Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organizational Factors

M. Elisabeth Paté-Cornell[1]

(Received September 18, 1992; revised October 22, 1992)

The accident that occurred on board the offshore platform Piper Alpha in July 1988 killed 167 people and cost billions of dollars in property damage. It was caused by a massive fire, which was not the result of an unpredictable "act of God" but of an accumulation of errors and questionable decisions. Most of them were rooted in the organization, its structure, procedures, and culture. This paper analyzes the accident scenario using the risk analysis framework, determines which human decision and actions influenced the occurrence of the basic events, and then identifies the organizational roots of these decisions and actions. These organizational factors are generalizable to other industries and engineering systems. They include flaws in the design guidelines and design practices (e.g., tight physical couplings or insufficient redundancies), misguided priorities in the management of the tradeoff between productivity and safety, mistakes in the management of the personnel on board, and errors of judgment in the process by which financial pressures are applied on the production sector (i.e., the oil companies' definition of profit centers) resulting in deficiencies in inspection and maintenance operations. This analytical approach allows identification of risk management measures that go beyond the purely technical (e.g., add redundancies to a safety system) and also include improvements of management practices.

KEY WORDS: Piper Alpha accident; offshore platforms; human error; organizational errors; postmortem analysis; probabilistic risk analysis.

1. LEARNING FROM THE PIPER ALPHA ACCIDENT

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.[1,2] Piper Alpha received and sent to the shore the oil and gas production of a group of platforms. The disaster caused the death of 165 men (out of 226) on board the platform itself, and two men on board a rescue vessel. From this disaster, much can be learned for future risk management, on other offshore platforms as well as in other industrial sectors. The lessons from Piper Alpha should allow a better assessment of the risks involved before other accidents occur and should point to a variety of technical and organizational risk management measures.

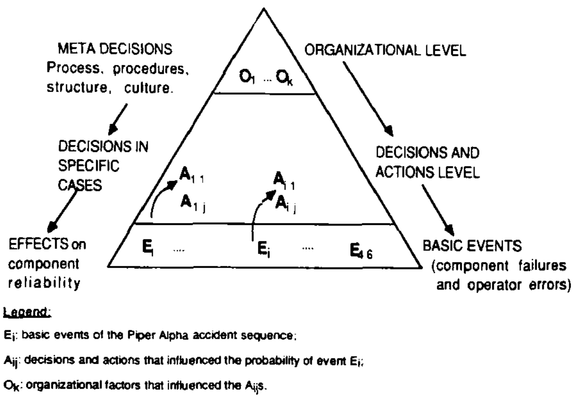
Risk analyses for offshore structures often focus on the probability that an extreme event (e.g., an extreme value of the wave load) exceeds the actual structural capacity. It was shown previously that this "bad luck" type of case constitutes only a small part of the overall risk of platform failures.[3,4] The Piper Alpha accident was one of the cases that can hardly be attributed to "an act of God": it was mostly self-inflicted. Although the coincidence of the final events that triggered the catastrophe was not in itself controllable, the failure resulted essentially from an accumulation of management errors. For example, a piece of equipment (a critical pump with one redundancy) had been turned off for repair and the night crew that operated the platform had not been informed of it. This problem, in turn, was mostly a failure of the "permit-to-work system" that did not ensure proper communications. Things would have not taken catastrophic proportions, however, if the deluge systems had operated properly and/or if the platform had not been "decapitated" at the onset of the accident both technically (the control room was located on top of the production module) and organizationally (the Offshore

[1] Department of Industrial Engineering and Engineering Management, Stanford University, California 94305.

Installation Manager died in the accident). Furthermore, the design of the facility did not include sufficient protection of the structure against intense fires, nor redundancies and appropriate "decoupling" of the safety systems.

From a risk assessment perspective, learning from the Piper Alpha accident involves first understanding the different factors that led to this tragedy and, second, updating the probabilities of the different elements of the actual failure mode that occurred. This paper addresses the first issue by using the risk analysis framework and its extensions to management factors in order to capture the deeper levels of causality that led to the basic events of the failure mode (Fig. 1). First, the elements of the accident sequence (noted E_i) are systematically identified based on the two major inquiries that followed the accident.[1,2] Second, for each of these basic events, the human decisions and actions (noted A_{ij}) that have influenced their occurrences are described. Third, the organizational roots of these "human errors" or questionable actions are explored.[5,6] The objective of this analysis is not to identify the culprits but rather to point to risk reduction measures that go beyond the purely technical (e.g., add a redundancy to the fire protection system) to also include organizational improvements (e.g., make sure that the profit center structure of the corporation does not provide direct incentives to cut corners in maintenance operations of the production sector).

The case of the Piper Alpha accident is particularly interesting for several reasons. First, its severity was such that it could not be (and it not being) ignored by the oil and gas industry worldwide, where a certain number of measures are currently implemented based on this event.[7] Second, it is generalizable to many other industries and industrial processes: denial of the risk, unrecognized (and unnecessary) couplings in the design, insufficient redundancies in the safety systems, difficulties in managing the tradeoff between productivity and safety, and a tendency to stretch maintenance operations when production pressures increase are all problems common to many industrial facilities.[8] Learning from Piper Alpha using a risk assessment model structure can thus be the first step toward improving and updating risk management models for similar platforms and other industrial plants. Such models, in turn, allow assessment of the cost-effectiveness of the different safety measures that can be envisioned based on this experience.[9,10]


META DECISIONS
Process, procedures, structure, culture.
DECISIONS IN SPECIFIC CASES
EFFECTS on component reliability
ORGANIZATIONAL LEVEL
DECISIONS AND ACTIONS LEVEL
BASIC EVENTS (component failures and operator errors)
O_1 ... O_k
A_{11}
A_{1j}
A_{i1}
A_{ij}
E_1 ....
E_i ....
E_{46}

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.

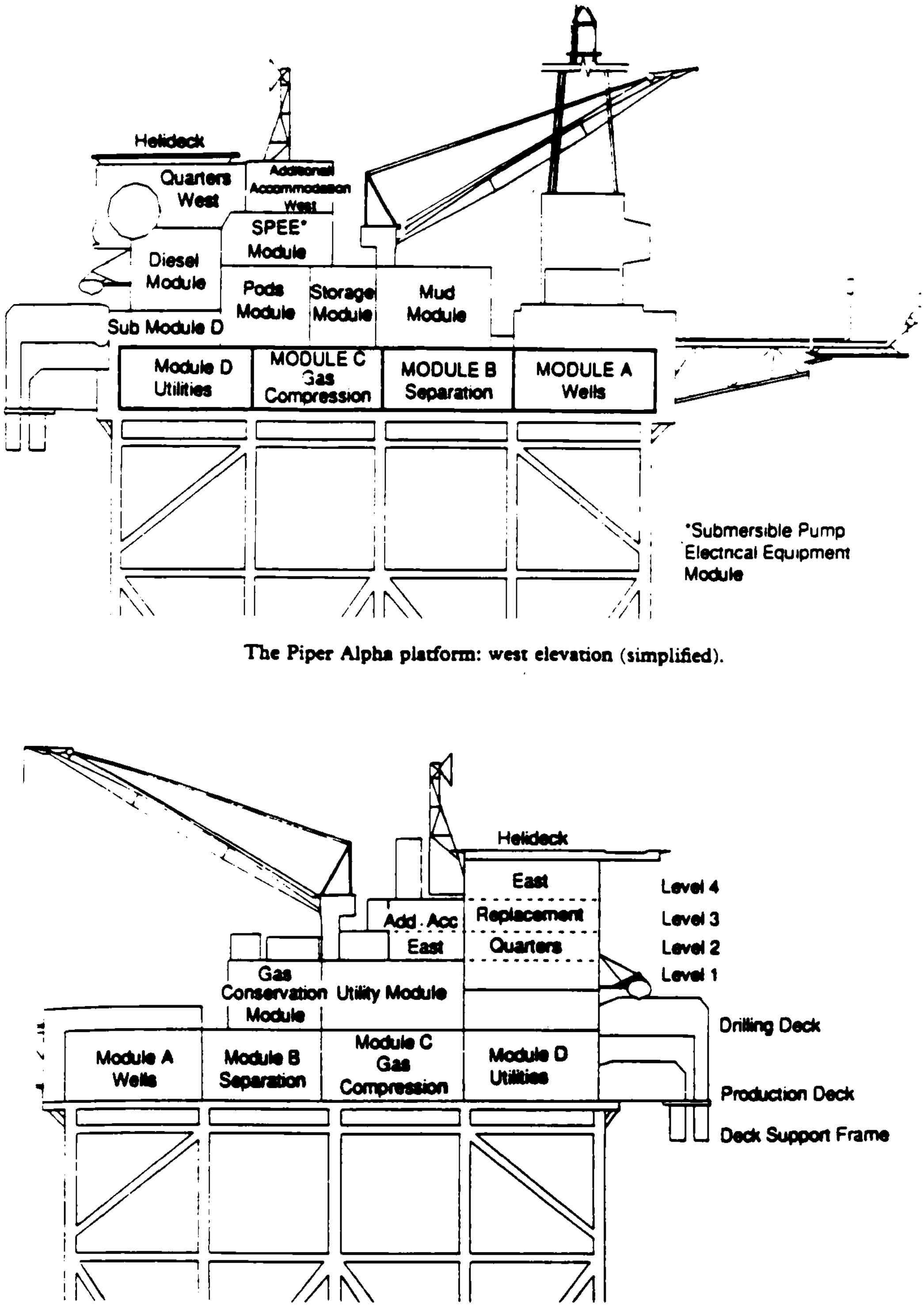
Fig. 1. Hierarchy of root causes of system failures: management decisions, human errors, and component failures.[4].

2. THE ACCIDENT AND THE FAILURE PATH

The accident 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 B and C to critical centers, and to destroy the control room and the radio room in the early stages of the accident (Fig. 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 ordered, 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, all in the same location, were mostly inaccessible. The fire fighting equipment on board could not be operated because the diesel pumps, which had been put on manual mode, were inacessible and seem to have been damaged from the beginning. Fire boats were at hand, but waited for orders from OIM 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 $3 billion (U.S.).[6]

The risk analysis model structure[2] is the basic analytical tool to identify the "failure path" or accident sequence that occurred on Piper Alpha including: (1)

[2] There is no attempt here to assess after the fact the probability of the Piper Alpha accident because, at this stage, it is a moot point (the accident has already occurred). Also, the probability of such an accident could be made arbitrarily small by controlling the level of detail in which the accident is described. For similar platforms and for a well-defined class of accidents, however, this study is the first step toward an improved PRA.



The Piper Alpha platform: west elevation (simplified).

The Piper Alpha platform: east elevation (simplified).

Fig. 2. The layout of Piper Alpha.[1]

initiating events, (2) intermediate developments and direct consequences of these initiating events, (3) final systems' states, and (4) consequences (i.e., the losses of the accident). The basic events of the failure mode and the dependencies among them are presented in the influence diagram of Fig. 3. This *post facto* failure mode identification excludes secondary events that may have promoted the basic events but are not part of the failure

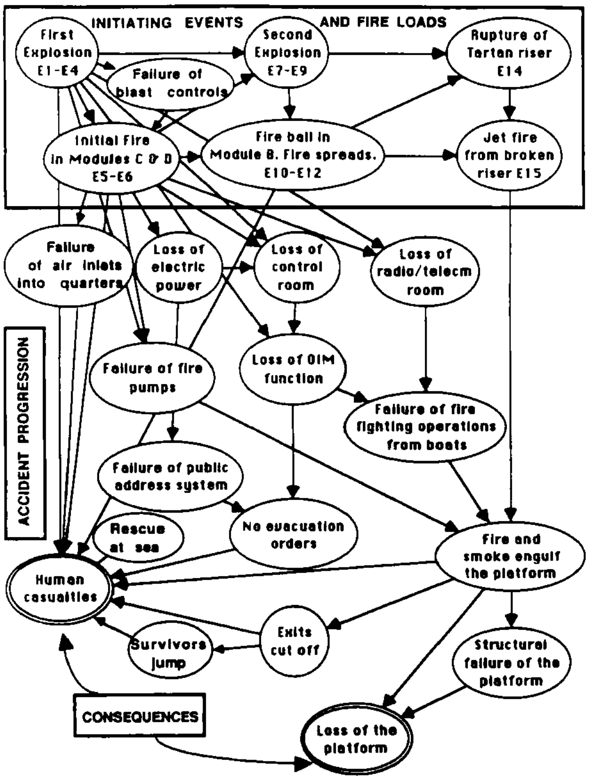

INITIATING EVENTS AND FIRE LOADS
First Explosion E1-E4
Failure of blast controls
Second Explosion E7-E9
Rupture of Tartan riser E14
Initial Fire in Modules C & D E5-E6
Fire ball in Module B. Fire spreads. E10-E12
Jet fire from broken riser E15
Failure of air inlets into quarters
Loss of electric power
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

Fig. 3. Event dependencies in the Piper Alpha accident scenario (influence diagram representation).[4]

mode—for example, the error made earlier in the fitting of the blind flange. Note that the labeling of the basic events (E_is) has been chosen for analytical purposes and does not imply a chronolgical order; for example, the iniating events and the major loads (fires and explosions) have been separated from their consequences. References to the investigations described in the Cullen Report[1] and the Petrie report[2] include the specific sections of these detailed documents. 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.

Initiating Events (IE): Major Explosions and Fire Loads

A. Primary initiating event (IE_1): First explosion. July 6, 1988, 21:58.

- E_1: Process disturbance (21:45 to 21:50).
- E_2: Two redundant pumps inoperative in module C: condensate pump "B" trips; the redundant pump "A" was shut down for maintenance.
- E_3: Failure of a blind flange assembly at the site of Pressure Safety Valve 504 in Module C.
- E_4: Release of condensate vapors in module C (~45 kg, filling ~25% of the module volume); failure of gas detectors and emergency shutdown.
- E_5: First ignition and explosion. Possible ignition sources include hot surfaces, broken light fitting, electrostatic sparks, and electric motors (Ref. 1, p. 60).
- E_6: Almost total failure of gas detectors and fire detection/protection (deluge) systems.
- E_7: Partial (almost total) failure of the emergency shutdown system.
- E_8: Failure of C/D fire wall. No blowout panel to contain explosion inside the module. Failures of the emergency shutdown and of the deluge system (E_6 and E_7) and failure of containment function (E_8) led to further explosions.

B. Secondary initiating event (IE_2): Second explosion. Propagation of the fire to module B. (Almost immediately, i.e., shortly after 22:00.)

- E_9 : Rupture of B/C fire wall (single layer, 4.5 hr integrity wall).
- E_{10}: Rupture of a pipe in module B (projectile from B/C fire wall).
- E_{11}: Large crude oil leak in module B.
- E_{12}: Fireball and deflagration in module B.
- E_{13}: The fire spreads back into module C through a breach in B/C fire wall.
- E_{14}: The fire spreads to 1200 barrels of fuel stored on the deck above modules B and C.

C. Tertiary initiating event (IE_3): Jet fire from broken riser (22:20).

- E_{15}: Failure of fire pumps: automatic pumps have been turned off; manual (manually started, diesel powered) pumps in module D are damaged by failure of C/D fire wall.
- E_{16}: Rupture of riser (Tartan to Piper Alpha) caused by pool fire beneath it (E_5,E_{12}, E_{13}); "high temperature reducing the pipe steel strength to below the hoop stress induced by internal pressures" (Ref. 1, p. 133).
- E_{17}: Intense impinging jet fire under the platform.

Further Effects of Initiating Events and Final Subsystems' States

A. From IE_1 (consequences of first explosion).

- E_{18}: Immediate loss of electric power.
- E_{19}: Failure of emergency lighting.
- E_{20}: Failure of the control room (no lights on mimic panels).
- E_{21}: Failure of the public address/general alarm system.
- E_{22}: Failure of the radio/telecommunication room.

E_{23}: Loss of the OIM function, both on board and as OSC of rescue operations.

E_{24}: The smoke prevents the Tharos helicopter from reaching the helideck.

E_{25}: Fire and smoke envelop the North side of the platform.

E_{26}: Casualties in A, B, C modules.

E_{27}: Escape of some people from 68 ft level to 20 ft level; some jump into the sea.

B. From IE_2 (consequences of second explosion).

E_{28}: Fire from modules B and C spreads to various containers ("lubricating oil drums, industrial gas bottles: oxygen, acetylene, butane").[2]

E_{29}: Fire from modules B and C causes rupture of pipes and tanks.

E_{30}: Some survivors jump into the sea from 68 ft and 20 ft levels.

E_{31}: Some people are engulfed in smoke and die in the quarters (22:33).

E_{32}: Partial failure of Tharos fire-fighting equipment.

C. From IE_3 (consequences of the jet fire).

E_{33}: Rupture of the MCP-01 riser at Piper Alpha.

E_{34}: Most people remain and are trapped in living accomodations.

E_{35}: Third violent explosion (22:52).

E_{36}: Some survivors jump from the helideck (175 ft level).

E_{37}: Collapse of platform at 68 ft level below B module (22:50).

E_{38}: Collapse of western crane from turret (23:15).

E_{39}: Fourth violent explosion (23:18); rupture of Claymore gas riser.

E_{40}: Major structural collapse in the center of the platform.

E_{41}: Slow collapse of the north end of the platform.

E_{42}: Collapse of the pipe deck, White House, and OPG workshop (additional casualties).

E_{43}: Accomodation module overturned into the sea (AAW north end of platform) (00:45).

E_{44}: Rescue of survivors at sea (throughout the accident) by on-site vessels.

Losses

E_{45}: Human casualties: 167 (165 men on board; 2 rescue workers).

E_{45}: Loss of the platform; damage in excess of \$3 billion (U.S.).

3. DECISIONS AND ACTIONS SPECIFIC TO PIPER ALPHA

3.1. Human Actions Linked to Basic Events of Piper Alpha Accident

Each of these basic events have been influenced by a number of decisions and actions. 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. At least some of these conjunctions could have been anticipated. The decisions and actions A_{ij} are labeled according to the phase where they occurred: design (DES), construction (CONST), operation (OP), and more specifically, maintenance (OPM).

E_1: Process disturbance around 21:45

E_1 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:

$A_{1.1}$: Decision to produce in the Phase 1 (high-pressure level) mode (OP).

$A_{1.2}$: Physical and managerial interdependencies in the platform network (DES; CONST).

$A_{1.3}$: Decision to promote personnel to critical positions on a temporary basis (OP).

$A_{1.4}$: Missed signals (OP).

$A_{1.5}$: Lack of redundancies in the design of trip signals (DES).

Phase 1 production mode was not common on Piper Alpha. It occurred because, at the time of the accident, the gas driers essential to Phase 2 operations had been shut down and isolated for routine maintenance (Ref. 2, 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 (Ref. 2, 4.2.4.2)) which was 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.[1] The network had apparently grown in an unpreplanned manner as the system was developed and constructed over time to accommodate 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 toward 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 equipment on 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 (Ref 2, 8.1.2). Sufficient 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 could operate the platform). The members of the production management team had been promoted one level above their normal position (Ref. 2, 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 (e.g., the fact that the southwest flare was roaring and larger than normal) and "the control room operator did not check which heads were detecting gas prior to the explosion" (Ref. 2, 5.14.1). Furthermore, in Phase 1, there was insufficient redundancy in the signals of alarm (i.e., one single trip signal) (Ref. 2, 10.1.4).

E_2: 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 (hence, an 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 (Ref. 2, 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 a 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 (Ref. 2, 8.3.2.12). This failure can be traced back to the work permit system (Ref. 1, Chapter 11) and is discussed further.

E_3: Failure of the blind flange assembly at the site of PSV 504

$A_{3.1}$: 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 (Ref. 1, 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.

E_4: Undetected release of condensate vapors in module C

$A_{4.1}$: Faulty 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 45 kg 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 caused real ones to be ignored and, second, there were read out problems in the control room (Ref. 2, 5.14) that were due to the design of the panels, and perhaps to the actions of the operator.

E_5: First ignition

$A_{5.1}$: Possible error of detection of potential ignition source (OPM).
$A_{5.2}$: Poor design of control mechanisms: spark arrestors and deluge system (DES).

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. Electrostatic 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 could have prevented ignition. An effective, explosion-resistant and properly maintained deluge system may have prevented the fire from spreading in its initial phase.

E_6,E_7: Failure of gas detectors, fire protection (deluge), and emergency shutdown systems

$A_{6\text{-}7.1}$: Design of the Main Control Room (location of the detector module rack) (DES).
$A_{6\text{-}7.2}$: Failure of operator to check origin of gas alarms from detector module rack (OP).
$A_{6\text{-}7.3}$: Design of the low-gas alarm system (DES).
$A_{6\text{-}7.4}$: Design of the gas detection system: couplings to the electric power system (DES).
$A_{6\text{-}7.5}$: No automatic fire protection upon gas detection in west half of module C (DES).
$A_{6\text{-}7.6}$: Lack of redundancy in the fire pumps (DES; OP).
$A_{6\text{-}7.7}$: Deluge system of limited effectiveness (DES).
$A_{6\text{-}7.8}$: Failue to upgrade some safety functions to Phase 1 mode (DES; CONST; OP).

Prior to the initial explosion, gas alarms were received in the main control room; but because of 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 (Ref. 2, 5.14). 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. 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 (e.g., at the site of the riser from Tartan). In module C, the fire deluge system had experienced repeated clogging and was inoperable (Ref. 1, 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 and some safety features (e.g., the automatic trip mechanism) may not have been fully adapted to accomodate the pressures of Phase 1.

E_8, E_9: Failure of the C/D and B/C fire walls

$A_{8\text{-}9.1}$: No blast control panels; fire walls with little resistance to blast pressures (DES).

Fire walls and blast walls have different characteristics, and blast walls may cause new problems by creating projectiles if and when they finally break. However, fire and blast containment systems on board Piper Alpha were generally insufficient (Ref. 1, 66; Ref. 2, 9.4.15). In particular, the blowout (side) panels were ineffective.

E_{10},E_{11}: Pipe rupture in module B and large oil leak

$A_{10\text{-}11.1}$: Couplings in the design of the modules (insufficient space separation) (DES).
$A_{10\text{-}11.2}$: Couplings due to poor protection against fire propagation (DES).
$A_{10\text{-}11.3}$: Insufficient protection of critical equipment against blast projectiles (DES).

The propagation of the accident at this stage involves general problems of layout, separation and couplings: tight space, and insufficient blast 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 attenuate coupling problems.

E_{12}, E_{13}: Fire ball in module B that spreads back into module C

$A_{12\text{-}13.1}$: Poor fire insulation (DES).

The spreading of the fire at this point cannot 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 adjacent ones.

E_{14}: 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.

E_{15}: Failure of diesel power fire pumps

$A_{15.1}$: Poor design of the manual fire-fighting system (DES): bad location, no redundancy, and poor protection of the pumps against fires and blasts.
$A_{15.2}$: 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 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.

E_{16}, E_{33}, E_{39}: Rupture of the risers, first from Tartan, then from MCP-01 and Claymore

$A_{16\text{-}33\text{-}39.1}$: No fireproofing of the riser connection (DES).

$A_{16\text{-}33\text{-}39.2}$: Poor design of the deluge system (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 failure 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.

E_{17}: 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 fire severity (and optimism) on other platforms (OP).

$A_{17.5}$: To some extent: the decision to continue production on Tartan (communication problems; insufficient procedures and enforcement of existing procedures) (DES; OP).

The decision to continue production on the other platforms even though there were clear and visible signs of a severe condition on Piper Alpha (and even to increase the pressure as it was beginning to drop in order to maintain production) may not have considerably worsened the situation 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 Alpha and ordered production to stop (Ref. 1, 133); but on Claymore, insistance on maintaining pipeline pressure and optimism about the capabilities of containing the fire on Piper Alpha against all signals to the contrary led the OIM to 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.

E_{18}, E_{19}: Immediate loss of electric power; failure of emergency lighting

$A_{18\text{-}19.1}$: Design error: decision to run the cable route through module D (DES).

$A_{18\text{-}19.2}$: Inadequate redundancies in the electric power system (OPM).

$A_{18\text{-}9.3}$: Lack of inspection and maintenance of emergency generators (DES).

Loss of electric power can be one of the most devastating accident initiators if there is not adequate redundancy in the system since many emergency features require electricity (on offshore platforms as in nuclear power plants and many other systems). In this case, the cable routes were running through one of the most vulnerable of the production areas without adequate redundancy (Ref. 1, 4.3.6). After the main generator tripped, the emergency generator did not start. The drilling generator started, then failed. A few batter-activated systems functioned for a while. The emergency lighting functioned briefly, then failed.

E_{20}: 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 command and control (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.

E_{21}: Failure of the public address system

$A_{21.1}$: Design of public address system; no redundancy for loss of electric power (DES).

The public address system was entirely dependent on electricity; couplings among the backups of electric power supply caused a power failure; therefore, there was no sound.

E_{22}: 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 Alpha 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).

E_{23}: Loss of the OIM function

$E_{23.1}$: 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, in particular evacuation orders that could have saved many lives (Ref. 1, 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 behond procedures that could not apply and of ordering an improvised evacuation. The technical decapitation of the system was compounded by an organizational decapitation as no one took charge except the personalities that emerged as leaders.

E_{24}, E_{25}, E_{28}, E_{29}, E_{31}: Fire and smoke spread throughout the platform

$A_{24\text{-}25\text{-}28\text{-}29\text{-}31.1}$: Layout decisions; lack of physical separation (DES).
$A_{24\text{-}25\text{-}28\text{-}29\text{-}31.2}$: Equipment design; insufficient fire proofing and smoke filters (DES).

A combination of lack of fire-fighting capabilities and design decisions that allowed fire propagation across modules and components caused the fire to spread to utility modules and escape routes, and the smoke to fill the living accomodations.

E_{32}: Ineffectiveness of the Tharos in fighting the fire

$A_{32.1}$: Delay in the decision of the Tharos master to take charge as OSC in time (OP).
$A_{32.2}$: Failure of the Tharos fire-fighting equipment (DES; OP).

The semisubmersible 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 personnel 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 nonfunctional.[1]

E_{26}, E_{30}, E_{34}, E_{36}, E_{44}: Casualties on board; escape and rescue of survivors

$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.1}$: Design/planning of evacuation routes (lack of redundancies) (DES).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.2}$: Failure of the OIM to give evacuation orders (OP).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.3}$: No alternative official authority when OIM is incapacitated (OP).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.4}$: Individual initiatives to escape and jump off against previous information about survivability of jumping in the sea from more than 60 ft. (OP).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.5}$: Poor training for evacuation (OP).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.6}$: Failure to properly locate, install, and inspect emergency exit equipment, rafts, and boats. Poor location of the lifeboats; no redundancy (DES; OPM).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.7}$: Failure to properly inspect and maintain inflatable rafts (OPM).
$A_{26\text{-}30\text{-}34\text{-}36\text{-}44.8}$: 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 TEMPSC's (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 (Ref. 1, p. 163). As in many emergency situations, leaders emerged, 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 accomodation 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 68 ft 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 (Ref. 1, p. 158). At least one life raft could not be inflated (it may not have 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 lifeboats around the platform (Ref. 2, 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 two in rescue operations.

E_{37}, E_{38}, $E_{40\text{–}43}$. Structural failures and collapse of the structure

$A_{37\text{-}38\text{-}40\text{-}41\text{-}42\text{-}43.1}$: No specific fire load provisions in design of structure (DES).

$A_{37\text{-}38\text{-}40\text{-}41\text{-}42\text{-}43.2}$: Decision to ignore early warning that the platform could not sustain severe fire loads for more than 10 min.

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. This bad judgment was based on an error of reasoning and, apparently, a wrong assumption of independence in the successive failure events.[3]

3.2. Classification of the Decisions and Actions That Contributed to 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 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 organization decapitation of Piper Alpha at the onset of the accident. The human errors, questionable decisions, and bad judgments that have been identified above and contributed to the accident can therefore be divided into four categories: (1) design decisions; (2) production and expansion decisions; (3) personnel management; and (4) inspection, maintenance, and correction of detected problems.[4]

3.2.1. 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 linked to power generation); (2) high probability 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 features had simply been neglected in the design.

The overall design of the network of platforms (Piper Alpha, Claymore, Tartan, MCP-01) made them physically interdependent without providing sufficient management integration both for production decisions that

[3] Occidental management had been warned by Elmslie Consultancy Services that a prolonged high-pressure gas fire would have grave consequences for the platform and its personnel (Ref. 1, p. 227); but it had been concluded at a subsequent meeting that "[the probability of the event] was so low that is was considered that it would not happen" (Ref. 1, pp. 228–229).

[4] It should be noted that some of these decisions (e.g., design decisions) were considered acceptable at the time and conformed to the existing codes and practices of the industry. It is these codes and common practices that are questioned below and need improvement.

affected operations on other platforms and for coherent and quick decisions in case of emergency. The general layout of Piper Alpha was questionable because of lack of redundancies, unnecessary complexities (e.g., storage of fuel on the deck), and excessive compactness. 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 lifeboats, 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 the 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 shutdown, 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.[1] 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 heat 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 (Ref. 1, p. 228). Indeed, prevention of small and frequent accidents is, in the short run, more cost-effective. However, backing up judgments regarding rare and serious events requires an in-depth 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" (Ref. 1, p.3).

3.2.2. 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 (Ref. 2, 3.1.6, 3.1.7); the living quarters were designed to accomodate 135 persons.[11] The platform was completed in 1976. It reached a peak production of about 320,000 barrels per day in 1979. 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 the addition of equipment, 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."[11] Other modifications included the addition of a produced water facility in 1980, of supplementary living quarters, installation of oil lift pumps, etc. (Ref. 2, Annex B).

Although the structure itself was reinforced in 1979, the deck surface was fixed and the result of unpreplanned additions was an extremely packed space. Not only additional components were stacked, thus creating new couplings, but also, the recordkeeping of these additions was inadequate: it was not even clear what was on board and where at the time of the accident.[6] 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.[6] At the end of this growth process, the situation on Piper Alpha was described by Bea[6] 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 1 hr 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.

3.2.3. 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 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 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 and a clear line of authority become more crucial.[12] 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 and properly estimates their probabilities. In this respect, there is a general tendency toward denial, which for Piper Alpha occurred with the rejection of prior information that indicated a very real danger of a serious fire.

3.2.4. Inspection and Maintenance Decisions

Inspection on Piper Alpha appears after the fact to have 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 inquiry concluded that for a gas 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 (Ref. 1., pp. 193–194).

4. ORGANIZATIONAL ROOTS OF DECISIONS SPECIFIC TO PIPER ALPHA

The decisions, human errors, and questionable judgments that contributed to the Piper Alpha accident can be in turn related to a certain number of basic 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 British government authorities.[5]

Key organizational factors that are at the root of the decisions identified in the previous section are the following: (1) questionable judgment in the management of productivity vs. safety; (2) flaws in the design philosphy and the design guidelines; (3) problems of personnel management; and (4) insufficient attention to maintenance and inspection (see Fig. 4). All of these involve questions of information (Do the personnel have appropriate levels of knowledge? 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, procedures that allowed cutting corners, and a culture that encouraged flirting with disaster.[5] Once again, the conditions described here may not have existed in July 1988 in other

[5] For example, the temptation to shut down gas alarms and deluge systems. This tendency 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" reassigned[6].

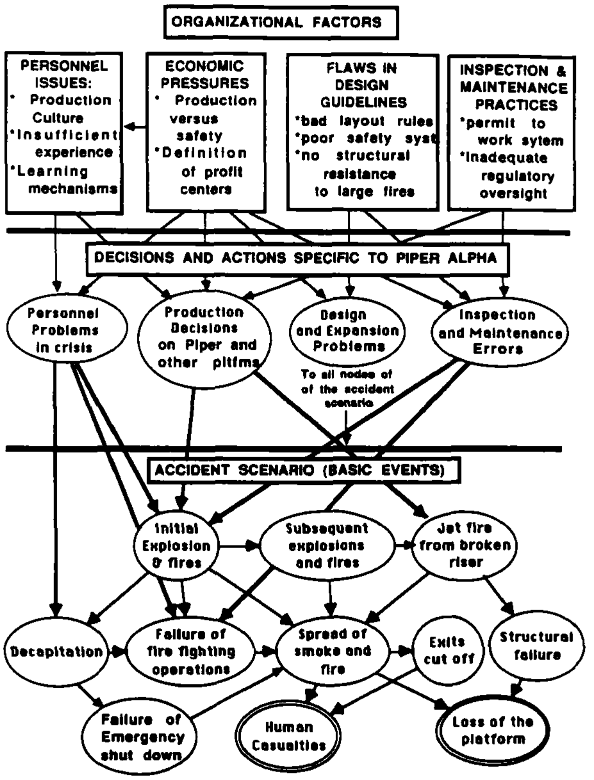

ORGANIZATIONAL FACTORS
PERSONNEL ISSUES:
• Production Culture
•Insufficient experience
•Learning mechanisms
ECONOMIC PRESSURES
• Production versus safety
•Definition of profit centers
FLAWS IN DESIGN GUIDELINES
•bad layout rules
•poor safety syst
•no structural resistance to large fires
INSPECTION & MAINTENANCE PRACTICES
•permit to work sytem
•Inadequate regulatory oversight
DECISIONS AND ACTIONS SPECIFIC TO PIPER ALPHA
Personnel Problems in crisis
Production Decisions on Piper and other pltfms
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 shut down
Human Casualties
Loss of the platform

Fig. 4. 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 Fig. 3).[4]

oil companies and may or may not exist at this time in particular oil companies.

4.1. The Management of Production vs. Safety

There is no golden rule for managing the productivity vs. safety trade-off. The desirability of a particular safety measure is the result of: (1) 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., Ref. 13) 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.

4.1.1. 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 toward 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. 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.

4.1.2. A "Reverse Safety Culture"

A safety culture is generally defined by a clear understanding of the system and its safety features, a positive attitude toward safety measures, and an incentive system that encourages safety in operations.[14] 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 flow rates 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.

However, pushing the envelope without disaster requires understanding the consequences. This is not the case when: (1) operators, production engineers, and/or system designers are not aware of all the dependencies of a naturally complex system; (2) undertrained and underexperienced people are allowed to run the operations; and (3) negative experiences and stories of near-misses and incidents tend to be ignored and suppressed because 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 inquiry 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) vs. "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.

4.1.3. The Role of Government and Safety Regulations

Before the Piper Alpha accident, Carson[5] had already pointed out that the British government, eager to benefit from 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.[6] Furthermore, in their guidelines, the approach of these government 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 task of the offshore operators who simply had to show that they satisfied the requirements. 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 (Ref. 1, 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 United Kingdom and the United States.[7] 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 United Kingdom, regulation had to change emphasis in its scope, and focus on the result (actual safety) rather than on the details.[7] 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.

4.1.4. Separation vs. 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,[15] 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

[6] Carson[5] 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).

[7] According to the U.S. Coast Guard, this situation is evolving in the United States, where industry and the Coast Guard have been working together for 2 years on revisions of OCS regulations.

and punishing dangerous actions. Governments (in the United Kingdom as well as in the United States) 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.

4.1.5. 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.[6] 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 nonimmediate 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 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.

4.2. Flaws in the Design Philosophy

4.2.1. 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 disastrous. Even if the number of backups is specified, the safety gains will depend, in the end, on the robustness of the equipment 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 shutdown, the public address, and the general alarm systems that are designed for these very circumstances. Finally, lack of redundancies in the lifeboats (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 shutdown, 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. Moreover, of course, once installed, these backups must be regularly inspected and maintained, even if they are seldom called upon.

4.2.2. Flaws in Some of 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.[16] In the United States, 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 nonsparking. 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 United States, 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.

4.2.3. Later Modifications and Unpreplanned 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, unpreplanned 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 the 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.

4.2.4. Lack of Specific Fire Criteria in Design of Structure

Fire risk is accounted for, in the design of the topside, by trying to prevent (as described above) the coexistence of vapors and ignition sources, and by providing means of fire-fighting. Fire protection thus relies on fire pumps, water spray and deluge systems, resistive coatings, and steel fire-proofing.[8] Fire loads, however, are not directly accounted for in the design of the structure[(17)] 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 for 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.

4.3. Problems of Personnel Management

4.3.1. 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,

[8] Beyond design issues, fire safety also involves fire training, securing, and evacuation.

however, did not guarantee that appropriate experience was available when needed. Furthermore, there seemed to be inadequate redundancy in human functions, at the level of the OIM as well as in the supervision of the production and maintenance crews.

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. In particular, a platform network has to be able to operate safely in situations of distributed decision-making, especially in the case of a catastrophic fire. 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 costs are implemented.

4.3.2. 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 (Ref. 1, 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.

4.4. Insufficient Attention to Maintenance and Inspection

4.4.1. Deficiencies of the Permit-to-Work System

The permit-to-work system is described in detail in the Cullen report (Ref. 1, Chap. 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" (Ref. 1, 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" (Ref. 1, 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 shortcuts to alleviate the load. If that is the case, the procedures should be streamlined and simplified so as to remove the source of the problem.

4.4.2. 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.[9]

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,

[9] Carson[5] discusses 13 cases of serious safety violations of the North Sea oil industry that reached the British 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" (Ref. 5, p. 251).

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.[5] 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.

5. 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 pressures. Measures that are then taken to save money in the short term have 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 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 neglect of the 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.

ACKNOWLEDGMENTS

This study was funded as part of a Joint Industry Project entitled "Management of Human Error in Operations of Marine Systems," headed by Robert G. Bea of the Department of Naval Architecture and Offshore Engineering of the University of California at Berkeley.

REFERENCES

1. The Hon. Lord Cullen, *The Public Inquiery into the Piper Alpha Disaster,* Vols. 1 and 2 (Report to Parliament by the Secretary of State for Energy by Command of Her Majesty, November 1990).
2. J. R. Petrie, "Piper Alpha Technical Investigation Interim Report" (Department of Energy, Petroleum Engineering Division, London England, 1988).
3. M. E. Paté-Cornell, "Organizational Aspects of Engineering System Reliability: The Case of Offshore Platforms," *Science* 1210–1217 (1990).
4. M. E. Paté-Cornell and R. G. Bea, "Management Errors and System Reliability: A Probabilistic Approach and Application to Offshore Platforms," *Risk Analysis* **12,** 1–18 (1992).
5. W. G. Carson, *The Other Price of Britain's Oil: Safety and Control in the North Sea* (Rutgers Universtiy Press, New Brunswick, New Jersey, 1982).
6. R. G. Bea, Personnal communications (1991).
7. The Institute of Marine Engineers, "Offshore Operations Post Piper Alpha" (Proceedings of the February 1991 Conference, London, England, 1991).
8. C. Perrow, *Normal Accidents* (Basic Books, New York, 1984).
9. M. E. Paté-Cornell, "Fire Risks in Oil Refineries: Economic Analysis of Camera Monitoring," *Risk Analysis* **5,** 277–288 (1984).
10. M. E. Paté-Cornell "A Post-mortem 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, September 1992).
11. Bechtel Corporation, "Piper Production Platform, Project Profile," and "Piper Gas Conservation, Project Profile" (Bechtel Corporation, San Francisco, California).
12. K. H. Roberts, "Some Characteristics of High Reliability Organizations," *Organization Science* **1,** 1–17 (1990).
13. H. Raiffa, *Decision Analysis* (Addison-Wesley, 1968).
14. K. E. Weick, "Organizational Culture as a Source of High Reliability," *California Management Review* (Winter 1987).
15. C. Heimer, "Social Structure, Psychology, and the Estimation of Risk," *Annual Review of Sociology* **14,** 491–519 (1988).
16. W. E. Gale, Personnal communications (1991).
17. R. G. Bea and W. E. Gale, "Structural Design for Fires on Offshore Platforms" (presentation to the NAOE Industrial Liaison Program Conference, University of California, Berkeley, 1990).
18. B. J. Garrick, "Recent Case Studies and Advancements in Probabilistic Risk Assessments," *Risk Analysis* **4,** 267–279 (1984).