value of any device or procedure of fire detection and fire prevention in oil refineries. The corresponding data would have to be collected to model the growth and extinction of other types of fires (e.g., fires originated in petroleum tanks). With appropriate parameters, the method could also be used for fire detection in

Table VI. Effect of Type I Delay on the Benefits of the New Camera for One Fire

		Expected value of loss in one pump fire ($)			Expected value of loss in one valve & lines fire		
Response time	Probability	Status quo	New camera	Difference	Status quo	New camera	Difference
2 mn	0.9	215,000	170,000	45,000	93,600	62,000	31,600
3 mn	0.06	215,000	*a*	0	93,600	89,000	4,500
4 mn	0.03	215,000	*a*	0	93,600	*a*	0
5 mn	0.01	215,000	*a*	0	93,600	*a*	0

[a] Fire is detected by present monitoring system before the end of Type I delay.

other settings (e.g., industrial, commercial, or apartment buildings).

APPENDIX 1

Markov Model of Fire Growth and Extinction

The transition matrix A is the matrix of probabilities of transition from state i to state j in any given time unit.[13] It is defined by several "component matrices."

- The first component is the 4 × 4 matrix G of the probabilities of transition among the four considered fire sizes in the initial uncontrolled phase of fire growth.
- The second component is the 4 × 4 diagonal matrix D of the probabilities of detection of fires of each size at the active stage.
- The third component is the 4 × 4 matrix W of the probabilities of transition among the four considered fire sizes in the "working" phase.
- The fourth component is the 4 × 4 diagonal matrix C of the probabilities that, at the working stage, fires of different sizes are brought under control.
- The fifth component is the 4 × 4 matrix CG of the probabilities of transition among the four considered fire sizes in the "controlled" phase.
- The sixth component is the 4 × 4 diagonal matrix X of the probabilities of extinction of fires of each size at the controlled stage.

The structure of the global transition matrix A is described in Fig. 3.

I is the unit 4 × 4 matrix. GN is an adapted form of G; this form assures that the transition probabilities for each line add up to 1. GN is obtained by multiplying the transition probabilities of matrix G by the probability that fires of each considered size are not detected in each time period. In the same way, WN is obtained by multiplying the elements of matrix W by the probability that fires of each size are not brought under control at each time period, and CGN is obtained by multiplying the elements of matrix CG by the probability that fires of each size are not extinguished at each time period.

The transition matrix A includes a delay factor (noted k in Fig. 3), which is the number of time periods between detection and the moment when the firemen begin fighting the fire. During this time, the fire grows at the same rate as if it had not been

	ACTIVE GROWTH	DETECTION	WORKING GROWTH	CONTROLLED GROWTH	EXTINCTION
ACTIVE GROWTH	GN	D	0	0	0
DETECTION	0	0	G^k	0	0
WORKING GROWTH	0	0	WN	C	0
CONTROLLED GROWTH	0	0	0	CGN	X
EXTINCTION	0	0	0	0	I

Fig. 3. Structure of the fire growth transition matrix (See notations in the text).

detected for k periods, then enters the "working" phase. The growth during the delay is, therefore, equivalent to a one-period growth described by the transition matrix G^k.

Let L be the vector of mean dollar losses in each of the four ranges considered. L_i is the ith component of this vector. $P(0)$ is the vector of probabilities that the fire starts in each of the twenty possible states. As the fire actually begins in the active, uncontrolled phase, the first four components of $P(0)$ represent the probabilities $P_0(L_i)$ that the fire starts in each of the four considered fire sizes. $P(0)$, therefore, has the following structure:

$$P(0) = [p_0(L_1), p_0(L_2), p_0(L_3), p_0(L_4), 0, \ldots, 0] \tag{1}$$

Let $P(t)$ be the vector of probabilities that the fire is in each of the twenty states at time t. $P(t)$ is given by the following product[9]:

$$P(t) = P(0) \times A^t \tag{2}$$

The goal is to find the final distribution of losses after fire extinction, and, therefore, the limit of A^t when t becomes infinite. Instead of proceeding analytically and computing the eigen values of A, the choice was to compute the successive powers of A in order to observe the time evolution of fire losses. Computation was interrupted by the following stopping rule: either 99.5% of the fires were extinguished (which turned out to be the binding constraint in all cases considered here) or 50 time units had elapsed. Let t^* be the total time elapsed when the process is stopped. At this point, virtually all fires have been extinguished and the system is in one of the last four states. The result is, therefore, a vector $P(t^*)$ of the following form:

$$P(t^*) \simeq [0, \ldots, 0, p^*(L_1), p^*(L_2), p^*(L_3), p^*(L_4)] \tag{3}$$

The p^*'s are the steady state probabilities of the process. They give the probability distribution of final fire losses for the considered dollar values L_1, L_2, L_3, or L_4. The algorithm used here gives a close approximation of the p^*'s.

APPENDIX 2

Probabilistic Model of Costs and Benefits of a Monitoring Camera

Step 1: Expected Value of the Avoided Loss in One Pump Fire by Addition of the Camera

The notations are the following:

A_p	transition matrix for the growth and extinction of a pump fire with current monitoring;
A'_p	transition matrix for the growth and extinction of a pump fire with the added camera;
$P_p(t^*)$	steady state probability vector for a pump fire with current monitoring [including the final fire loss distribution $p_p^*(L_i)$];
$P'_p(t^*)$	steady state probability vector for a pump fire with proposed added camera [including the final fire loss distribution $p_p'^*(L_i)$];
$P_p(0)$	initial state vector (initial fire size) for a pump fire;
$EV(LP)$	expected value of the losses in one pump fire with current monitoring practice;
$EV(LP')$	expected value of the losses in one pump fire with proposed camera;
B_p	expected value of the loss reduction (benefits) due to added camera in one pump fire;
B_{ap}	expected value of the loss reduction (benefits) due to added cameras, as if all pumps in the refinery were under proposed new monitoring system;
$p(m\|f_p)$	conditional probability that given the occurrence of a pump fire somewhere in the refinery, it actually happens in the monitored area;
b_p	expected value of the annual loss reduction (benefits) in a pump fire in the monitored area;
N_p	number of pump fires in 1 yr in the whole refinery (random variable).

A_p and A'_p differ by the matrix D because the probability of the detection of fires of all sizes at each time period is higher with the camera than without.

Without the new camera, the steady state probabilities of the system are given by:

$$P_p(t^*) = P_p(0) \times (A_p)^{t^*} \tag{4}$$

The expected value of the losses in one pump fire given current monitoring practice is equal to:

$$EV(LP) = \sum_{i=1}^{4} p_p^*(L_i) \times L_i \tag{5}$$

The elements $p_p^*(L_i)$ are the last four elements of vector $P_p(t^*)$.

With the new camera, the steady state probabilities of the system are given by:

$$P'_p(t^*) = P_p(0) \times (A'_p)^{t^*} \tag{6}$$

The expected value of the losses in one pump fire with the proposed monitoring system is:

$$EV(LP') = \sum_{i=1}^{4} p'^*(L_i) \times L_i \tag{7}$$

The elements $p'^*_p(L_i)$ are the last four elements of vector $P'_p(t^*)$.

$$B_p = EV(LP) - EV(LP') \tag{8}$$

Step 2: Expected Value of the Annual Loss Reduction in Pump Fires in the Monitored Area

Let N_p (random variable) be the annual number of fire pumps in the whole refinery, and $EV(N_p)$ its expected value.

If all the pumps in the refinery were monitored, the expected value of the annual benefits would be:

$$B_{ap} = B_p \times EV(N_p) \tag{9}$$

$p(m|f_p)$ is the probability that given the occurrence of a pump fire, it happens in the monitored area. If, for example, one assumed that all pumps are equally likely to become defective and cause a fire, this conditional probability could be approximated by the proportion of all the pumps of the refinery that are located in the monitored area.

The benefits of loss reduction in pump fires in the monitored area are then:

$$b_p = B_{ap} \times p(m|f_p) \tag{10}$$

Step 3: Expected value of the avoided loss in one valve and line originated fire (valve and line fire) by addition of the proposed camera

This step is similar to Step 1 with data corresponding to the growth and extinction of a fire generated by failure of a valve or a line. The notations are the following:

A_v	transition matrix for the growth and extinction of a valve and line fire with current monitoring;
A'_v	transition matrix for the growth and extinction of a valve and line fire with the added camera;
$P_v(t^*)$	steady state probability vector for a valve and line fire with current monitoring (including the final fire loss distribution $p_v^*(L_i)$);
$P'_v(t^*)$	steady state probability vector for a valve and line fire with proposed added camera (including the final fire loss distribution $p'^*_v(L_i)$);
$P_v(0)$	initial state vector (initial fire size) for a valve and line fire;
$EV(LV)$	expected value of the losses in one valve and line fire with current monitoring practice;
$EV(LV)'$	expected value of the losses in one valve and line fire with the proposed camera;
B_v	expected value of the loss reduction (benefits) due to added camera in one valve and line fire;
B_{av}	expected value of the annual loss reduction (benefits) due to added cameras, as if all lines and valves in the refinery were under the proposed new monitoring system;
$p(m\|f_v)$	conditional probability that given the occurrence of a valve and line fire somewhere in the refinery, it

actually happens in the monitored area;

b_v expected value of the annual loss reduction (benefits) in a valve and line fire in the monitored area;

N_v number of valve and line fires in 1 yr in the whole refinery [random variable; expected value: $EV(N_v)$].

The equations are similar to those used to analyze loss reduction for pump fires:

Steady state probabilities with current monitoring:

$$P_v(t^*) = P_v(0) \times (A_v)^{t^*} \qquad (11)$$

Losses in one valve and line fire with current monitoring:

$$EV(LV) = \sum_{i=1}^{4} p_v^*(L_i) \times L_i \qquad (12)$$

Steady state probabilities with added camera:

$$P_v'(t^*) = P_v(0) \times (A_v')^{t^*} \qquad (13)$$

Losses in one valve and line fire with added camera:

$$EV(LV') = \sum_{i=1}^{4} p_v'^*(L_i) \times L_i \qquad (14)$$

Benefits of added camera in one valve and line fire:

$$B_v = EV(LV) - EV(LV') \qquad (15)$$

Step 4: Expected value of the annual loss reduction in valve and line fires in the monitored area

Again, the equations are similar to those used to analyze loss reductions for pump fires:

Annual benefits of the new system as if all lines and valves of the refinery were under proposed monitoring:

$$B_{av} = B_v \times EV(N_v) \qquad (16)$$

Annual benefits (loss reduction) for valve and line fires in the monitored area:

$$b_v = B_{av} \times p(m|f_v) \qquad (17)$$

Step 5: Economic results [14]

The notations are the following:

C first cost of the camera system (including camera monitoring screen, connections, etc.);

R minimum acceptable rate of the return of the firm (e.g., rate of interest, rate of discount, etc.);

Y number of years of the economic life of the new system;

c_p annual cost of the operation and maintenance of the new system;

c total value of the annualized costs of the new system;

b total value of the annual benefits of the new system.

The total value of the annual benefits of the proposed camera, that monitors an area where fires can be caused either by pump failure or by failure of lines and valves, is:

$$b = b_p + b_v \qquad (18)$$

It is assumed that the salvage value at the end of Y yr is 0. The equivalent uniform annual cost of the system is c, the sum of the annualized first cost[14] and of the annual cost of operation and maintenance of the camera:

$$C = c_p + C\frac{R(1+R)^Y}{(1+R)^Y - 1} \qquad (19)$$

Results

- The expected value of the benefit-cost ratio is simply the ratio b/c.
- The net present value of the cash flow is the difference:

$$NPV = \sum_{t=1}^{Y} \frac{b - c_p}{(1+R)^t - C} \qquad (20)$$

- The internal rate of return (IRR) of the investment (treated as if the expected value of avoided losses were sure benefits) is the solution of the equation:

$$\sum_{t=1}^{Y} \frac{b - c_p}{(1 + IRR)^t} - C = 0 \qquad (21)$$

ACKNOWLEDGMENTS

This study was partially funded by a grant from the Stanford Center for Economic Policy Research, whose support is gratefully acknowledged. The author thanks Mr. David Blumquist and Mr. Frank Talbot from Standard Oil of California for their help in the initial phase of the project, and Mr. Timothy O'Grady for his assistance in the computational part of this study.

REFERENCES

1. American Petroleum Institute, *Reported Fire Losses in the Petroleum Industry for 1975* (API, Washington, D. C., 1976).
2. American Petroleum Institute, *Reported Fire Losses in the Petroleum Industry for 1976* (API, Washington, D. C., 1977).
3. American Petroleum Institute, *Reported Fire Losses in the Petroleum Industry for 1977* (API, Washington, D. C., 1978).
4. American Petroleum Institute, *Reported Fire Losses in the Petroleum Industry for 1978* (API, Washington, D. C., 1979).
5. American Petroleum Institute, *Reported Fire Losses in the Petroleum Industry for 1979* (API, Washington, D. C., 1980).
6. American Petroleum Institute, *Fire Protection in Refineries* (API RP 2001, Washington, D. C., March, 1974).
7. M. E. Paté-Cornell, *Warning Systems: Signals and Response* (Research Report to the Stanford Center for Economic Policy Research, Stanford University, California, 1983).
8. M. E. Paté-Cornell and T. S. O'Grady, *Reduction of Fire Risks in Oil Refineries: Costs and Benefits of Camera Monitoring* (Technical Report TR84-1, Department of Industrial Engineering & Engineering Management, Stanford University, Stanford, California, January 1984).
9. W. C. T. Ling and R. B. Williamson, "Using Fire Tests for Quantitative Risk Analysis," *Fire Risk Assessment* (American Society for Testing and Materials, STP 762, 1982), pp. 38–58.
10. Standard Oil Company of California, *Corporate Fire Loss, 1979* (San Francisco, California, 1979).
11. Standard Oil Company of California, *Corporate Fire Loss, 1980* (San Francisco, California, 1980).
12. Standard Oil Company of California, *Corporate Fire Loss, 1981* (San Francisco, California, 1981).
13. S. Karlin, *A First Course in Stochastic Processes* (Academic Press, New York, 1971).
14. E. L. Grant, W. G. Ireson, and R. S. Leavenworth, *Principles of Engineering Economy* (John Wiley & Sons Inc., New York, 1982), 7th ed.