Managing Fire Risk Onboard Offshore Platforms: Lessons from Piper Alpha and Probabilistic Assessment of Risk Reduction Measures

Elisabeth Paté-Cornell
Paté-Cornell is with the Department of Industrial Engineering and Engineering Management at Stanford University in California.

Abstract

The offshore oil platform Piper Alpha was destroyed in July 1988 by a catastrophic fire. The causes of the accident included a combination of technical and organizational factors. In this paper, I describe the accident, its chronology, and the dependencies involved. I then examine some of the human errors that led to the disaster and their organizational roots, such as economic pressures, the permit-to-work system, and the inadequacy of regulatory oversight in the United Kingdom at the time of the accident. Risk-reduction measures can be costly, however, and priorities must be set based on costs and benefits. To this end, I describe a probabilistic risk analysis model that can be used to assess the benefits of different fire safety measures, focusing on reinforcing the emergency water pumps.

Post-Mortem Analysis of Piper Alpha

The fire that engulfed the Piper Alpha platform on July 8, 1988 apparently began with the technical failure of a blind flange assembly at the site of a pressure safety valve (see Figure 1). The accident led to the total loss of the platform and the deaths of 167 men. These failures and their consequences were, in large part, the result of questionable—or bad—decisions, themselves rooted in management problems.[1,2,3]

These decisions concerned the design of the platform deck and jacket, production levels and capacity expansion, inspection and maintenance procedures, and personnel management. Their organizational roots included the way the company managed, on a daily basis, the trade-off between productivity and safety, the flaws in the design philosophy, the problems in personnel hiring and promotion procedures, the deficiencies of the work-permit system, and the relations between the company and regulatory authorities. By identifying these organizational problems and quantifying, even coarsely, their effects on the overall risk, we can consider a much broader spectrum of risk management policies than would be possible if we restricted our analysis to technical measures.

In previous research, I developed a systematic method to link the basic events of probabilistic risk analysis (PRA) models both to human decisions and actions and to their organizational roots. I applied it to a variety of risk analysis problems, such as the management of the space shuttle's tile problem.[4] In this paper, I apply the same method in a postmortem mode to the Piper Alpha accident, propose some corrective measures to reduce the risks of fire on platforms, and describe a stochastic risk analysis model to compute their risk-reduction benefits.[2,3]

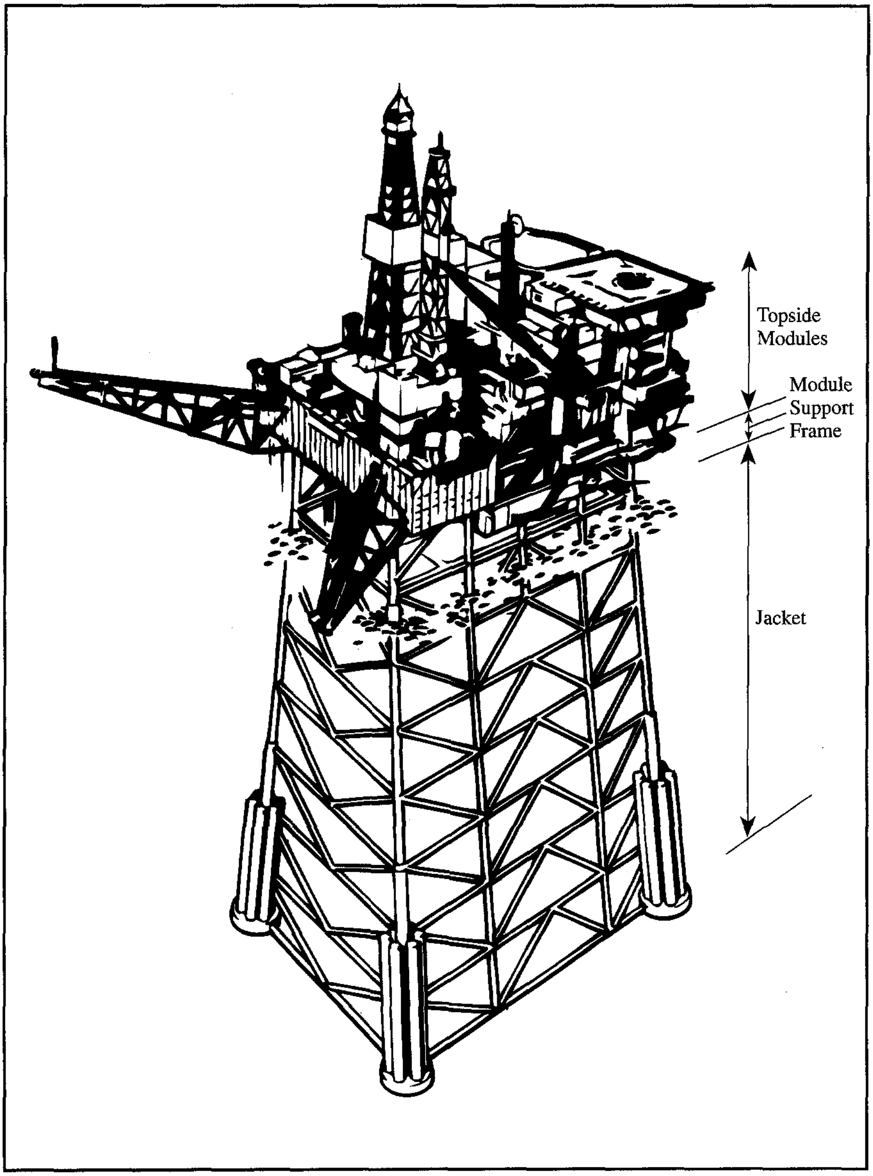


Figure 1. The Piper Alpha platform.[5]

Basic Events of the Piper Alpha Accident Sequence

The accident started with a process disturbance, followed by a flange leak that caused a vapor release. The explosions that followed 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 Piper Alpha deck. The layout of the topside was such that the fire propagated quickly from Production Modules B and C and destroyed the control room and the radio room in the early stages of the accident (see Figure 2). Electric power generation, public address, general alarm, emergency shutdown, and fire detection and protection systems also failed shortly after the first explosion.

Piper Alpha was part of a network of platforms, including platforms Tartan, Claymore, and MCP-01 (see Figure 3). The risers from these platforms started failing where they interfaced with the deck of Piper Alpha, causing further damage.

The superintendent of the platform—known as the Offshore Installation Manager, or OIM—panicked, was ineffective almost from the beginning, and died in the accident. Evacuation was not ordered—and even if it had been, it 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. Many evacuation routes were blocked, and the life boats, which were all in the same location, were mostly inaccessible.

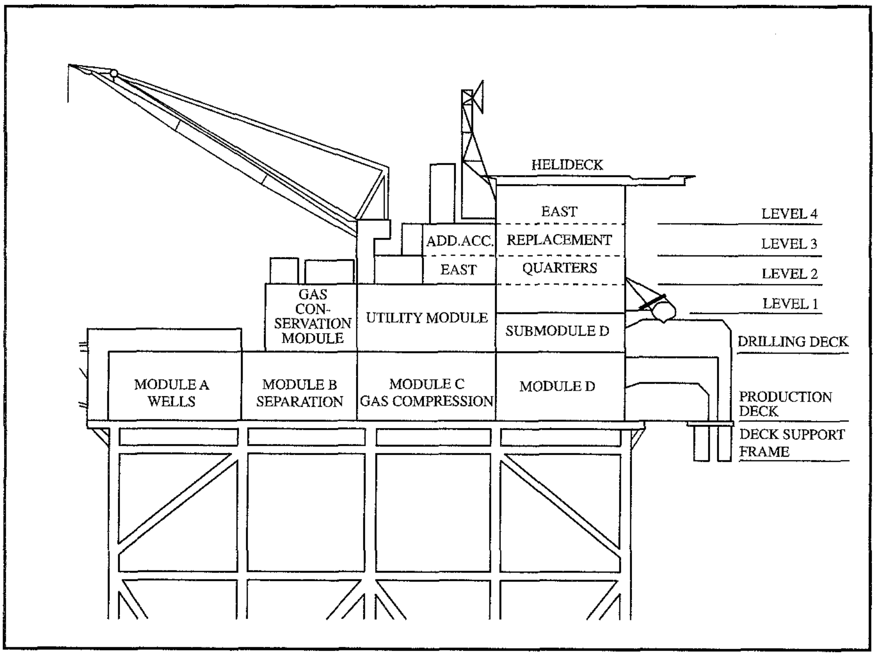


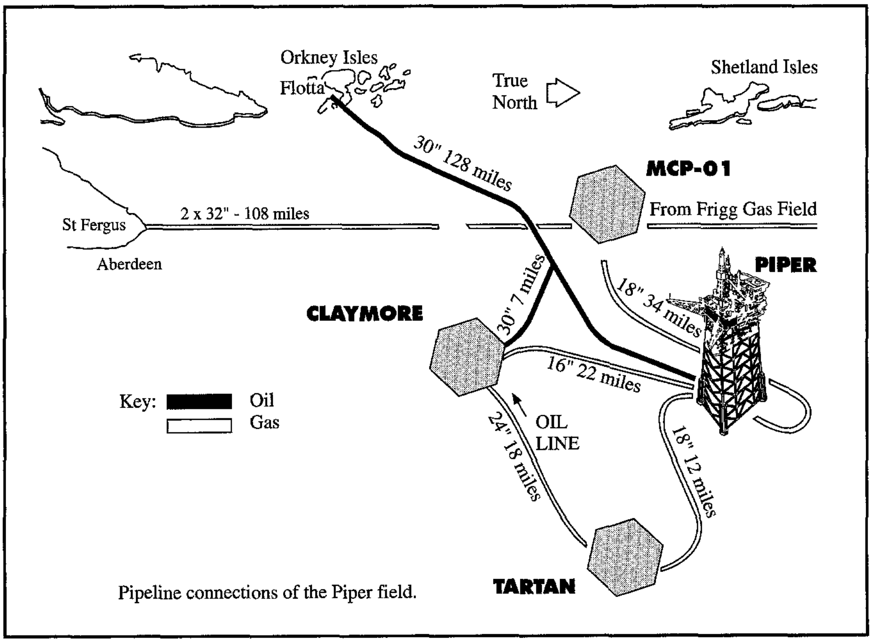
Figure 2. Location of modules (east elevation).[5]

The fire fighting equipment onboard could not be operated because the diesel pumps, which had been put on manual mode, were also inaccessible and seem to have been damaged from the beginning. Fire boats were at hand, but their crews waited to fight the fire until they received orders from the OIM. When the master of the vessel Tharos, which was on-site, decided to assume the role of on-scene commander, 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 U.S. $3 billion.[6]

In this study, I used a risk analysis model structure to identify the "failure path" or accident sequence that occurred on Piper Alpha. First, I examined the initiating events, encompassing three phases of explosions and fires and including not only the actual initial explosion and fire, but also, the subsequent ones that initiated further component failures. Then, I analyzed the consequences of these initiating events, from the emergency system failures, to the final system states, to the accident losses.

The basic events of the failure mode are presented in Table 1, and their dependencies are shown in the influence diagram of Figure 4. This influence diagram format is generally used *a priori* to assess the risks. It shows the events and random variables that affect the potential outcomes. In this case, the same format is used *a posteriori* to display the events, variables, and causalities in a past accident.



Pipeline connections of the Piper field.

Figure 3. The Piper Alpha Platform Network.[5]

Table 1
Basic Events of the Piper Alpha Accident Sequence

INITIATING EVENTS	CONSEQUENCES
First explosion	
• Process disturbance occurs • Redundant pumps become inoperative • Blind flange assembly fails • 45 kg of condensate vapors are released • Gas detectors and emergency shutdown fails • First ignition and explosion occurs • Gas detectors almost fail totally • The deluge systems fail • The emergency shutdown system fails • The fire walls fail	• Electrical power is lost • Emergency lighting fails • The control room fails • The public address system fails • The radio-telecommunication room fails • The operations manager (OIM) is lost • Helicopter rescue operations fail
Second explosion	
• Fire propagation spreads to other Modules • A pipe in Module B ruptures • Large crude oil leak occurs in Module B • Fire ball and deflagration occur in Module B • Fire spreads to 1,200 barrels of fuel stored on the deck	• Pipes and tanks rupture • Some survivors jumped into the sea • Some people die in the quarters (22:33) • The Tharos fire fighting equipment fails
Jet fire from broken riser	
• The fire pumps fail • The riser from Tartan to Piper Alpha ruptures • Intense impinging jet fire breaks out under the platform	• The MCP-01 riser at Piper Alpha ruptures • People are trapped in living accommodations • Some survivors jump from the helideck • The platform at the 68ft level collapses • Western crane collapses from the turret • The Claymore gas riser ruptures • Sequence of structural failures occur under fire loads a • Accommodation module overturns into the sea • Survivors rescued at sea by onsite vessels
Final losses	
• 167 die (165 men on board and 2 rescue workers) • The platform is a total loss, with financial damage exceeding three billion U.S. dollars	

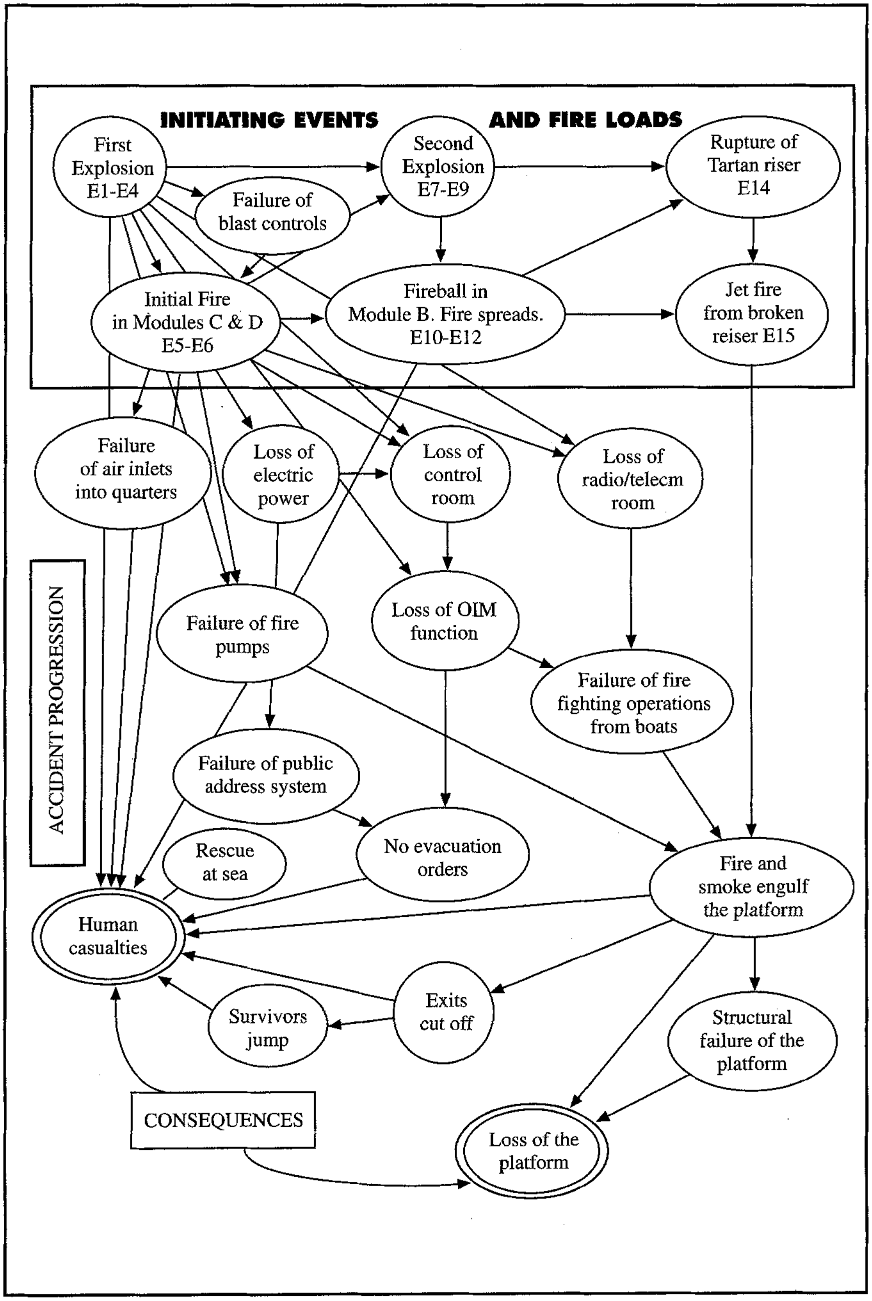

INITIATING EVENTS AND FIRE LOADS
First Explosion E1-E4
Second Explosion E7-E9
Rupture of Tartan riser E14
Failure of blast controls
Initial Fire in Modules C & D E5-E6
Fireball in Module B. Fire spreads. E10-E12
Jet fire from broken reiser E15
Failure of air inlets into quarters
Loss of electric power
Loss of control room
Loss of radio/telecm room
ACCIDENT PROGRESSION
Failure of fire pumps
Loss of OIM function
Failure of fire fighting operations from boats
Failure of public address system
Rescue at sea
No evacuation orders
Fire and smoke engulf the platform
Human casualties
Exits cut off
Survivors jump
Structural failure of the platform
CONSEQUENCES
Loss of the platform

Figure 4. Event dependencies in the Piper Alpha accident; influence diagram representation.[3]

The two main references of this study are the 1988 Petrie report[6] and the 1990 Cullen report.[7] Other sources include personal communications.[5,8]

Human Errors

The human errors that caused the basic events of the Piper Alpha accident can be classified into four categories: design and expansion issues, production decisions in the platform network, personnel problems and crisis management, and errors in inspection and maintenance operations. Figure 5 represents the different levels of causality among these factors. At the bottom is a simplified version of the accident scenario and its basic events. At the next level above are the decisions and actions that caused or influenced them. And at the top level are the basic organizational factors that influenced human errors.

A large number of these elements resulted from design decisions that caused dangerous couplings and dependencies. These included the direct linkage of failures—for example, the power supply and public address system; weaknesses in fire walls and separation, which caused quick fire propagation from Module B to Module C to the control room; and the vulnerability of several components to a common cause of failure—that is, to the same blast. The problem was compounded by lack of backups in many of the critical safety features, such as the power supply. In addition, the deck was packed with equipment, the living quarters were not adequately protected, and the evacuation routes and means of escape were inappropriate.

The compactness and lack of separation that caused a rapid fire spread were due, in large part, to the way the system had grown over time. In the end, it had been modified to accommodate higher levels of production than originally planned for, with added components and equipment brough onboard, some of which were simply stacked on the deck. Not only was the final layout different from the original, but successive additions had been made before anyone investigated their effect on safety features. For example, external additions to Module C prevented the blast relief from functioning adequately.[5]

Personnel management was also deficient. There were not enough qualified and experienced people onboard at the time of the accident, so available personnel performed critical functions on the basis of temporary promotion. Less experienced operators, maintenance crews, and production workers were allowed to run the platform in Phase 1 of operations at a high level of activity that should have required special attention.

The loss of the OIM illustrates a lack of crisis management training. Simple instructions about emergency procedures are insufficient because they may not apply in an actual accident. Leadership during crises requires appropriate protection of the people in charge, particular types of personalities, and an in-depth knowledge of the system, none of which seem to have been available on Piper Alpha when the accident occured.

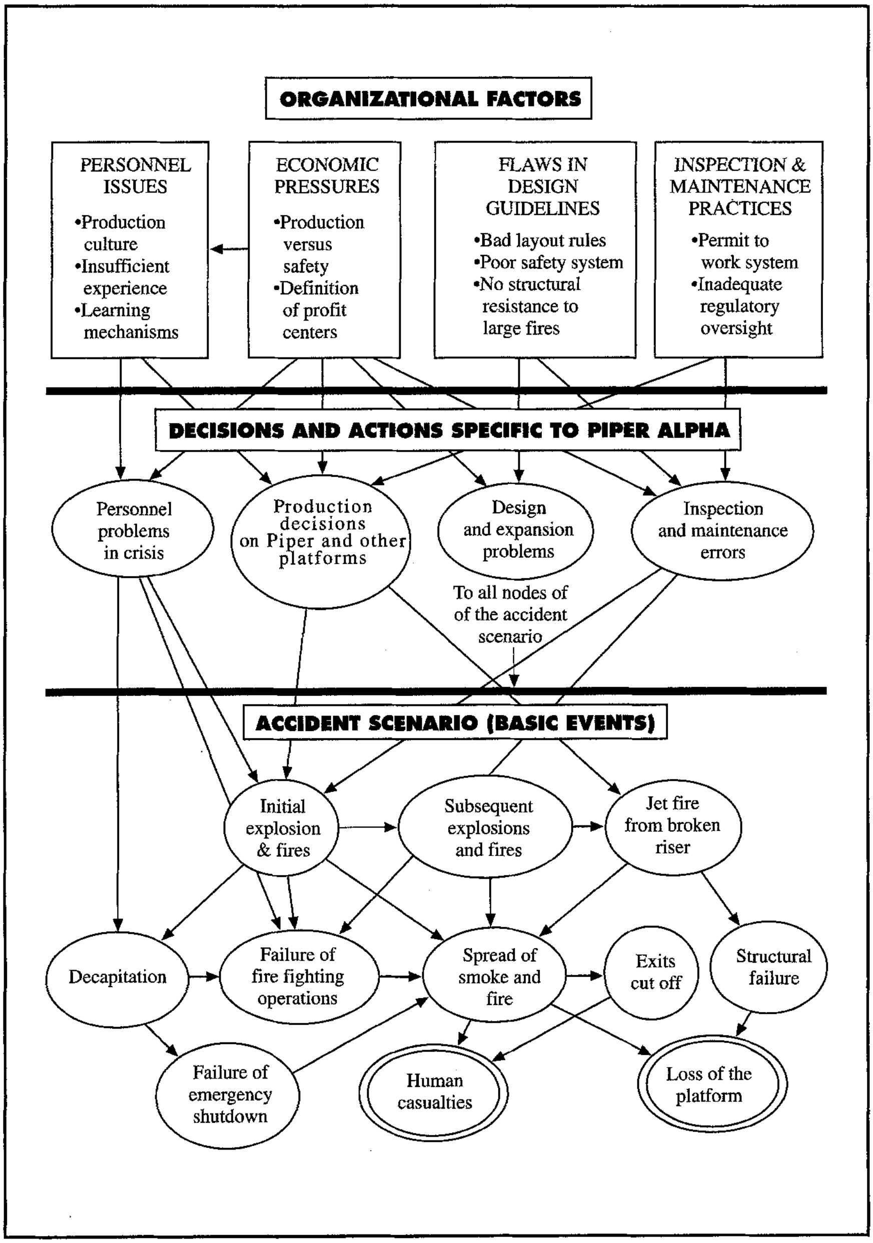

ORGANIZATIONAL FACTORS
PERSONNEL ISSUES
•Production culture
•Insufficient experience
•Learning mechanisms
ECONOMIC PRESSURES
•Production versus safety
•Definition of profit centers
FLAWS IN DESIGN GUIDELINES
•Bad layout rules
•Poor safety system
•No structural resistance to large fires
INSPECTION & MAINTENANCE PRACTICES
•Permit to work system
•Inadequate regulatory oversight
DECISIONS AND ACTIONS SPECIFIC TO PIPER ALPHA
Personnel problems in crisis
Production decisions on Piper and other platforms
Design and expansion problems
Inspection and maintenance errors
To all nodes of of the accident scenario
ACCIDENT SCENARIO (BASIC EVENTS)
Initial explosion & fires
Subsequent explosions and fires
Jet fire from broken riser
Decapitation
Failure of fire fighting operations
Spread of smoke and fire
Exits cut off
Structural failure
Failure of emergency shutdown
Human casualties
Loss of the platform

Figure 5. Organizational roots of the Piper Alpha accident. (Influence diagram representation; the low part is a simplified version of Figure 3.)[3]

Inspection and maintenance decisions and operations also proved seriously flawed. A pressure safety valve was removed and replaced by a blind flange assembly without proper tagging, thereby putting a pump out of service. The permit-to-work system failed; and there was no communication between the maintenance crews and the night operators, who were unaware that the pump was unavailable and tried to restart it. In addition, the inquiry concluded that, for a leak of that magnitude to develop, the assembly could not have been sufficiently tightened, and the quality of the work could not have been inspected. Finally, safety equipment inspection and maintenance seems to have been seriously defective.

Organizational Roots and Risk Management Measures

The decisions and actions that took place on Piper Alpha were influenced by fundamental organizational factors.[9,10,11] These factors, and the corresponding dependencies, are represented at the upper level of Figure 5. They can be divided into four categories: economic pressures that can result in questionable practices in production and safety management; personnel issues related, in part, to these economic pressures, a production culture, and deficiencies in learning mechanisms; flaws in the design guidelines and the design philosophy; and inspection and maintenance problems, including a deficient permit-to-work system.

Maintenance problems may have resulted, in part, from inadequate regulatory oversight in the United Kingdom. Such regulations should address fundamental organizational problems of three types. The first type is information: Do the personnel have the appropriate level of knowledge and access to relevant information? The second type is incentives and rewards: What are people actually rewarded for, and how can the incentive system accommodate the need for long-term safety? And the third type is resource constraints: What are reasonable time and budget pressures, and how much should be allocated to inspecting and maintaining safety features?

Most of these factors are rooted in financial constraints from the corporation, with emphasis on the short term. In the case of Piper Alpha, many decisions were made onboard under pressure to produce at the maximum level, to reduce design and construction costs (hence, a minimum deck surface), and to reduce production costs, often by cutting corners in inspection and maintenance operations. Such economic constraints are unavoidable. Yet, the tradeoff between immediate production levels and long-term probability and costs of a disaster seldom seem to be properly examined. The tendency is to focus on the immediate possibility of frequent incidents and to dismiss or ignore the risk of a catastrophe.

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

The risk management literature tends to recommend the creation of an independent safety function—for example, NASA conducted the investigation following the Challenger accident. In the United Kingdom at the time of the accident, a large part of the safety responsibility was in the hands of a dispersed set of government regulators. However, the British government was eager to accelerate the production of oil in the North Sea, and the safety of operations may not have been at the forefront of their concerns. Therefore, regulatory authorities overlooked important safety issues.[12]

Counting on external control and government regulators to discover problems and monitor their solution encourages an us-against-them mentality. A similar tension may actually exist inside a corporation, where relying on internal control for risk management encourages people to beat on the safety officer. Powerful safety divisions may be effective, provided they are given teeth and do not turn into convenient dumping grounds for the less productive. The strategy that keeps an operation knowledgeable and responsible may be better in the long run. Such a strategy assumes that the internal incentive system is not based solely on short-term production figures, but rewards long-term safety measures and punishes dangerous actions, as well. It also assumes that the production goals are set at a reasonable level and can accommodate contingencies.

The incentive system of the oil companies often relies on the performance of profit centers. The corporation may define profit centers somewhat arbitrarily by assessing, through internal pricing, the performance of each unit. Problems arise in the oil industry when production and refinery are structured into separate profit centers, leaving the production sector squeezed by fluctuations in the price of crude oil on the world market. Reducing the production costs is then the only way to maintain profit margins. This is often achieved by decreasing inspection and maintenance costs—for example, by delaying system repairs that are not immediately essential to production. Some of the major U.S. oil companies have apparently recognized this problem of organizational structure, but it remains a key issue elsewhere.

Economic pressures, in turn, directly affect corporate culture, personnel management, turnover, experience, and the process of learning from past mistakes and incidents. Within the oil industry, the priority given to short-term production has often created what is called a reverse-safety culture. Formal and informal rewards tend to encourage employees to push industrial systems to the limits of their capacities without sufficient precautions. In such systems, there are few incentives for checking that additional equipment and incremental "debottlenecking" do not stress existing equipment beyond their actual capacities, do not create dangerous couplings, and do not interfere with existing safety features.

Such concerns require a thorough understanding of the system, its complexities, and its interdependencies, based on experience. This knowledge is lacking when undertrained people are allowed to run a platform, for example, because the more experienced are on leave or have been fired in times of budget restrictions. In addition, stories of near-misses and minor incidents are often suppressed because they run counter to this culture and to a corporate image of success. As a result, the corporation fails to learn from past mistakes. Again, the fundamental problem is one of incentives, formal or informal, and of the culture that they promote.[13]

Some of the flaws in the design philosophy can also be linked to economic pressures that encourage development beyond that initially planned, often on a minimal deck surface. Others are related to a culture of denial of serious risks and to the failure to think through the possible consequences of incidents and the dependencies that may exist. Redundancies are particularly critical in functions of command and control, especially in the power supply and in fire protection equipment. Yet, safety equipment is sometimes considered extra baggage that gets in the way of higher production rates and consumes precious maintenance resources.

Proper design of redundancies and elimination of couplings often requires a formal risk analysis of the type proposed in this paper in order to examine explicitly the tradeoffs between costs and safety. Yet, such analyses are seldom performed. The design guidelines for deck layout are based on concepts of area-classification, where the goal is to separate the flammable vapors expected under normal operating conditions from ignition sources, particularly electrical equipment. These guidelines are designed to prevent fires. However, they do not require the separation of production modules and other units, such as living accommodations and the control rooms, which can be located anywhere, even in the process area. Furthermore, there are no specific fire criteria (similar to wave-load criteria) in the design of the structure and, therefore, no in-depth defense against sustained heat loads.[14] Fire protection relies exclusively on quick response, appropriate training, and properly functioning emergency systems—which are not available if they have been turned off or are left out of service, as was the case on Piper Alpha.

In such an environment, inspection and maintenance are critical. Unfortunately, economic pressures, periodic financial restrictions of the production sector, and procedures such as the permit-to-work system have proved detrimental to system safety. The permit-to-work system, investigated extensively in the Cullen report, did not ensure communications. Nor did there seem to be any concern about the dependencies created by simultaneously shutting off redundant equipment. In the U.K. sector of the North Sea, deficiencies in maintenance may be attributed, in part, to inadequate regulatory oversight. Elsewhere, they may simply be the results of a myopic approach to financial performance.

Probabilistic Assessment of Risk Management Measures

Most of the safety measures that can be envisioned to address such fundamental problems are costly, and the economic constraints of the oil and gas industry will remain. Yet, a number of safety measures must be implemented to reach a tolerable safety level and to control the enormous losses of potential catastrophes. It is thus important to assess the costs and benefits of different safety measures in order to set priorities.

One of the key elements of fire safety in any critical facility is the proper functioning of the fire pumps, which requires that enough redundancies exist and are not compromised by design flaws or poor maintenance. It is then useful to assess the fire risks involved in the current system, and then, the risk-reduction benefits of potential improvements. For illustrative purposes, I focus here on the system of emergency water pumps. The probabilistic risk analysis that yields the probability of system failure, given the state of its components, is a direct application of the classical method[15] and is described in Appendix 1.

However, fault tree analyses are static tools. 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 yields the probabilities of the different states after t time units.[16] The overall fire risk analysis model is thus a dynamic model that includes, in addition to this static probabilistic risk analysis for the pumps, a fire propagation model. This overall model applies to many other fire safety problems and allows one to make choices among policies involving physical systems, as well as procedures.

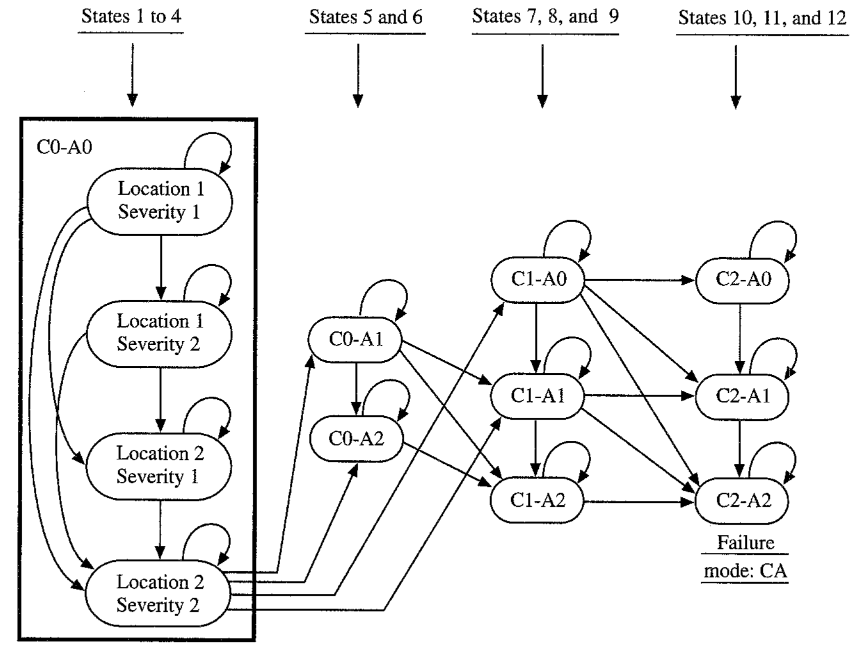
Consider, for example, one particular failure mode of the emergency water pumps, as described in Appendix 1: "Access routes are blocked by the fire," so there can be no manual pump activation, and "electric cables are destroyed by the fire," so the electric pump does not work. Assume that the cables and access routes are located close to each other. Assume also, for simplicity's sake, that the fire can start only in one particular location—Module 1—and at one of two levels of intensity. Low intensity is called Severity 1, while high intensity is called Severity 2. Finally, assume that the fire has to reach another location—Module 2, close to the emergency pumps—and the higher level of intensity, or Severity 2, 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 of Figure 6. The computations involved in this model are presented in Appendix 2. The Markov model yields the probability distribution of the time to failure of the water pumps through one particular failure mode, and the failure of both the electric cables and access to the manual pumps. Similar models can be developed for the other failure modes. It is clear from the logical analysis alone that the electric cables should not run along the access to the manual pumps. In addition, the Markov analysis yields the probability that this particular coupling will cause a catastrophic fire.

This analysis (and similar ones for the other nine failure modes, and possibly for some conjunctions of failure modes) allows us to assess the benefits of a number of safety measures. For each of the following examples, I identify the effects of the proposed measure on the model data. The model then yields the corresponding reduction of the probability that the fire pumps will become unavailable in a fire.

In the design phase, the fire pumps can be isolated by better layout or by reinforcing the pump area's fire protection. Given a fire, one wants to decouple the possible failures of the access to the manual pumps and the electric cables. The effect on the model data is to decrease the probabilities of transition between any state of the cables and the access routes and higher levels of fire severity.

In the operations phase, procedures can be enforced to forbid closing the water



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; index 1: minor fire damage but still functioning; index 2: damaged by fire, failure state.

Figure 6. Markov diagram and transition among states for the subsystem: access to water pump(s), A, and electric cables, C, feeding the electric pump(s).[2]

inlet; the divers can be protected through other means. The effect on our model is to decrease the probability of the failure mode "failure of water feed." One can also introduce human redundancy into the operation of the manual pumps by making sure that several individuals have access to, and can operate, the pumps. The effect is to decrease the probability of failure modes that involve an operator. One can also consider changing the policy that allows less experienced personnel to operate the platform. The effect is then to decrease the probability that a will fire start; the probability that a fire, once started, will reach Modules 2 and 3, where the emergency pumps are located; and the probability that no operator will be available should the automatic pumps fail to function. Finally, the maintenance procedures can be made more thorough or more frequent in order to decrease the probability of leaks in pumps and valves. The effect on the model data is to decrease the initial probability of fire and the probability that the fire will start at a high level of intensity.

The benefits of measures aimed at decreasing the probability of losing water pumps in a fire can be evaluated by assessing the contribution of fires and blasts to the overall probability of platform failure and assessing the contribution of emergency pump failure to the probability of losing the platform, given that a fire starts. Then, using our model, we can assess the contribution of each of the failure modes to the probability of an emergency pump system failure and compute 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 measures, and other measures aimed at decoupling the different parts of the system, produce multiple benefits because they reduce the probabilities of several failure modes. These benefits should thus be computed across the relevant failure modes. In particular, improvements of inspection and maintenance procedures can increase overall system safety by adapting the frequency and the extent of maintenance interventions to the loads and deterioration rate of each component. In some cases, a choice must be made between maintenance on-schedule and on-demand, and an expected-utility decision analysis can support this decision.[17,18]

Conclusions

The fire that destroyed the Piper Alpha platform resulted from technical failures rooted in organizational and management problems. Reducing the probability and the severity of such fires starts with improving the design in several ways—that is, modifying the layout, improving fire protection devices, and taking other measures aimed at decoupling the different parts of the system. Many of these measures produce multiple benefits because they reduce the probabilities of several failure modes.

The design guidelines must include severe accident criteria for fire protection of the structure itself, as well as a better configuration of the pipeline risers and safety valves, which have to be both accessible and protected.[19,20] The deck layout must adequately separate or insulate the different modules, and the living quarters should be located on a separate accommodation platform whenever feasible. The process of platform growth must be strictly controlled. Expansion should not take place unless provisions have been made for it in the design phase, so that added systems do not interfere with the safety of operations.

Preventing the recurrence of accidents similar to the fire that occurred on Piper Alpha in 1988 requires organizational improvements. In general, the burden of safety must be placed squarely on the oil companies. First, they must recognize that the probability of truly catastrophic fires is far from remote. Second, they must devise comprehensive risk management strategies, instead of providing minimal responses to regulatory requirements or equating risk management with insurance programs. Such a strategy includes a commitment to promoting a safety culture, to alleviating production pressures under hazardous circumstances, and to providing consistent incentives for accident prevention in the immediate and more distant future. In the production phase, risk reduction also requires improving inspection and maintenance, including the work-permit system, improving personnel safety and evacuation procedures, and improving platform network coordination and communications.

Given the costs of risk management, priorities must be set. Probabilistic risk analysis allows us to evaluate risk reduction benefits for specified platforms and safety measures, and, therefore, to optimally allocate risk management resources. In many cases, the computation can be limited to parts of the system. Once the results are available, corporate management must decide how to balance costs and benefits. Eventually, the final safety level and the residual risk should be the responsibility of the oil companies, not of government regulatory agencies.

References

1. Paté-Cornell, M. E., "A Postmortem Analysis of the Piper Alpha Accident: Technical and Organizational Factors," *Report No. HOE-92-2,* Department of Naval Architecture and Offshore Engineering, University of California, Berkeley, 1992.

2. Paté-Cornell, M. E., "Risk Analysis and Risk Management for Offshore Platforms: Lessons from the Piper Alpha Accident," *Journal of Offshore Mechanics and Arctic Engineering,* Volume 115, 1993a, pp. 179 to 190.

3. Paté-Cornell, M. E., "Learning from the Piper Alpha Accident: Analysis of Technical and Organizational Factors," Risk Analysis, Volume 13, No. 2, 1993b, pp. 215 to 232.

4. Paté-Cornell, M. E. and Fischbeck, P. S., "PRA as a Management Tool: Organizational Factors and Risk-Based Priorities for the Maintenance of the

Tiles of the Space Shuttle Orbiter," *Reliability Engineering and System Safety,* Volume 40, 1993, pp. 239 to 257.

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

6. Bea, R. G., Personal communication, 1991.

7. Cullen, The Hon. Lord, *The Public Inquiry into the Piper Alpha Disaster,* Volumes One and Two, Report to Parliament by the Secretary of State for Energy by Command of Her Majesty, November 1990.

8. Gale, W. E., Personal communication, 1991.

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

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

11. Paté-Cornell, M. E. and Bea, R. G., "Management Errors and System Reliability: A Probabilistic Approach and Application to Offshore Platforms," *Risk Analysis,* Volume 12, No. 1, March 1992, pp. 1 to 18.

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

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

14. Bea, R. G. and Gale, W. E., *Structural Design for Fires on Offshore Platforms,* NAOE Industrial Liaison Program Conference, University of California, Berkeley, 1990.

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

16. Paté-Cornell, M. E., "Fire Risks in Oil Refineries: Economic Analysis of Camera Monitoring," *Risk Analysis,* Volume 5, No. 4, 1984, pp. 277 to 288.

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

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

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

20. Adams, A., "Experience in Offshore Pipeline Management," *Proceedings of the International Workshop on Offshore Pipeline Safety,* D. V. Morris, Ed., New Orleans, Louisiana, December 4 to 6, 1991, pp. 34 to 43.

Acknowledgments

The original study on which this article is based was funded as part of a joint industry project entitled “Management of Human Error in Operations of Marine Systems,” headed by Professor Robert G. Bea in the Department of Naval Architecture and Offshore Engineering of the University of California, Berkeley. This article is based in large part (and at the request of the editors) on two articles on the same topic published in *Risk Analysis* and in the *Journal of Offshore Mechanics and Arctic Engineering*.

Appendix 1: Static Probabilistic Risk Analysis for the Emergency Fire Pumps

Notations

$fist_m$: final states of the different components (index *m:* three possible states: intact, partially damaged, totally failed)

$loss_k$: levels (indexed in *k*) of final losses

loc_l: location of fire start (indexed in l)

sev_j: level of initial fire (indexed in j)

The probabilistic analysis is done in four steps.

•First, a logical analysis of the functions involved and fault tree analysis are performed.

•Second, probabilistic analysis is performed on the different failure modes for the top event, which, in this example, is “failure of emergency pumping.”

•Third, probability of fire start and propagation to the location of the pumps and their accesses is computed using a Markov model. The final system’s state is described by the vectors $fist_m$. The probabilities computed here are those of the $fist_m$’s, in which the element corresponding to the emergency fire pumps indicates that they do not function.

•Finally, the risk reduction benefits of several types of measures are assessed by computing the contribution of the pumps in limiting overall fire losses. Examples of such measures include adding a second manual redundancy or adding protection against the effects of fires and blasts to the pumps.

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.

$$p(loss_k) = \sum_m \sum_l \sum_j \underbrace{p(fire) \times p(loc_1|fire) \times p(sev_j|fire, loc_1)}_{\text{fire initial state}} \times \underbrace{p(fist_m|fire, loc_1, sev_j)}_{\text{fire propagation}} \times \underbrace{p(loss_k|fist_m)}_{\text{final losses}} \tag{1}$$

The vector $fist_m$ represents the possible final system states, and the loss of the pumps may be one of its elements. Therefore, a key element of the probability $p\ (fist_m\ |fire,\ loc_l,\ sev_j)$ is the probability of fire pump failure. It can be analyzed by the classical PRA techniques,[15] starting with the simplified functional diagram shown in Figure 7. The function "water feed" is needed for both manual and automatic functions. The automatic pump requires that the power supply and electric cables are both functioning, and the electric pump itself must function. The manual pump requires that an operator is available, that the access has not been blocked, and that the pump itself functions. To simplify the diagram, we assume that the subsystem "manual pump" includes its own emergency electric supply.

The fault tree corresponding to the top event T = "the water pumps do not function" is represented in Figure 8. Each component's state is represented by a Boolean variable X. All values of X are defined in Figure 6; for example, C is

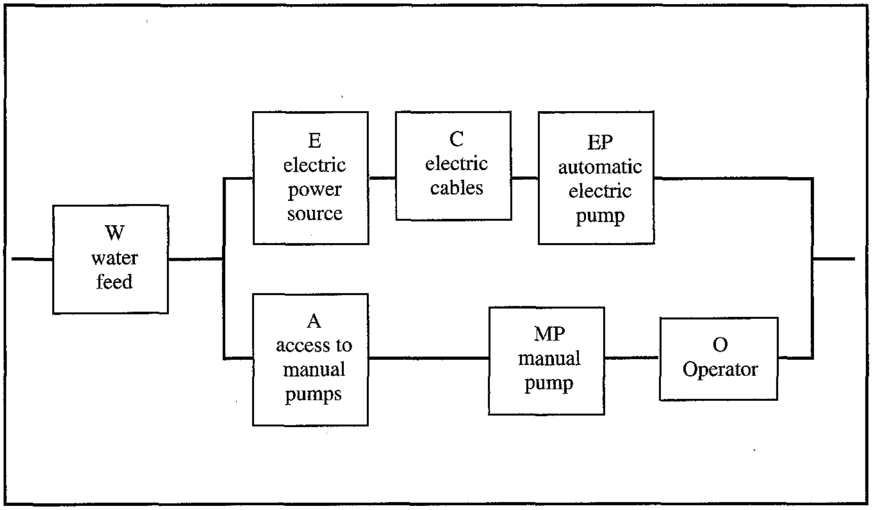


Figure 7. Functional diagram for the emergency water pumps.[2]

defined as state of the electric cables. X is equal to 1 if the corresponding element does not function, and to 0 otherwise. The Boolean polynomial corresponding to this fault tree is:

$$T = W + (E + C + EP) \times (A + O + MP) \tag{2}$$

Expansion of this polynomial yields the 10 failure modes of the pumps:

$$\begin{aligned} T = {} & W + E \times A + C \times A + EP \times A + E \times O + E \times MP \\ & + C \times MP + EP \times MP \end{aligned} \tag{3}$$

Thus, the probability of failure of the pumping function is

$$\begin{aligned} p(T) = {} & p(W) + p(E) \times p(A|E) + p(C) \times p(A|C) \\ & + p(EP) \times p(A|EP) + p(E) \times p(O|E) \\ & + p(C) \times p(O|C) + p(EP) \times p(O|EP) \\ & + p(E) \times p(MP|E) + p(C) \times p(MP|C) \\ & + p(EP) \times p(MP|EP) - \sum p\,(\text{two failure modes at a time}) \\ & + \sum p\ (\text{three failure modes}) \ldots \text{etc.} \end{aligned} \tag{4}$$

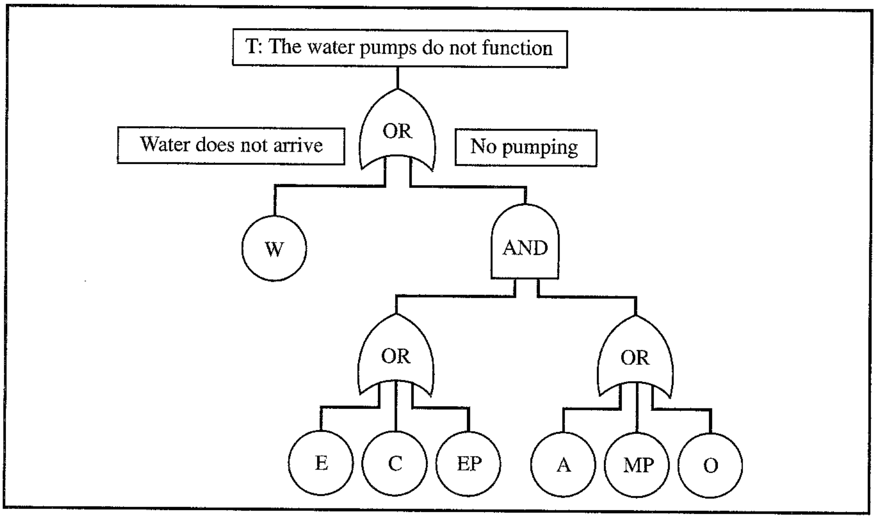


Figure 8. Fault tree for the top event, "the water pumps do not function."[2]

Given the strong dependencies introduced by the possibility of accident initiators such as fires, the probabilities that two or more failure modes will occur at the same time can be high. Therefore, these terms must be explicitly computed in Equation 4. An example of two failure modes at a time is the conjunction $E \times O \times EP \times A$ (failures of the electric power source, of the operator, of the automatic electric pump, and of the access to the manual pump).

Fire is one of the "common causes of failure" that can affect the probability of all 10 failure modes. The probability of losing the fire pumping function in a fire, event *F,* depends on the location 1 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 4 becomes:

$$\begin{aligned} p(T) &= p(F) \times p(T|F) \\ &= p(F) \times \sum_{l} \sum_{i} [p(W|F, loc_l, sev_j) \\ &\quad + p(E|F, loc_l, sev_j) \times p(A|F, E, loc_l, sev_j) + \ldots] \qquad (5) \end{aligned}$$

in which all the terms of Equation 4 are conditioned on the occurrence of a fire, its location, and its initial severity.

Equations 1 to 5 thus permit us to compute the probability that the emergency pumps have failed by a specified time *t,* given the state of the different components at that time.

Appendix 2: Dynamic Markov Model of Fire Risks

In Figure 6, *C* represents the state of the electric cables—*C0* meaning no damage, *C1* minor fire damage but still functioning, and *C2* failure due to fire—and *A* represents the state of the access to the manual pump—that is, 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 6. The final state *C2–A2* represents the failure mode $C \times A$ of the water pumps.

The Markov Chain

This Markov Chain has 12 states, numbered 1 to 12 by column in Figure 6. State 1 is *C0–A0,* Location 1, Severity 1. State 5 is *C0–A1.* State 7 is *C1–A0.* And state 12 is *C2–A2.* We assume here that the fire always grows and damages the two components *C* and *A* continuously, without jumps in severity levels. Human intervention is not modeled here explicitly. The probabilities of transition among states depend on fire fighting activities and on the availability of water—that is, whether the other failure modes of the emergency pumps have occurred before $C \times A$. Once the fire has reached Module 3, or 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 when a fire starts in Module 1.

$$P(O) = [p_O(1), p_O(2), 0, \ldots, 0] \tag{6}$$

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, such as 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 :[1]

$$P(t) = P(0) \times \Pi^t \tag{7}$$

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 $P_{12}(t)$. We can obtain the probability distribution and the mean of the time to failure of the water pumps through this particular failure mode.

This Markov model thus permits us to compute the probabilities of the different failure modes of the fire pumps within given time intervals after the start of a fire in a specified location.

Reference

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