7th Draft - April 16, 1997

Panel on Risk Assessments of Offshore Platforms

(Draft Report)

Introduction

~~Although~~ The need to evaluate and manage risks associated with the production of oil and gas from ~~offshore~~ fixed platforms ~~has been~~ was identified from the earliest days of offshore oil and gas development fifty years ago. Initial efforts ~~were~~ focused mainly on risk of structural failure due to environmental force loadings. Much work has gone into calculation of return intervals for various environmental loads due to waves, currents, wind, earthquake, the effects of wave induced soil movement and the probability of failure of offshore structures exposed to these loads. In the past 20 years there has been a growing awareness of the need to identify, evaluate and manage safety, environmental risk and economic loss associated with drilling and producing operations including blowouts, fires and explosions and ship collisions. This effort has increased greatly since the 1988 Piper Alpha accident in the North Sea and the 1989 South Pass Block 60 accident in the Gulf of Mexico. While the recent use of ~~QRA~~ risk assessment has concentrated on the risks to individuals, there is an increasing ~~use of QRA to~~ trend also to include ~~assess both~~ environmental risk and risk of economic loss.

A Brief History of Offshore Development

Today, offshore sources account for more than (%) of the world's annual oil production, and more than (%) of the world's annual production of natural gas (source). The majority comes from fixed platforms, and the remainder from floating production facilities and subsea developments. The oil industry grew up in the United States and the offshore industry grew up in the Gulf of Mexico. Therefore, the United States has long been at the forefront of the development of offshore technology. Only with the discovery of oil in the North Sea and with the start of production from the Ekofisk oilfield in 1971, and from

Argyll and Forties in 1975, have changes been found necessary to US technology to meet the specific needs of the more severe environment and operating conditions first found offshore Norway and the UK.

The early technical lead established in the oil industry by the US has been well documented. Coal fueled the first industrial revolution, which started in Britain around 1760 and slowly spread to the rest of Europe after the Napoleonic War. Coal then remained the dominant energy source in western Europe well into the twentieth century. In the United States, things were very different. The first oil well was dirlled by E. L. Drake at Titusville, Pensylvania, in 1859. In 1900 there were 78,745 producing oil wells in the United States, and by 1970 the U.S. had 539,990 producing oil wells, or 89% of the free world total. At the start of the First World War in 1914, the United States was producing 266 million barrels (65%) of a world total of 408 million barrels, and Europe accounted for only 87 million barrels (Arney, 1992).

Initial offshore development was a simple extension of land practice. The first offshore well was drilled in 1897 from a wharf made of wooden piling and timbers which extended about 300ft into the Pacific Ocean near Santa Barbara, California. By the early 1930s, oilfields had been discovered in the inshore and coastal areas of Lake Maracaibo, Venezuela; Louisiana; and the Caspian Sea. In 1938, Creole discovered an oilfield one mile offshore Louisiana by directional drilling from land. In 1947 Kerr McGee installed the first offshore platform out of sight of land 15 miles from shore in 20 ft waterdepth in the Gulf of Mexico, and by the end of (1987) more than (4,187) platforms had been installed in the Gulf of Mexico alone. (Arney, Internal Marathon Report). Today, offshore oil exploration and production is a worldwide industry. Exploration has taken place off the coasts of more than 75 nations (McGraw Hill, Encyclopedia of Science and Technology), and around the world there are now more than 7000 producing platforms (fig x).

Types of Fixed Offshore Platforms

Many of the first offshore platforms were simple steel or concrete structures, either piled trestles decked over, or gravity based which were towed to location in shallow water and sunk. Although there were a number of variations, the vast majority of fixed platforms are simple welded steel tubular space frame, fixed to the seabed with hollow steel piles and with a steel framed deck to carry the drilling and production equipment (fig x). Many platforms in shallower water are too small to support self-contained drilling rigs, and wells are drilled from a jack-up rig over the structure (fig x) or using a platform rig with a tender alongside (fig x). On many platforms, the wells are drilled from a packaged rig which is removed after the development wells have been completed (fig x). Integrating the rig and drilling equipment completely into the topsides design started with oilfield development in Cook Inlet, Alaska in the mid-1960s and the North Sea in the late-1960s (fig x).

The size and complexity of an individual offshore platform is determined by a number of considerations which include waterdepth, wave load, number of wells, the process facilities required and distance from shore. Arney and Murphy (1988) analyzed 278 typical platforms around the world. Design and operating conditions may be divided into three basic environments, calm, intermediate and rough (fig x). Jacket weight increases with waterdepth, and as expected the lighter jackets are also associated with the calmer offshore areas and lower wave loading (fig x). Arney and Murphy were also able to relate jacket weight to topsides load (and hence size and complexity of topsides) for both the Gulf of Mexico (fig x) and the North Sea (fig x). Further analysis shows that of a total of 4,500 platforms in the Gulf of Mexico OCS in 1992, some 3,000 had less than five slots, 1,500 had six slots or more, and only 26 were installed in waterdepths greater than 600 ft (fig x). Such small individual platforms with few well slots (fig x) also occur in most offshore areas around the world (figs x through x).

It can therefore be seen that fixed platforms in calm and intermediate environmental areas have generally evolved into what has become typically known as a "Gulf of Mexico" structure. The general characteristics of such platforms are light jackets, since wave loads

are low and the joints are not generally subject to fatigue, and open decks with light topsides loads (figs x-x). Even in rough weather areas such as the North Sea, many platforms and especially early structures installed in waterdepths of less than 250 ft are properly classified in the same way (fig x).

It is mostly in the Northern North Sea, where the distance from shore, rough environment, high process throughputs on individual platforms and high manning requirements have combined to produce the typical "North Sea" platform (fig x). The jackets of such platforms are heavy, due both to the topsides load they are required to carry and to the wave loading and fatigue requirements. The topsides of such platforms are heavy and enclosed, and the drilling rig or rigs are integrated into the production facilities and equipment. Accommodation is often provided for between one and two hundred permanent crew who work on a rotational schedule. There are, however, until now less than (100) such platforms in either the North Sea or in other offshore areas around the world (fig x).

The Move Subsea and to Deeper Water

The two tallest fixed platforms installed to date anywhere in the world are Cognac (xxxx ft) and Bullwinkle (xxxx ft) both in the Gulf of Mexico. In deep water the weight and cost of fixed platforms becomes prohibitive, and alternative technologies are found such as the compliant tower and tension leg platform, and subsea developments and floating production systems. It is the use of these last two technologies which has permitted Petrobras to develop in deep water offshore Brasil, and enabled the present march to deepwater in the Gulf of Mexico. Their use has also enabled the selective development in shallower water of smaller fields which cannot on their own support the cost of a fixed platform. Examples include....

The Development of Design Codes for Offshore Platforms

When Kerr McGee installed their first offshore platform in the Gulf of Mexico in 1947, the US oil industry was already 88 years old. The American Petroleum Institute (API) had been writing oil industry standards since 192x. Although in 1947 established codes and standards were available for the drilling and production operations, none was directly applicable to the new class of steel tubular framed offshore platform structures, nor to determination of wave heights and wave forces which contribute most of the environmental loading. Therefore, the codes and standards needed for a new technology and new industry had to be developed, and for many years the design and construction of offshore platforms was primarily a structural matter entrusted to civil engineers. Evolution of the API offshore structures code API/RP2A has been well documented elsewhere (xxxxxx) and the 20th edition was published in 1997. Most of the more than 7000 offshore platforms which have to date been installed around the world are typical Gulf of Mexico structures, and the majority of these have been designed and built to API standards.

When offshore oil and gas development started in the North Sea in 19xx, with (which/where), American Petroleum Institute (API) standards were de-facto international standards used throughout the world by the oil and gas exploration and production industry (Arney, 1992). Therefore, the jackets and topsides of the first North Sea platforms were also designed primarily to API standards, augmented by international agreements relating to safety of life at sea. For instance, BPs West Sole gas field platform C installed in 1969 is a typical Gulf of Mexico type export: a piled steel jacket in (70ft) waterdepth, with an open steel deck to provide real estate for the drilling and production equipment. The drilling rig was brought out in packages and the derrick assembled offshore, similar to a land rig, and removed on completion of drilling (figs x and x).

It was only with discovery in 19xx and development of the BP Forties oil field that the move began in the North Sea away from Gulf of Mexico type platforms and field development methods, dictated by the waterdepth, distance from shore, the more severe operating environment, and the size of topsides facilities required to handle the high individual well

flow rates and high production rates from the large reserves which could be developed from each platform.

Forties is located in 400ft waterdepth and has recoverable reserves in excess of 2 billion barrels, and is an interesting contrast with West Sole. Development required four combined drilling and production platforms with the largest jackets and heaviest topsides (15,000 tons operating weight) designed to that time. The jackets were traditional steel structures, but the topsides were designed and built in individual modules weighing up to 800 tons since the established practice of piece-small offshore assembly would have been inefficient and taken too long. The modules were preassembled and precommissioned onshore, and lifted into place by derrick barge ready for hook-up. The drilling rig became an integral part of the topsides, primarily to share power and safety systems with the rest of the platform. Figs x and x show the Forties topsides. The same safe area principles drove the design as for West Sole, but some modules needed artificial ventilation and pressurization to qualify them as safe areas, and a sophisticated gas and fire alarm and extinguishing system was also required.

Industry appears to be moving in the general direction of goal setting regulations implemented by prescriptive standards. This is good, since the whole purpose of a standard is to capture what has been found by experience, by design or by test to work well, so that it can be repeated. This whole purpose is negated if a standard is prepared as a totally functional document, since past knowledge is not captured and every new design must then start from first principles. Problems also arise when prescriptive standards are written directly into legislation and regulation, such that acceptable alternatives cannot be used or improvements can only be made with great difficulty.

Definitions of Risk and Structural Reliability

There are three main categories of risk to the offshore platform. The first is due to structural collapse from environmental overload, and structural reliability becomes the 'static risk' case. The platform process pipework, separators, pumps and compressors

should not leak hydrocarbons, and upsets when operating under normal steady state conditions may be defined as the 'steady state risk' case. During unusual operations, including drilling, start-up, shut-down, maintenance and new construction, the static and steady state conditions no longer apply. This is the 'dynamic risk' case, and it is important to note that the UK Offshore Safety Case, which is described in detail later in the report, grew out of a dynamic failure on the Piper Alpha platform.

Structural Reliability

Historically, the structural reliability of offshore platforms have not been determined implicitly. Platforms were designed first to elastic and sometimes more recently to load factor structural codes, with environmental loading determined from an estimated wave height which has settled for traditional fixed platforms with a normal life expectancy to be either the 50 year (in the North Sea) or 100 year (in the Gulf of Mexico) maximum wave with a 0.67 probability of being reached or exceeded one or more times in any year. [What does this mean?]

It is only with the Norwegian move towards Quantitative Risk Assessment and since 1992 with the UK safety case that explicit numbers have been more widely sought. Available literature indicates a structural reliability for platforms in the Gulf of Mexico in the order of 1*10E-3 to 1*10E-4, and in the North Sea in the order of 1*10E-5. However, the risk of loss of life from structural failure of a fixed platform in the Gulf of Mexico and the Northern North Sea appears to be identical because platforms are normally evacuated in the Gulf of Mexico when a design event occurs (xxxx).

<u>Perception of Risk</u>

Acceptable levels of risk are both technically and socially determined, vary through time and are different in different societies. The matter has been studied elsewhere in detail by Pate-Cornell (19xx) and others. In the offshore arena, acceptable limits of risk are still being determined. Since the definition of acceptable target risk levels is essential for the

development of probabilistic design and operating codes, offshore codes and regulations therefore remain, in common with the codes and regulations governing the performance of other industries, largely deterministic in scope and content.

However, in regard to the link between what is technically possible, economically achievable and socially desirable, it is not comforting that, according to Hambly and Hambly (1994) "Perceptions of risk are frequently based on news; and news is sold by sensationalism, not realism.....the public perception of risk is a much clearer fact than any statistic, but.....any policy which aims to match safety provisions to public perceptions, as opposed to scientific assessment, is an expedient open to manipulation....."

There is no doubt that public perception of what is an acceptable risk is linked in some way to general advances in public health and public safety. The death rate in England per 1000 inhabitants has declined from 30 in the early 1700s to 20 in the early 1800s (Baudel [1979] after Trevelyan) to 10 by the mid part of the 20th Century (Encyclopedia Britannica). In the South African War the annual incidence of enteric infections (typhoid and paratyphoid) was 105 per 1000, and the annual death rate was 14.6 per 1000. The comparable figures for World War One after immunization had been fully introduced were 2.35 and 0.139 respectively (Ibid, page 896).

These statistics help to explain why public acceptance of loss of life in industrial accidents (which is different from the perception issue involved with the high consequence/low probability event) changes with the increasing expectancy to live out a natural life. What was an acceptable death and accident rate in the coal mines and steel mills of Victorian England is no longer acceptable in an advanced industrial society. In other words, increase in average life expectancy appears to be inversely related to the tolerance a democratic society has for complex industrial accidents of both the steady state and dynamic kind. Indications of present levels of tolerance can be found inter alia in Hambly and Hambly (1994), including a 'tolerable' FAR from living near a nuclear power plant of 0.1*10E-8h, and an average for the UK construction industry of 5*10E-8h. These numbers compare with FARs for the average man in his 30s from diseases and accidents both at 8*10E-8h.

(Reinsert paragraph describing FAR)

I. Regulatory Requirements

The first regulations in the oil industry addressed property rights and taxation, in other words they provided only the legal and commercial framework within which industry could operate (reference). Within this framework, the American Petroleum Institute (API) was established in 1919 as the first national trade association in the United States to encompass all branches of the petroleum industry. The API Division of Standardization was formed in 1923. At that time, the marketplace for production equipment was chaotic. There was little interchangeability between different manufacturers' pipe, fittings, equipment and tools. Inventories were correspondingly high. Discrepancies caused higher costs, and safety hazards. The goal of the API standardization program was to facilitate the broad availability of safe and interchangeable products. The API standardization program initially focused on dimensional uniformity among the same products for different manufacturers. Gradually, the standards increased in complexity and began to include wider ranges of sizes, materials, chemistry and working pressures, as well as strength and other physical requirements (Arney, 1992). API standards also extended to include safe design and operating and maintenance practices, and the present API catalogue lists more than 400 standards covering all areas of oil industry operations.

More recently, regulations have also extended into areas beyond strict legal and commercial requirements, usually driven by public concern as the result of major industrial incidents such as at Flixborough (1974) and Seweso (1976), loss of Sea Gem in the North Sea in 1976, the Valdez grounding in 19**, and the Piper Alpha disaster in 1988. It is important to note, however, that regulations are not and cannot be a substitute for good industry practices and good industry codes and standards. This is demonstrated by evolution of the UK safety case since Piper Alpha, which is described in detail in Section IA below.

Requirements for risk assessment differ in different parts of the world based on both the physical and financial risks involved and the political environment of the regulatory agency. For example, in the North Sea where platforms tend to be big, complex, contain a relatively large number of people and are difficult to evacuate due to weather conditions, one would expect greater efforts expended on safety risk identification and mitigation than in the Gulf of Mexico and other offshore areas around the world where platforms are much smaller and easier to evacuate.

Much of the present work on offshore risk assessment is being carried out in the United Kingdom, Norway, the United States and, to a lesser extent, Australia. It therefore seems appropriate to discuss in more detail the regulatory requirements for risk assessments in these four important and representative areas of the world.

A. United Kingdom

Loss of the jack-up rig Sea Gem, while drilling an exploration well for gas in the Southern North Sea in 1966, gave direct rise to the Mineral Workings Act (1971). This Act enables Regulations to be introduced covering oil and gas exploration and production activities in the UK North Sea (Birkenshaw, 1994).

The first gas platforms installed in the UK Southern North Sea were designed and built prior to 1971, primarily to API standards augmented by international agreements for matters relating to safety of life at sea. With the discovery of oil in the Central North Sea area, and the awareness that the platforms needed for field development here would be substantially larger and more complex than for established offshore areas in other parts of the world, the requirement was seen for a more structured platform design approval and inspection process. Therefore, the Offshore Installations (Construction and Survey) Regulations SI 289 (1974) were introduced. SI 289 followed contemporary industry practice, and established a certification regime based on plan approval of drawings to prescriptive requirements and periodic surveys of the completed installations.

By the end of 1997, a total of *** platforms had been installed and were operating in the UK and Norwegian sectors of the North Sea. One of these was the Piper Alpha platform, installed in 19**.

On 6 July 1988 an explosion on Piper Alpha led to the loss of 167 lives. The direct cause of the explosion was a failure of the lockout - tagout procedures, but there were many other human and organizational factors (HOF) and design deficiencies which led to the inability to mitigate the accident and organize evacuation and recovery of personnel.

The disaster and the loss of 167 lives was a shock to the UK. A public inquiry was set up headed by Lord Cullen, which recommended a number of changes to the Certification regime. These recommendations were strongly influenced by the UK Health and Safety Executive's experience regulating major hazards onshore under the Control of Industrial Major Accident Hazard Regulations 1984 (CIMAH) (SI 1984/1902).

The CIMAH Regulations (which also implement a number of European Community Directives) were drafted in response to certain major accidents that took place during the 1970s, notably the Flixborough accident in the UK in 1974 and the disaster at Seveso, Italy in 1976. They require an inventory of hazardous materials, liaison with local emergency services concerning emergency plans, the demonstration of safe operation of the facility, and certain installations are also required to submit a safety report to the HSE. In the first instance the safety report is a means by which manufacturers demonstrate to themselves the safety of their activities, but it also serves as a basis for the regulation of major hazard activities.

During his inquiry, Lord Cullen considered both the CIMAH and the Norwegian models for the control of major hazards. He concluded that the operator should be required by regulation to submit to the Health and Safety Executive (HSE) a safety

case in respect of each of its installations, and that this requirement should be analogous to regulation 7 of the CIMAH Regulations. However, Lord Cullen also concluded that, given the distinctive features of offshore operations compared with normal onshore activities (including the fact that the workforce both live and work offshore and in the North Sea the impracticability of rapid evacuation in the case of emergency) that the offshore safety regime should go further than CIMAH in a number of respects.

Accordingly, following Lord Cullen's recommendations, the Offshore Installations (Safety Case) Regulations include the following requirements which have no direct counterpart in CIMAH:

(a) That the duty holder's standards for management of health and safety and the control of major hazards shall be subject to formal acceptance

(b) that measures to protect the workforce shall include arrangements for temporary refuge from fire, explosion and associated hazards to permit sufficient time for evacuation after an incident

(c) that suitable use should be made of quantitative risk assessment (QRA) as part of the demonstration of the adequacy of preventive and protective measures, and

(d) formal requirements relating to safety management and audit.

Lord Cullen also recommended that, in parallel with the move to the safety case regime, the existing UK offshore legislation should be comprehensively reviewed with a view to its progressive replacement by a modernized and rationalized structure of Regulations, mainly in goal-setting (rather than prescriptive) form and supported by non-mandatory guidance. This recommendation took account of

experience of similar reforms onshore, developed by the Health and Safety Commission using their powers under the 1974 Health and Safety at Work Act.

The Offshore Installations (Safety Case) Regulations 1992 were prepared to implement the recommendations made by Lord Cullen. Specifically, Lord Cullen's report on the Public Inquiry into the disaster recommended that the operator or owner of every offshore installation should be required to prepare a safety case, and submit it to the UK Health & Safety Executive (HSE) for acceptance.

The requirement to submit a Safety Case applies to both fixed and mobile installations, and a Safety Case is must be submitted at various stages in the installation's life. The Design Safety Case for a fixed installation, covers the concept design and offshore construction and commissioning. This is submitted early enough so that any issues raised by the HSE can be taken into account in the detailed design. The Operational Safety Case for a fixed installation, covers the detailed design and operation, and is submitted six months before hydrocarbons are likely to be on the platform. An Abandonment Safety Case for a fixed installation, covers the methods of decommissioning, and is submitted six months in advance of abandonment. For mobile installations, a Mobile Installation Safety Case must be submitted three months before the vessel operates in UK waters.

The Safety Case describes the operator's management system and explains its adequacy in complying with the Health and Safety at Work Act 1974 and other relevant statutory provisions, and must be formally accepted by the HSE before the installation is allowed to operate. The safety case explains the steps taken to assure the operator has established adequate arrangements for audit of the management system, to identify all hazards with the potential to cause a major accident and to evaluate risk, and introduces the important concept that measures should be taken to reduce the risks to persons affected by those hazards to assure a risk level as low as reasonably practicable (ALARP).

(Define ALARP and explain what it means and how it ties in to QRA)

The Schedules to the Safety Case Regulations, which list the information to be included in each type of safety case, state that the safety case must include a demonstration, by reference to the results of suitable and sufficient quantitative risk assessment, that the measures taken will reduce risks to the health and safety of persons to the lowest level that is reasonably practicable.

(Explain concept of temporary refuge, and that only "risk" number given in Safety Case guidance is 10E-3 for the integrity of the temporary refuge).

As experience has been gained with the Safety Case in the UK, and in order to implement the further recommendation made by Lord Cullen that existing UK offshore legislation should be comprehensively reviewed, further regulations were prepared and the Safety Case relies on five further Statutory Instruments executed between 1992 and 1996 (fig x).

These include the Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995 (PFEER) which promotes an integrated risk-based approach to managing fire and explosion hazards and emergency response. Their requirements include an assessment of the major accident hazards arising from fire and explosion events which may require evacuation, with the purpose of identifying appropriate arrangements for dealing with them.

Perhaps the most significant of these new regulations supporting the Safety Case is the Offshore Installation (Design and Construction) Regulations SI 913 (1996), which establish further practical requirements to implement the 1992 Safety Case Regulations, and replace the certification regime established by the Offshore Installations (Construction and Survey) Regulations SI 289 (1974). SI 913 dispenses with the concept of a Certifying Authority, and places sole responsibility for the development and maintenance of a safety facility on the owner or operator (referred

to for convenience as the duty holder). Under the 1996 Regulations, the duty holder is required to list safety critical elements, have these subject to independent review, and develop a scheme for the verification of their performance throughout their life cycle.

SI 913 is specific in requiring engineering specification for the design, manufacture, operation, maintenance and inspection of critical elements, which might include structure, downhole well equipment, production equipment such as separators and compressors, and platform emergency and shutdown systems and their individual components. In other words, the safety case continues properly to rely on design carried out and equipment manufactured and supplied to industry codes and standards. However, the Guidance Notes to the Safety Case warn that prescriptive industry standards may become outdated, and (by inference) need to be kept up to date and provision should be made to allow alternative engineering solutions when this is appropriate.

~~The Offshore Installation (Design and Construction) Regulations 1996 further amend the Safety Case Regulations, and replace the certification regime which was established by the Offshore Installations (Construction and Survey) Regulations 1974. The new Construction and Survey Regulations dispense with the concept of a Certifying Authority, and instead place sole responsibility for the development and maintenance of a safe facility on the owner and operator. The owner/operator is required to list safety critical elements, to have these elements subject to independent review, and to develop a scheme for the verification of their performance throughout their life cycle.~~

Both qualitative and quantified risk assessments are used in U.K. Safety Cases. It is noteworthy that the Safety Case Regulations require only that all hazards with the potential to cause a major accident have been identified and that risks have been evaluated and measures taken to reduce the risks to persons affected by those hazards to the lowest level that is reasonably practical. In regard to the design of a

fixed installation, the only specific reference to quantitative risk assessment is made in Schedule 1.12 to the Regulations, which states that, among the particulars to be included in a safety case submission should be "A demonstration by the results of suitable and sufficient quantitative risk assessment, that the measures taken (in relation to the hazards) will reduce risks to the health and safety of persons to the lowest level that is reasonably practical." Considerable guidance is given on the intent of the Regulations in the HSE publication A Guide to the Offshore Installations (Safety Case) Regulations 1992.

Since the enabling legislation for the 1992 UK Offshore Safety Case Regulations was the existing Health and Safety at Work Act 1974, the primary purpose of the Regulations must be to reduce risks to the workforce employed on offshore installations or in connected activities. This can be done both by attention to reducing the frequency of loss of containment incidences by design, operations and maintenance procedures, and lowering the potential consequence of an incident through attention to mitigation and evacuation concepts. However, "requirements designed to reduce the risks to the offshore workforce from major accident hazards will also protect the installations themselves and (also) reduce threats to the marine environment" (Guidance Notes, Introduction, #18,). This is a concept often repeated in personal conversations with UK HSE personnel. It is obviously impossible fully to protect the people on any large and fully integrated Northern North Sea platform without also protecting the installation.

B. Norway

The Norwegian Petroleum Directorate (NPD) is the government department responsible for offshore safety in Norway. The "Regulations Concerning Implementation and Use of Risk Analyses in the Petroleum Activities" were issued by NPD in 1990. The Regulations themselves are brief, 16 Sections on only two pages. A further four pages of non-mandatory Guidelines were issued in 1992. The purpose of the regulations (Section 1) is, "through requirements with regard to risk

analyses, to contribute to establishing and maintaining a fully satisfactory level of safety for people, for the environment, and for assets and financial interests in the petroleum industry." ~~It states that "risk analysis shall be carried out in order to identify the accidental events that may occur in these activities and the consequences of such accidental effects for people, for the environment and for assets and financial interests." Thus it covers risk to life, the environment and the economy.~~

Risk analyses are considered a means to identify areas of concern for improvement, and thereby to enhance safety. Neither the regulations nor the guidelines give any details about the methodology to be employed. Indeed, the Guidelines state that "The term risk analysis is used in the regulations in a broad sense (and) comprises a number of different methods both quantitative and qualitative." ~~Instead, the operator is required to perform risk analyses as necessary to maintain safety. The regulations do not specify that the risk analysis must be quantitative, but QRA is implied by the guidelines.~~

The general Norwegian approach seems to mirror that of the UK, in so far as the Operator is required to define acceptable risk and have this agreed by the Authorities. Therefore, also in Norway provision is made for the uncertainties surrounding what it is at any given time feasible to achieve.

The only mandated reliability levels which have been found are in the Regulations Relating to Loadbearing Structures in the Petroleum Activities, 1996, and concern environmental and other loads on offshore structures . This Code specifies a maximum annual probability of exceedance for environmental loads of 10E-2, which is decreased to 10E-4 for abnormal progressive collapse conditions. However, various combinations of load coefficients greater than 1.0 are also specified, and this makes calculating probabilities of failure and risk more complex. [Are we sure this is right?]

The Regulations Concerning Use of Risk Analysis provide considerable flexibility in the type and extent of documentation to be submitted, as well as in regard to the timing of the submission. What is specific is, however, that the NPD shall agree with the documentation required in consultation with the operator, and that the NPD shall be informed if the Operator later alters the safety objectives and acceptance criteria for risk.

Other similarities between the UK and the Norwegian approach include the objective that enhancement of safety becomes a dynamic and forward looking process, and that the level of risk in activities must at all times be kept as low as possible (sic. from the NPD translation, but the overall context is taken to mean as low as reasonably practical).

The Norwegian Guidance Notes go further (re Section 11) to specifically address the issue of learning from experience, which is often central to the debate on functional versus prescriptive codes and standards. "The risk of an accidental event may be accepted, but the actual occurrence of an accidental event cannot be accepted. Each and every accidental event or near miss must consequently be followed up in order to prevent recurrence." The goal-setting requirement is to avoid the accident. The specific of how best to avoid its recurrence is often best captured in prescriptive standards, always bearing in mind that waiver must be readily available from prescription which is no longer relevant to a specific case in hand.

The remainder of the Regulations and Guidelines provide further explanation at a text-book level on how to handle risk analysis and co-ordinate with the NPD on the results. A number of technical papers have been written giving details of specific risk analyses carried out for Norwegian offshore oilfield operations, and it is believed that the explanation of process given above will help make easier interpretation of the results from these works.

C. Australia

The Australian Safety Case Regime is based upon the 1967 Commonwealth Petroleum (Submerged Lands) Act with the legal requirement beginning 1 July 1996. The Act is administered at the Australian State level with the Department of Minerals and Energy (DME) as the Designated Authority. The DME grants approval and conducts compliance audits. Documents required are: a Vessel Safety Case (MODU), Facility Safety Case (Platforms), and a Bridging Document, which defines safety management links, i.e., implementation of the Safety Case. The components of the Vessel Safety Case are: a facility Description, the Safety Management System, and the Formal Safety Assessment (FSA) which records the risk assessment analysis and results.

Operators are expected to prioritize hazards using QRA, set acceptance criteria, demonstrate that these standards are met, and use cost-benefit analysis to ~~show~~show that the risks are ALARP. Non-quantitative approaches may be accepted, provided that hazards have been identified and assessed, and measures taken to make the risks ALARP.

D. United States

Safety of Offshore producing operations in the United States are regulated primarily by the states to the limit of their jurisdiction (normally three miles from shore, with the exception of Texas and the West Coast of Florida, which are nine miles, and by the Minerals Management Service of the Department of the Interior (MMS) in waters beyond state jurisdiction which is designated the Outer Continental Shelf (OCS). Other Federal Government agencies have specific regulatory responsibilities such as:

- Coast Guard - Life safety including fire fighting and evacuation for platforms, safety of mobile drilling units and mobile production units

- Army Corps of Engineers - Construction activity especially dredging, and platform and pipeline installation, within shipping fairways. Outside of shipping fairways, the ACoE uses MMS criteria for permitting.

- Environmental Protection Agency - Air and water discharge, and oil spills. EPA has authority over air emissions from offshore platforms through Clean Air Act except for the Western and Central GOM which are under MMS jurisdiction. The Clean Water Act charges EPA with regulation of discharges through National Pollutant Discharge Elimination System (NPDES) permits.

- Department of Transportation - Oil and gas pipelines which are not part of gathering systems regulated by the MMS.

Through the use of interagency memorandum of understanding, the MMS has primary responsibility for establishing regulations and assuring compliance for design, construction and operations in federal waters as it applies to the drilling and operation of wells, and the design, construction and operation of fixed platforms, production facilities and most pipelines. Current rules are prescriptive in nature and do not specifically require the development of a Safety Case or the use of risk assessment.

The focus of effort is on risk management rather than a specific assessment of risks for each installation and a quantification of risk for that installation. The assumption is made that the risks are well known **from numerous studies on similar designs and accident evaluations.** Adherence to good design and operation management practices will produce a level of risk to personnel, the environment and economic loss which is "acceptable" and which approximates ALARP. These practices evolve with time as new technologies become available.

The structural design, construction, installation and monitoring of fixed structures as prescribed in the Code of Federal Regulations (30 CFR 250) is based on American Petroleum Institute (API) Recommended Practice (RP) 2A, 'Recommended Practice for Planning, Designing and Constructing Fixed Offshore Platforms - Working Stress

Design." Inspection details and frequencies are mandated as are rules for requalification due to changes in anticipated loads or inspection results.

The procedures included in API RP 2A Supplement 1 for "Assessment of Existing Platforms" are based on an assignment of consequence as to life safety consequence (manned - non-evacuated, manned-evacuated and unmanned) or economic consequence (high or low) as shown in Figure ID-1. 'Fire, Blast and Accident Loading" assessments are based on a risk derived from Figures ID-2 and ID-3, which are based on both a determination of consequence and a qualitative assessment of probability of occurrence (high, medium and low). Most of Gulf of Mexico structures are open and allow natural ventilation and are designed and operated in accordance with API RP 75 which places them in low probability of occurrence and are thus either categorized as Risk Level 2 (requiring study to define **probability** consequence and cost mitigation) or Risk Level 1 (insignificant risk that can be eliminated from further considerations).

~~The validity of~~ This approach to structural safety is ~~attested~~ **supported** by the fact that there has been no loss of life due to loss of platform structural integrity in the history of the development of the U.S. OCS and the only loss of platforms designed to 'modern" editions of API RP 2A (editions since the mid-1970's) have been due to ship ~~collisions~~ **allisions**. This approach has also proven efficient in that structures for U.S. locations are demonstrably less expensive to design, construct, install and maintain than structures subjected to similar environmental forces in any location in the world where the requirements of other regulatory regimes must be met. ~~*The costs associated with documenting compliance with regulations is also the least expensive in the world.*~~

Drilling and producing operations are required to meet certain prescribed safety standards detailed in 30 CFR 250 which are based, for the most part on API Specifications and Recommended Practices. Because the hazards associated with this activity are well known and have been subjected to numerous hazards analysis, the emphasis of MMS regulations is on assuring that design is in accordance with 'good engineering practice," **and that operations and maintenance activities follow well understood safety**

Figure ID-1

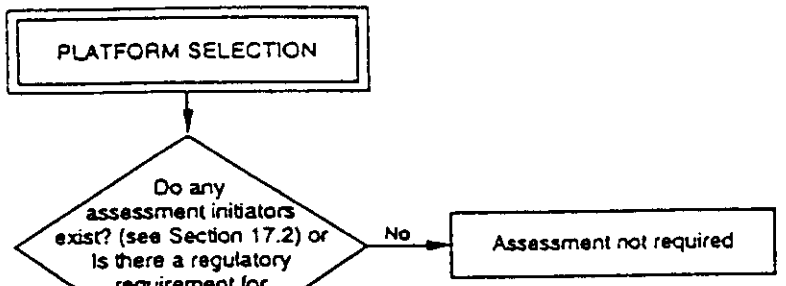


Table 17.5.2a–ASSESSMENT CRITERIA—U.S. GULF OF MEXICO
(see Table 17.6.2-1)

Level	Exposure Category		Design Level Analysis (see Notes 1 and 2)	Ultimate Strength Analysis
L-1	High Consequence	Manned-Evacuated	High Consequence design level analysis loading (see Figure 17.6.2-2)	High Consequence ultimate strength analysis loading (see Figure 17.6.2-2)
		Unmanned		
L-2	Low Consequence	Manned-Evacuated	Sudden hurricane design level analysis loading (see Figure 17.6.2-3)	Sudden hurricane ultimate strength analysis loading (see Figure 17.6.2-3)
L-3		Unmanned	Minimum consequence design level analysis loading (see Figure 17.6.2-5)	Minimum consequence ultimate strength analysis loading (see Figure 17.6.2-5)

Table 17.5.2b—ASSESSMENT CRITERIA—OTHER U.S. AREAS
(see Table 17.6.2-1)

Level	Exposure Category		Design Level Analysis (see Notes 1 and 2)	Ultimate Strength Analysis
L-1	High Consequence	Manned-Nonevacuated	85% of lateral loading caused by 100-year environmental conditions (see Section 17.6.2b)	Reserve strength ratio (RSR) ≥ 1.6 (see Section 17.6.2b)
		Unmanned		
L-3	Low Consequence	Unmanned	50% of lateral loading caused by 100-year environmental conditions (see Section 17.6.2b)	(RSR) ≥ 0.8 (see Section 17.6.2b)

Notes 1. Design level analysis not applicable for platforms with inadequate deck height.
2. One-third increase in allowable stress is permitted for design level analysis (all catagories).

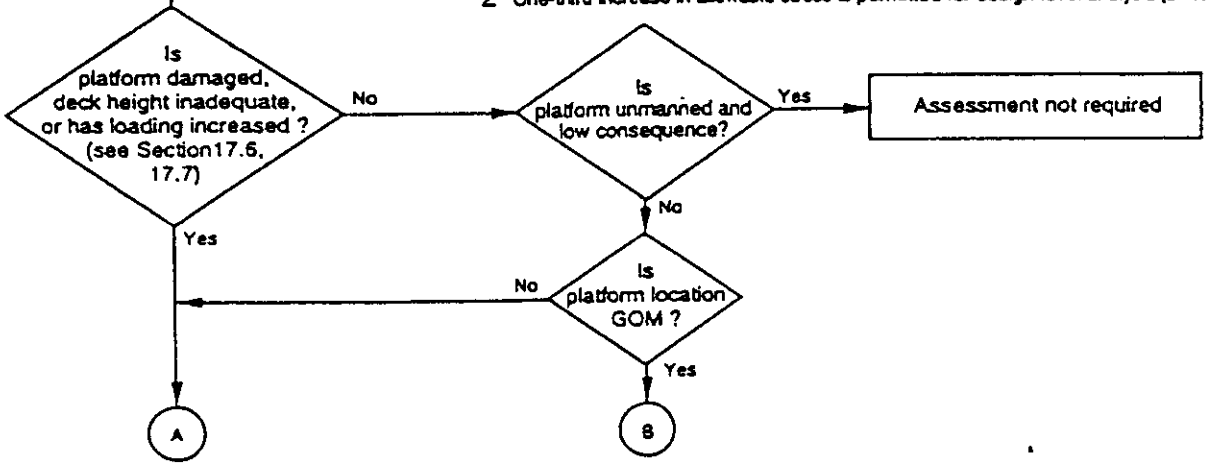


Figure 17.5.2—Platform Assessment Process—Metocean Loading

Figure ID- 1

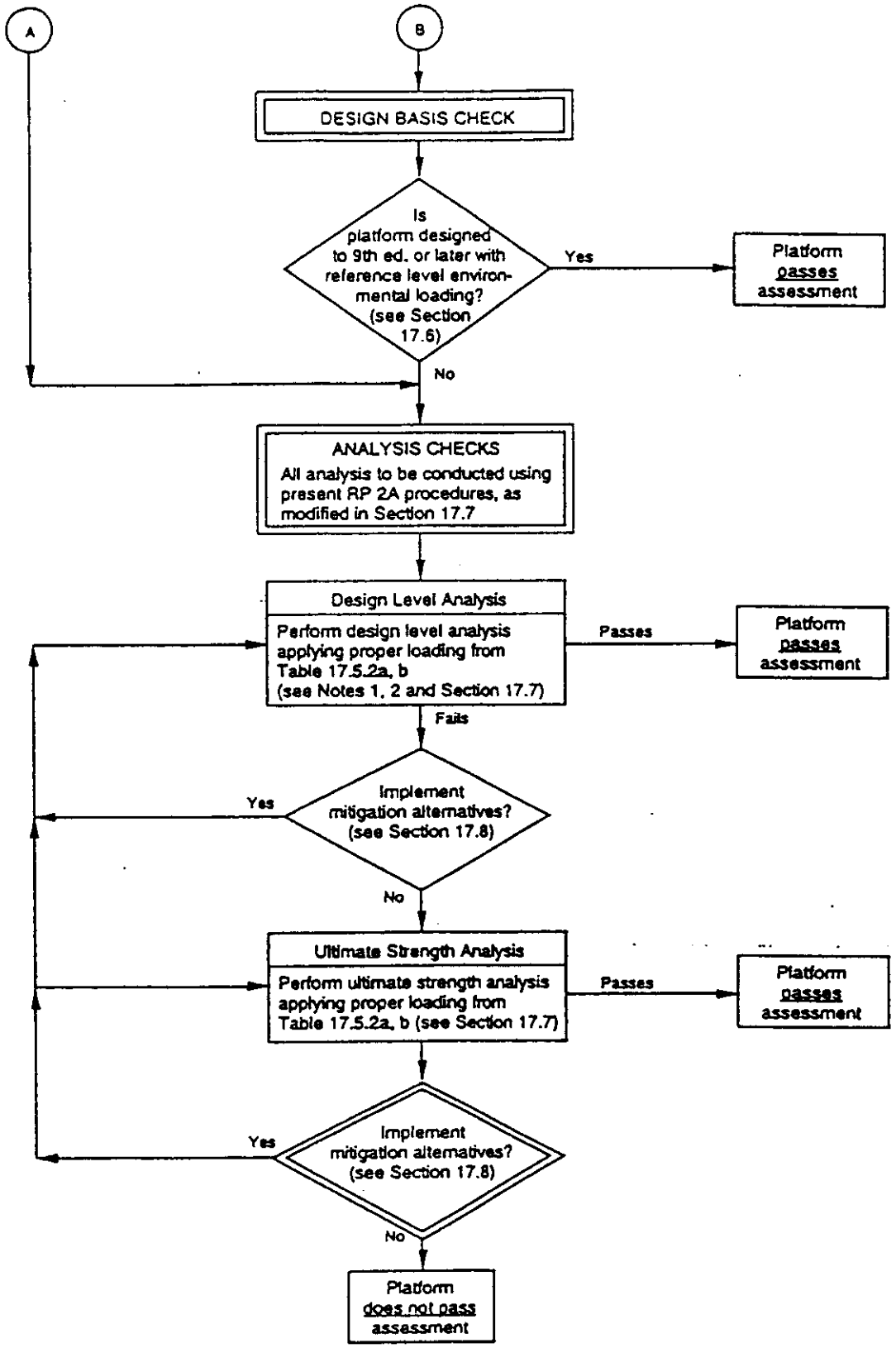


Figure 17.5.2—Platform Assessment Process—Metocean Loading (Continued)

Figure ID-2

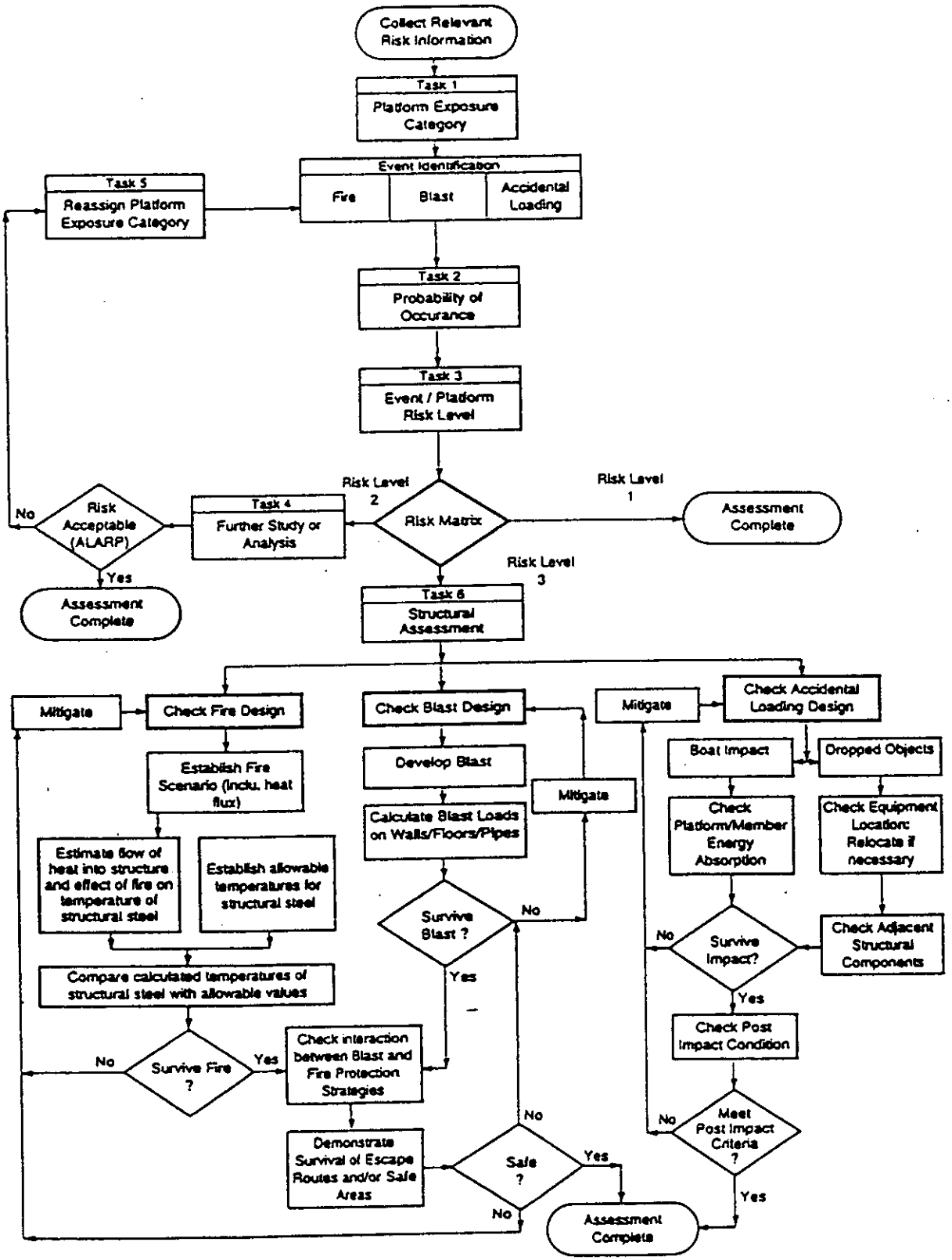
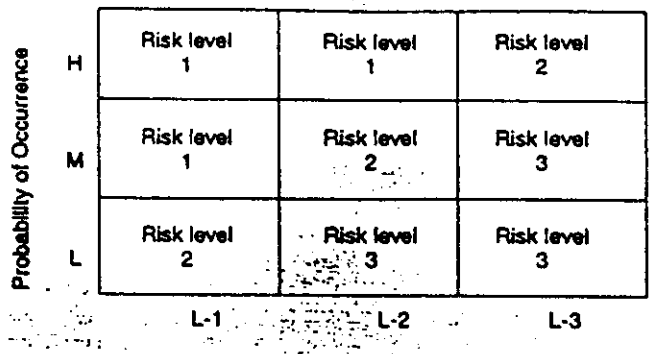


Figure 18.2-1—Assessment Process



Note: See Sections 1.7 and 18.5 for definitions of abbreviations

Figure 18.5-1—Risk Matrix

management principles. The design and operation of production facilities can be used to illustrate the point.

All production processes must be analyzed in accordance with API RP 14C, 'Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms," to determine that sufficient shutdown and other safety devices have been installed to detect and automatically respond (with specified minimum redundancies) to measurable process upsets (level, pressure and temperature). The technique employed by RP 14C is based on an FMEA of each ~~component~~ **sub-system** in a production facility carried out in a generic manner. This is then made facility specific in a manner which is reproducible and easy to audit. Testing frequencies for these devices are mandated by 30 CFR 250.

The application of this procedure in API RP 14C includes a Safety Analysis Table (SAT) for each of the sub-systems shown in Table ID-4. A sample SAT for a pressure vessel is shown in Table ID-5. Table ID-6 is a document which was used in the original development of RP 14C to develop the devices which are required to be considered for a pressure vessel.

RP 14C also provides standard reasons allowing the elimination of certain devices when the process component is considered as part of an overall system. Table ID-7 shows the Safety Analysis Checklist (SAC) for a pressure vessel. Each safety device identified by the SAT is listed. It must either be installed or it can be eliminated if one of the reasons listed is valid. For components not covered by SAT and SAC tables in RP 14C, specific tables can be developed using the procedure described in the RP.

The SAC list provides a handy shorthand for communicating which devices are required and the reasons why some may not be used. For example, for any pressure vessel there is either a PSH required, or a rationale numbered A.4.a.2,

Table ID-4

Process Subsystems Addressed in API RP 14C

Wellheads and Flow Lines
Wellhead Injection Lines
Headers
Pressure Vessels
Atmospheric Vessels
Fired and Exhaust Heated Components
Pumps
Compressor Units
Pipelines
Heat Exchangers (Shell-Tube)

Table ID-5

Safety Analysis Table (SAT) for Pressure Vessels for API RP 14C

UNDESIRABLE EVENT	CAUSE	DETECTABLE ABNORMAL CONDITION AT COMPONENT
Overpressure	Blocked or restricted outlet Inflow exceeds outflow Gas blowby (upstream component) Pressure control system failure Thermal expansion Excess heat input	High pressure
Underpressure (vacuum)	Withdrawals exceed inflow Thermal contraction Open outlet Pressure control system failure	Low pressure
Liquid overflow	Inflow exceeds outflow Liquid slug flow Blocked or restricted liquid outlet Level control system failure	High liquid level
Gas blowby	Liquid withdrawals exceed inflow Open liquid outlet Level control system failure	Low liquid level
Leak	Deterioration Erosion Corrosion Impact damage Vibration	Low pressure Low liquid level
Excess temperature	Temperature control system failure High inlet temperature	High temperature

Table ID-6

Primary and Secondary Protection Required From FMEA of a Pressure Vessel

Event	Primary	Secondary
Overpressure	PSH	PSV
Large Gas Leak	PSL and FSV	Fire Detection, ASH, Minimize Ignition Sources
Large Oil Leak	LSL and FSV	Sump tank (LSH)
Small Gas Leak	ASH, Minimize Ignition Sources	Fire Detection
Small Oil Leak	Sump Tank (LSH)	Manual Observation
Inflow Exceeds Outflow	LSH	PSH and Downstream Vessel
High Temperature	TSH	Leak Detection Devices

Legend:

PSH - High Pressure Sensor
PSL - Low Pressure Sensor
PSV - Relief Valve
FSV - Check Valve
LSH - High Level Sensor
LSL - Low Level Sensor
TSH - High Temperature Sensor
ASH - Atmospheric Gas Detector

Table ID-7

Safety Analysis Checklist (SAC) Pressure Vessels from API RP 14C

A.4 PRESSURE VESSELS.

a. High Pressure Sensor (PSH).

1. PSH installed.
2. Input is from a pump or compressor that cannot develop pressure greater than the maximum allowable working pressure of the vessel.
3. Input source is not a wellhead flow line(s), production header, or pipeline and each input source is protected by a PSH that protects the vessel.
4. Gas outlet is connected by adequately sized piping without block or regulating valves to downstream equipment protected by a PSH which also protects the upstream vessel.
5. Vessel is final scrubber in a flare, relief, or vent system and is designed to withstand maximum built-up back pressure.
6. Vessel operates at atmospheric pressure and has an adequate vent system.

b. Low Pressure Sensor (PSL).

1. PSL installed.
2. Minimum operating pressure is atmospheric pressure when in service.
3. Each input source is protected by a PSL and there are no pressure control devices or restrictions between the PSL(s) and the vessel.
4. Vessel is scrubber or small trap, is not a process component, and adequate protection is provided by downstream PSL or design function (e.g., vessel is gas scrubber for pneumatic safety system or final scrubber for flare, relief, or vent system).
5. Gas outlet is connected by adequately sized piping, without block or regulating valves, to downstream equipment protected by a PSL which also protects the upstream vessel.

c. Pressure Safety Valve (PSV).

1. PSV installed.
2. Each input source is protected by a PSV set no higher than the maximum allowable working pressure of the vessel and a PSV is installed on the vessel for fire exposure and thermal expansion.
3. Each input source is protected by a PSV, set no higher than the maximum allowable working pressure of the vessel, of which at least one PSV cannot be isolated from the vessel.
4. PSVs on downstream equipment can satisfy relief requirement of the vessel and cannot be isolated from the vessel.
5. Vessel is final scrubber in a flare, relief or, vent system, is designed to withstand maximum built-up back pressure, and has no internal or external obstructions, such as mist extractors, back pressure valves, or flame arrestors.
6. Vessel is final scrubber in a flare, relief or, vent system, is designed to withstand maximum built-up back pressure, and is equipped with a rupture disk or safety head (PSE) to bypass any interal or external obstructions, such as mist extractors, back pressure valves, or flame arrestors.

d. High Level Sensor (LSH).

1. LSH installed.
2. Equipment downstream of gas outlet is not a flare or vent system and can safely handle maximum liquid carry-over.
3. Vessel function does not require handling separated fluid phases.
4. Vessel is a small trap from which liquids are manually drained.

e. Low Level Sensor (LSL).

1. LSL installed to protect each liquid outlet.
2. Liquid level is not automatically maintained in the vessel, and the vessel does not have an immersed heating element subject to excess temperature.
3. Equipment downstream of liquid outlet(s) can safely handle maximum gas rates that can be discharged through the liquid outlet(s), and vessel does not have an immersed heating element subject to excess temperature. Restrictions in the discharge line(s) may be used to limit the gas flow rate.

f. Check Valve (FSV)

1. FSV installed on each outlet.
2. The maximum volume of hydrocarbons that could backflow from downstream equipment is insignificant.
3. A control device in the line will effectively minimize backflow.

g. High Temperature Sensor (TSH)

High temperature sensors are applicable only to vessels having a heat source.

1. TSH installed.
2. (Deleted in Second Edition.)
3. Heat source is incapable of causing excess temperature.

A.4.a.3,A.4.a.4, A.4.a.5 or A.4.a.6 must be listed. It becomes a simple matter to audit the design by checki
ng that each device is either present or an appropriate rationale listed.

RP 14C uses a function matrix called a SAFE Chart to show the function performed by each device. Table ID-8 is a completed function matrix chart for a heater treater. Each component is listed in the left hand column with an identification number and description. Under "Device I.D.," each of the devices listed in the SAC is listed. If the device is not present, the appropriate SAC reference number is listed. If the SAC rationale requires that another device be present on another component, that device is listed under "Alternate Device," if applicable.

Listed across the top of the matrix are the various shut-down valves in the facility. A mark in each box indicates the function performed by each device to assure that it protects the process component. By comparing the functions performed by each device to the mechanical flowsheet, it is possible for an auditor to quickly ensure that the process component is indeed isolated.

Process equipment, piping, safety devices and electrical components must be specified and manufactured in accordance with specified API, ASME, and NEC requirements. Minimum training requirements are also specified in 30 CFR 250.

Although not mandated by regulation, the MMS with support from API, the Offshore Operators Committee, the National Ocean Industries Association, the Independent Producers of America Association and the International Association of Drilling Contractors, are encouraging operators to implement a Safety and Environmental Management Program (SEMP) based on API RP 75, 'Recommended Practices for Development of a Safety and Environmental Management Program for Outer Continental Shelf (OCS) Operations and Facilities." RP 75 requires that safety of design, construction and operation be managed by the operator with specific requirements in each of the following elements:

Table ID-8

Example Safety Analysis Function Evaluation Chart from API RP 14C

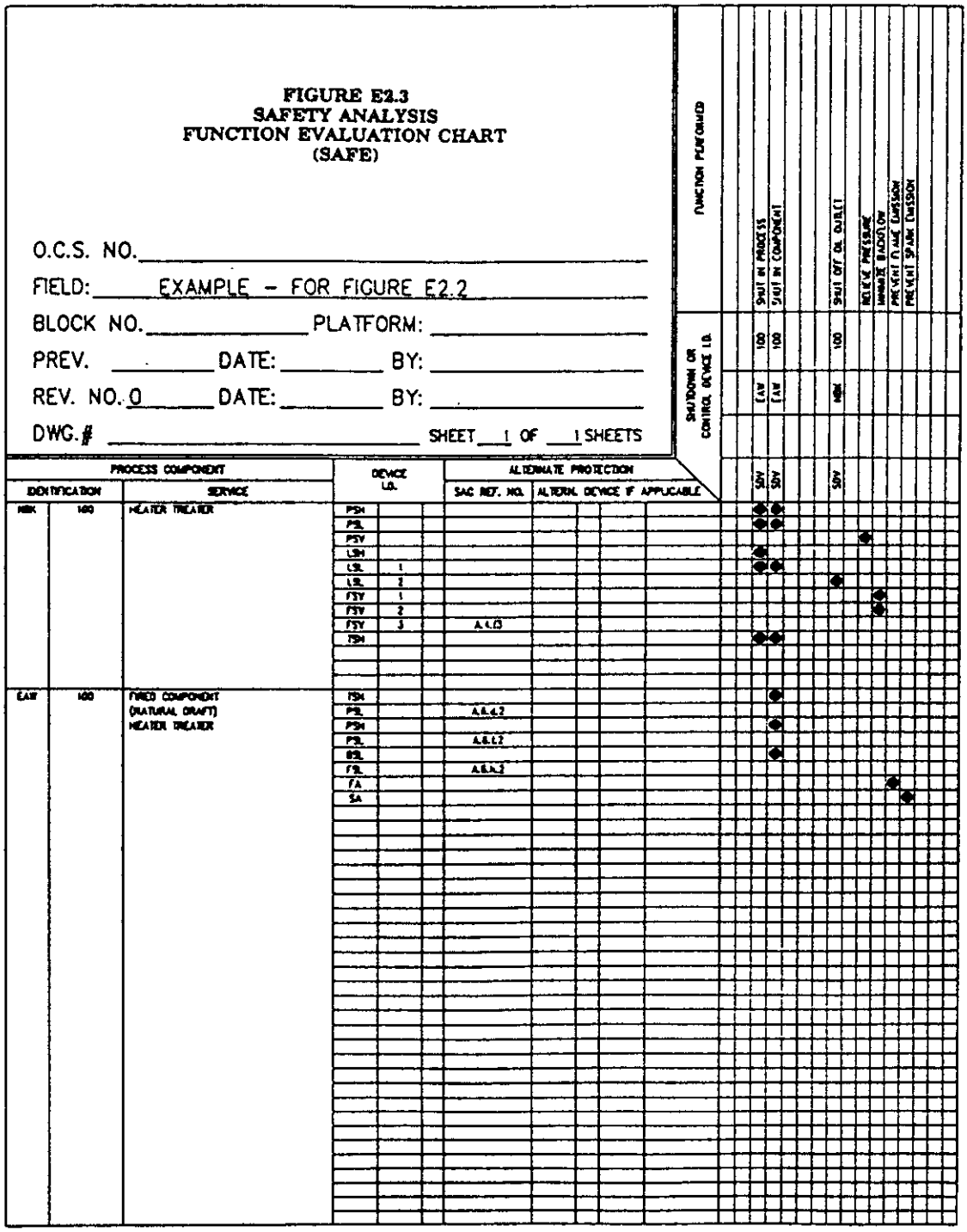


FIGURE E2.3
SAFETY ANALYSIS
FUNCTION EVALUATION CHART
(SAFE)

O.C.S. NO. _____

FIELD: EXAMPLE - FOR FIGURE E2.2

BLOCK NO. _____ PLATFORM: _____

PREV. _____ DATE: _____ BY: _____

REV. NO. 0 DATE: _____ BY: _____

DWG.# _____ SHEET 1 OF 1 SHEETS

FUNCTION PERFORMED

SHUTDOWN OR CONTROL DEVICE I.D.

PROCESS COMPONENT		DEVICE I.D.		ALTERNATE PROTECTION	
IDENTIFICATION	SERVICE			SAC REF. NO.	ALTERN. DEVICE IF APPLICABLE
HBK 100	HEATER TREATER	PSH			
		PSL			
		PSV			
		LSH			
		LSL	1		
		LSL	2		
		FSV	1		
		FSV	2		
		FSV	3	A.4.13	
		TSH			
EAW 100	FIRED COMPONENT (NATURAL DRAFT) HEATER TREATER	TSH			
		PSL		A.8.4.2	
		PSH			
		PSL		A.8.4.2	
		BSL			
		FSL		A.8.4.2	
		FA			
		SA			

Safety and Environmental Information

Hazards Analysis

Management of Change

Operating Procedures

Safe Work Practices

Training

Assurance of Quality and Mechanical Integrity of Critical Equipment

Pre-Startup Review

Emergency Response and Control

Investigation of Incidents

Audit of Safety and Environmental Management Program Elements

Rather than discuss in detail each of these elements, we will highlight the scope of three elements to show the coverage of this document.

One of the specific requirements of RP 75 are that a hazards analysis be performed to identify, evaluate, and where unacceptable, reduce the likelihood and/or minimize the consequences of uncontrolled releases and other safety or environmental incidents. Various methods which could be performed are discussed in a comparison API document (API RP 14J, Recommended Practice for Design and Hazards Analysis of Offshore Production Facilities). Hazards analysis are discussed in further detail in Section IIG.

The training section specifically requires that training address operating procedures, safe works practices, and emergency response and control measures. It also states that training takes place when any modification which occurs under the management of change element requires new or modified operating procedures. Contractor training is address as well.

Incident investigation is required for all incidents with serious safety or environmental consequences whether or not an accident occurred if the incident

"possessed the potential for serious safety or environmental consequences." Follow-up of investigations is required.

The MMS is monitoring voluntary compliance with SEMP. **Based on an industry wide survey as of the end of 1995 (Table ID-9), an element by element analysis of SEMP indicates that between 20 and 50% of the operators have implemented specific elements. Apparently, most operators had implemented some of the elements and were in the process of implementing the rest. Unfortunately, there are some operators (mostly small companies) which have done only a minimal amount of work to implement SEMP. The offshore Operators Committee is working with the MMS to provide incentives to companies which have fully functional SEMP program in place. Incentives may take the form of relief from having to submit certain documentation, decreased MMS inspections, etc.**

Before the SEMP initiative was begun, a 1990 Marine Board report on "Alternatives for Inspecting Outer Continental Shelf Operations" reviewed OCS accident data and concluded that **the record of safety and environmental pollution on the OCS has been good. "The United States has succeeded**

~~"The record of safety on the OCS has been good. In terms of injuries and fatalities, OCS drilling and production operations are comparable to other hazardous activities onshore, such as mining and construction. In terms of environmental impact, oil pollution from offshore operations contributes less than any other significant cause to the release of hydrocarbons into the marine environment. U.S. offshore industry spillage volumes and the amount spilled compared to total production has been reduced.~~

~~"Thus, MMS and the offshore industry are not faced with the problem of correcting a manifestly poor safety record.~~ ~~"The United States has succeeded~~ under its present inspection program in averting the kinds of catastrophic disasters that have befallen the offshore operations of many other nations. Although the evidence of a direct connection is lacking, certainly the activities and vigilance of the federal government have been a

Table ID-9

API RP 75 Implementation Status Assessment

As of December 31, 1995

ELEMENT	Percent Implemented [1]	
	By Population	By Production
1. General Management Program Elements & Information	54.0%	81.3%
2. Safety & Environmental Principles	36.9%	36.8%
3. Hazards Analyses	22.4%	33.5%
4. Management of Change	29.5%	39.5%
5. Operating Procedures	21.0%	23.0%
6. Safe Work Practices	46.3%	65.3%
7. Training	45.6%	56.5%
8. Assurance of Quality & Mechanical Integrity of Critical Equipment	36.6%	56.5%
9. Pre-startup Review	33.7%	39.6%
10. Emergency Response and Control	77.4%	89.6%
11. Investigation of Incidents	43.7%	65.2%
12. Audit of Safety and Environmental Management Principles	26.3%	54.5%

(1) RP 75 Generally in place or being reassessed for continuous improvement

Source: API RP 75 Implementation Status Assessment, API, May, 1996

factor." However, **the report indicated** an increase in the margin of safety on the OCS can be achieved by improving the link between the MMS inspection program and safety performance of the industry. ~~The committee's recommendations are intended to accomplish that end."~~ **The SEMP initiative is, in part, an outgrowth of that committee's report.**

With the exception of offshore California **and Alaska,** state regulations are prescriptive, minimal, and focused on environmental protection and safety of well design. There are no requirements for safety case development and **with the exception of the requirement for a structural risk analysis offshore California, there are no requirements** for the use of risk analysis.

In California state waters, the Division of Oil and Gas of the California Department of Conservation and the Minerals Resources Division of the California State Land Commission have overlapping regulatory requirements with respect to safety of offshore operations in state waters. The regulations of the State Lands Commission are specific and, like the MMS, require the application of the API Recommended Practices and Standards for all new installations and revisions to existing platforms and facilities. Platform structural modifications require the use of risk analysis which has to be approved by both the State Lands and the Coastal Commission. New production facilities or modifications to existing platform facilities require a complete API RP 14C analysis. The Division of Oil and Gas tends to focus on drilling and well design safety, but their regulations overlap those of State sands.

Offshore pipelines in California are regulated by State Lands which requires bi-annual internal inspections with smart pigs or by pressure testing, and external inspections with side scan sonar. Other requirements are similar to those of the MMS.

The Alaska Oil and Gas Conservation Commission has the primary responsibility for the safety of offshore operations. With few exceptions the regulations do not

specifically address offshore operations and focus on conservation of resources. The Alaska Department of Environmental Conservation regulations are more specific and require the use of API Recommended Practices and Standards. The operators of the Cook Inlet platforms have, on a more or less voluntary basis, performed hazards analyses on most of the platforms.

~~There has been little published comparing incident frequencies~~ **It is difficult to compare the level of safety attained** under different regulatory regimes. A paper published in the January, 1993 Journal of Petroleum Technology[1] describes the difficulty of obtaining a consistent set of incident data, but did attempt to show by region of the world trends in Lost Time Injury Frequency (LTIF) and Fatal Accident Rate as shown in Tables ID-10 and ID-11. From this it appears that injury and fatality rates in the U.S. under the MMS prescriptive regulations compare ~~favorably~~ with those in Europe, Australia and elsewhere. However, this information was gathered before the full implementation of the Safety Case regime in the U.K. and Australia, and the SEMP system in the U.S. With the full implementation of the Safety Case System there has been a decline ~~shown~~ in U.K. accident rates as shown in Table ID-12.

With full implementation of SEMP in the U.S., the U.S. rates should also decline, although there is only anecdotal data to indicate that the implementation of SEMP will result in the same type of decline in accident rates shown in Table ID-12. The Department of Energy has a program with Taylor Energy Company to develop a case study SEMP program and to report to industry on costs and benefits. Table ID-13 shows a ~~dramatic~~ decrease in some measures of both safety and environmental risk ~~experienced~~ **complied** by Taylor. ~~; however~~, It is much too early to use this data to ~~compare SEMP and Safety Case approaches to develop ALARP risk levels.~~ **determine whether the increased levels of safety (and therefore decreased levels of environmental risk) which are expected as result of the implementation of SEMP are comparable with the levels which will be achieved in the U.K. using the Safety Case to demonstrate a level of ALARP has been obtained.**

[1] E&P Safety Performance Monitoring by J. P. Visser, R. C. Asgill and Geoffrey Thorp

Table ID-10

Trend of LTIF by Region
(injuries per 1,000,000 man-hours)

	1987	1988	1989	1990	1991	Average of 5 years
Europe	9.3	11.5	9.3	7.8	7.5	9.1
U.S.A.	5.2	5.1	5.7	5.6	5.5	5.4
Canada	6.1	6.7	5.0	4.5	3.9	5.2
South America	6.5	4.0	7.2	5.3	5.7	5.7
Africa	3.3	2.4	3.4	2.2	2.4	2.7
Middle East	2.2	2.9	2.9	3.2	2.3	2.7
Australia/Asia	3.8	3.8	3.1	1.9	1.5	2.8
All regions	5.6	5.6	5.7	4.7	4.5	5.2
Total hours exposed (millions)	602.5	616.4	655.9	720.7	940.5	

*Member returns used for contractor data because API does not provide these

**Members data used; API data were not available at the time of publication

Table ID-11

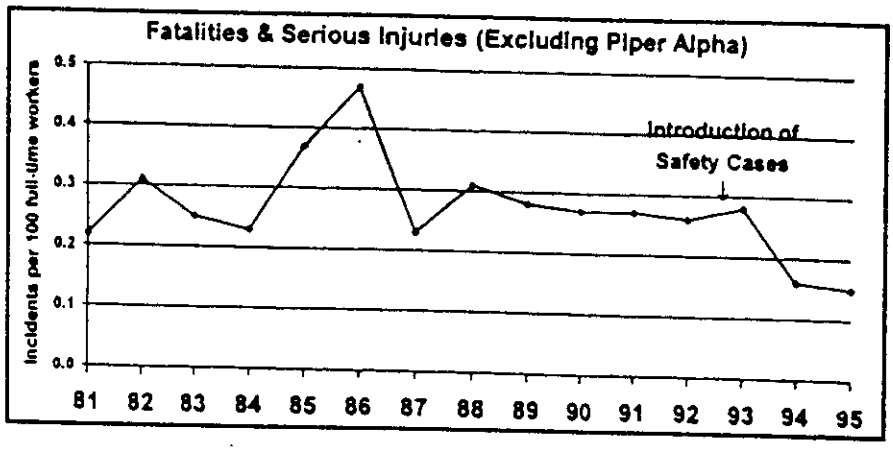
Summary of Frequency of Fatal Accident Rate by Region
(per 1,000,000 man-hours)

	1987	1988	1989**	1990**	1991	Average of 5 years
Europe	4.0	4.5	4.4	10.0	3.2	5.2
U.S.A.	5.1	3.9	5.7	4.1	7.3	5.2
Canada	23.4	16.9	19.3	0.0	3.2	12.6
South America	20.4	19.5	23.3	33.1	17.8	22.8
Africa	21.3	11.4	41.5	11.6	23.5	21.9
Middle East	40.2	8.6	9.5	17.6	10.1	17.2
Australia/Asia	3.8	10.9	4.4	7.6	3.9	6.1
All regions	9.8	8.9	13.9	13.2	9.6	11.1

*Member returns used for contractor data because API does not provide these

**Members data used; API data were not available at the time of publication

TABLE ID-12
UK ACCIDENT RATES FROM 1981-1995



Source: R. Lyn Arscott, SPE, Chevron Corp,; R.J. Edwardes, SPE, Exxon Corp.; Magne Ognedal, Norwegian Petroleum Directorate; and J.P. Visser, SPE, Shell Intl. Mij. B.V. "Sustaining Global Progress In E&P Health, Safety, And Environment." JPT, December 1996.

TABLE ID-13
TAYLOR ENERGY COMPANY
SAFETY AND ENVIRONMENTAL INDICES

(SEMP Initiated During 1995 - 1996)

	Year		
	1994	1995	1996
MMS Inspections			
Number	23	22	19
INC's [1]	86	60	16
INC's/Inspection	3.3	2.7	0.8
Worker's Comp			
Claims $	100,000	50,000	200
Incident Rate	12.6	N/A	0
Number of Spills [2]	9	N/A	4

(1) Incident of non-compliance reported by MMS inspector.
(2) All less than one barrel.

Source: Presentation by David Dykes, Taylor Energy Co., to IPAA Offshore Committee, March 5, 1997.

The U.S. regulatory regime has proven to be extremely cost efficient. A 1989 OTC paper [2] which compared the costs to design and construct a Gulf of Mexico offshore facility with that for a U.K. North Sea facility of the same size indicated a $5MM premium for the U.K. design to comply with increased governmental regulations. Much of this was for additional documentation requirements.

This comparison was made prior to the implementation of Safety Cases. The costs incurred by the U.K. industry for developing platform specific safety cases and the incremental internal management system associated with this effort can be approximated from a survey conducted by the HSE of 16 oil and gas companies and 3 drilling companies. Results are shown in Table ID-14. The cost of performing a Safety Case for an existing facility is on the order of $2-3MM, although a design safety case for a new not-normally-manned minimum facility can be performed for about $200,000 "by doing the QRA using a simple model technique."[3]

Although $200,000 may not sound like much, the total engineering design, procurement, inspection and construction management cost of a typical not-normally-manned Gulf of Mexico platform, facility and pipeline is only about $400,000[4].

The costs for Taylor Energy to implement SEMP for its existing operations is given in Table ID-15. For a new design the only costs would be for the hazards analysis and operating procedures ($10,000 to $40,000) since the non-site specific items are already developed and the safety and environmental information would normally be developed in any case during the design project. (The cost for training operators is not included in Taylor's costs.)

---

[2] K. E. Arnold and N. C. Roobaert: "Comparision of North Sea and Gulf of Mexico Design Philosophies," paper OTC 6117, 1989 Offshore Technology Conference

[3] Correspondence to Panel from Derek Moorfield, Granherne, Ltd., March 4, 1997

[4] K. E. Arnold, J. E. Barnes, and L. D. Danner: "Design and Construction of Minimum Cost - Quick Delivery - High Quality Offshore Platforms for Independent in the Gulf of Mexico," SPE Gulf Coast Section, 1994.

Table ID-14
Offshore Installation (Safety Case) Legislation Evaluation Survey Aggregate data 1992-1995
(16 oil/gas companies and 3 drilling companies)

Safety Case Preparation Cost (£m) (MOD)

Cost Category	1992	1993	1994	1995	Total 19 Companies	Estimated Industry[1]	Number	Cost/ S.C.
SC Preparation -new installations	1.3	5.9	7.7	11.5	26.3	31.6	13	2.4
SC Preparation -existing installations	30.3	41.3	21.6	8.9	102.1	122.5	216	1.8
SC Preparation - ongoing mods/re's/abandonments	0.0	0.0	2.4	3.6	6.0	7.2	8	0.9
Subtotal	31.6	47.1	31.7	24.0	134.5	161.3		
Incremental Internal Costs								
Incremental costs of SMS	4.7	6.7	10.1	6.0	27.5	33.0		
Incremental Safety Dept costs	3.1	7.2	2.3	1.7	14.3	17.2		
Incremental Safety Training costs	1.1	4.4	2.5	1.9	9.9	11.9		
Incremental costs of improvements to PTW system	1.0	2.3	1.2	0.5	4.9	5.9		
Subtotal	9.9	20.6	15.9	10.2	56.7	68.0		

[1] Use 1.2 multiplier. See page 28 of source

Source: An Interim Evaluation of the Offshore Installations (Safety Case) Regulations 1992, HSE, 1995.

Table ID-15 - Taylor SEMP Incremental Manhours and Costs

Description	Manhours	Costs
Non-Site-Specific Items:		
SEMP Manual, Safety Manual, Safe Drilling and Workover Practices Manual, Safety Handbook	325	$20K
Site-Specific Items (per platform):		
Safety & Environmental Information	150 - 1,050	$7K - $48K
Hazards Analysis	100 - 425	$6K - $28K
Operating Procedures	100 - 180	$5K - $9K
Mechanical Integrity (third-party wall thickness measurements)		$3K - $5K

Source: Jay T. Hoyle and J. David Dykes: "DOE/Taylor Safety and Environmental Management Program (SEMP) Case Study," 1997 Offshore Technology Conference

Thus, adding a requirement in the U.S. to perform Safety Cases and requiring calculation of individual risk rates would have a significant impact on engineering costs for new designs with no discernable increase in safety. Indeed, it is possible that after SEMP is fully implemented in the U.S., the level of safety may be equal to or better than that experienced in the U.K. at a cost which would allow the continued development of high cost marginal U.S. reserves.

~~As was the case for structures, the MMS regulatory regime has proven to be extremely cost efficient. The cost to document compliance with regulations governing the design, construction, installation and operation of production facilities for U.S. locations is lower than any other location where the requirements of other regulatory regimes must be met.~~

II. Examples of Risk ~~Analysis~~ Assessment and Management

In this section we describe examples showing how QRA and other risk ~~analysis~~ **assessment** and risk management techniques are currently being employed in the offshore industry. These examples are not meant to be all-inclusive or to describe how such techniques could be applied in other areas. They are presented to show that the idea of risk assessment and risk management is not a new thought to this industry and that various techniques are currently employed.

A. Using QRA to Establish Individual Risk Rate (IRR)

As described above, it has become the industry norm in Safety Cases to develop an individual risk rate (annual potential of loss of life for an individual working on the platform) to prove that the risk associated with a specific platform is ALARP. An example of now individual risk rates are calculated in a **specific** U.K. Safety Case is presented in Appendix C, and an example of how they are calculated in a **specific** Australian Drilling Safety Case is described in Appendix D. **Of course each individual safety case is different and these are presented only for illustrative purposes and not to imply that there is an approved procedure to perform a specific safety case.**

In calculating the individual risk rate there are problems in identifying ~~every possible relevant~~ scenario **groupings**, and uncertainties and assumptions regarding "correct" probabilities of failure or risk events. For example, **it is possible for the evaluator to incorrectly estimate** the probability of **a gas** leak for **a** compressor **using** data for liquid seals ~~or older design dry gas seals because the data exists,~~ when the specific design has a ~~newer design~~ dry gas seal **and for this to be overlooked because it is buried in the analysis.**~~is wrong on its face. Yet, some data sets do not distinguish these subsystems nor do some analysts~~. In the absence of high quality data, **either data may be used incorrectly, or there may be a heavy reliance on** ~~which is endemic in the industry,~~ "expert" judgment ~~is often used~~. The experience, knowledge, biases, and qualifications of **experts can be** suspect (see discussion on Qualitative Methods below), **and the IRR calculated may take on a legitimacy which it does not deserve.**

In making the **IRR** calculation, it is generally necessary to use or create a situational mathematical model. Some aggregation of scenarios, probabilities of event occurrences and/or probabilities of consequences are needed to reduce the calculation to manageable levels. The reasons for the need to simplify range from poor knowledge and understanding to lack of adequate computational capacity. Thus, errors may creep into the analyses, traceability of cause and effect through the calculation process may be lost, and it may be impossible to verify or calibrate the results with real experience.

The heavy reliance on QRA to establish an IRR and the use in turn of this analysis to show that the design and operation results in risks that are as low as reasonably practicable grew out of the Piper Alpha fire. It is generally conceded that the immediate cause of the accident was a failure of the lockout-tagout procedures which would have indicated that a relief valve had been removed for testing. To understand how an emphasis on calculating IRR and concentrating on proving ALARP can focus attention incorrectly, it is necessary to discuss the Piper Alpha accident in more detail.

Figure 1A is a schematic of the relief valve installation. Once a year the relief valve must be removed from service and bench-tested to assure it will open at the correct setting. When this is done, blind flanges must be installed to assure gas does not leak out the open pipe either form the protected equipment or from the relief header. To remove the valve, the protected equipment as well as well equipment tied into the relief header must be shut down and depressured. Once blind flanges are installed, the equipment tied into the relief header can be started up, and the protected equipment can be started up if it has a backup pressure relief device. After the valve has been tested to assure that it still opens at the proper set point, the procedure is reversed.

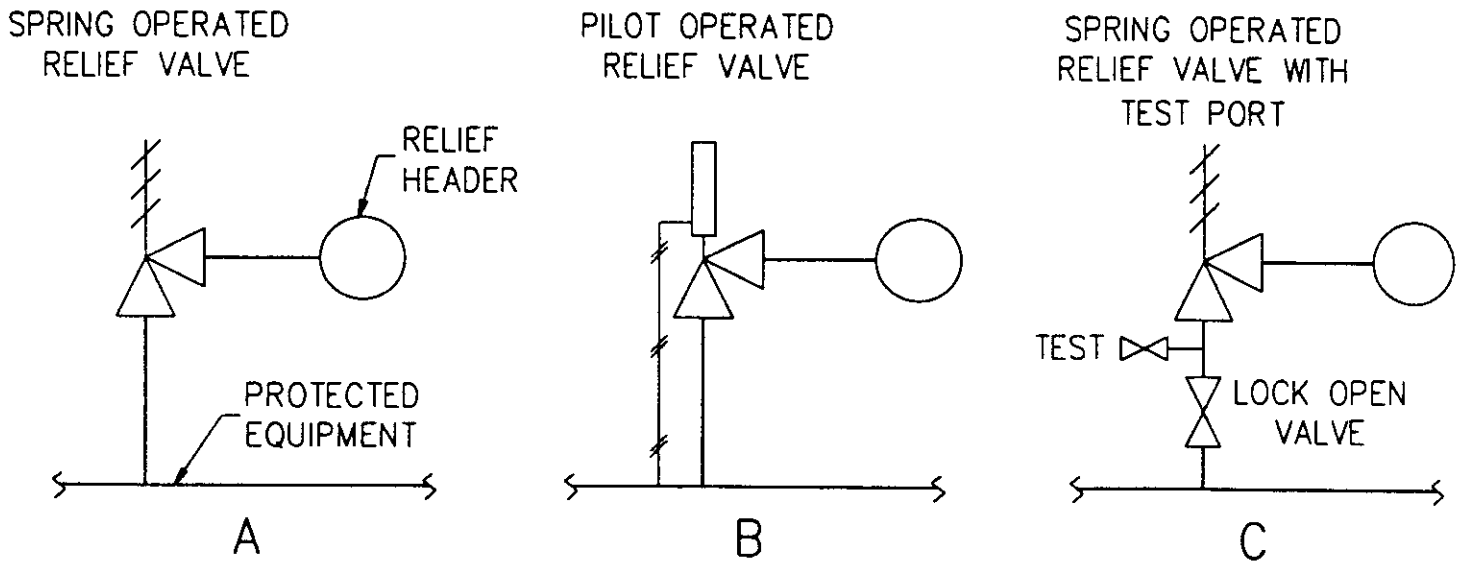
Figure IB shows a similar installation with a pilot operated relief valve. It is possible to equip the pilot with a test connection. To test the valve set point, pressure is put on the test connection and the pressure at which the pilot trips is recorded. This can be done without removing the valve, but the procedure does not physically test that once the pilot trips, the valve will open.

Figure 1C shows a relief valve similar to the one in Figure 1A. To test this valve, the lock-open isolation valve is closed and pressure put on the test connection. At the end of the test, the isolation valve is opened. If this valve is inadvertently left closed than the relief valve will not protect the equipment.

There are many other potential installations which allow in-place testing of relief valves using isolating valves, check valves, three-way valves, etc. In the Gulf of Mexico most relief valves are tested in-place once per year. It is extremely rare that valves have to be removed for repair as a result of failing the test. Bench testing relief valves is rarely, if ever, done. A review of MMS events records for a nine year period uncovered no events which were caused by the failure of a relief valve to operate.

Figure 1

EXAMPLE ALTERNATE RELIEF VALVE INSTALLATIONS



Even though the driving force behind calculating IRR in the North Sea was an event which occurred only because it was required to annually remove and bench test relief valves, few if any calculations of IRRs have identified the need to evaluate alternative testing of relief valves. The human factor drivers associated with the task of removing a valve for bench testing and the potential for saving time by failing to follow correct procedures (e.g. not shutting down and depressuring all equipment tied into the relief headers, failure to install gaskets and all bolts on blind flanges, failure to tighten all bolts with sufficient torque) have rarely, if ever, been identified as significant events for which there is a potential design, as opposed to a procedural, fix. If such an analysis had been done in any of the Safety Cases performed to date, it has not been made available as guidance to those in industry who have to make a choice on the proper way to install relief valves.

B. Using QRA for Structural Risk ~~Assessment~~ **Analysis**

Structural risk ~~assessment~~ **analysis** uses probability theory to determine the risk of loss of platform due to environmental loads. **Although the term "structural risk analysis" is common in industry it is perhaps more appropriate to refer to this as a "structural reliability analysis."** An example of structural risk ~~assessment~~ **analysis** to determine the effect on probability of loss of structure as a function of inspection frequency is described in Appendix A. The results of this analysis were to point out that the failure rate met a certain target and that frequent inspections had only a small impact on failure rate.

This type of analysis relies upon the accuracy of current knowledge regarding structural forces and effects. Current knowledge, however, may not be **as** accurate **as we believe it to be** in regard to estimating the probability of future environmental disturbances or loads. Thus, the **calculated** probability of failure may not be as accurate as we believe and may indeed change over time as our understanding increases of environmental loads and structural

responses. **Uncertainty analysis could be used to better understand structural risk, but this presupposes that we can somehow describe the uncertainty of our knowledge of environmental loads.**

As with most "structural risk assessments," the **example** study does not look at operational risks which could affect structural integrity nor does it address the potential risk of loss of life.

C. Using QRA to Assess Relative Risk Between Two **or More** Alternatives

Often special studies are performed to identify the potential risks associated with selection of design alternatives for a small system or sub-system. These studies do not normally include an evaluation of overall risk to an installation, but rather the incremental risk associated with selecting one alternative over another. ~~Appendix B includes a discussion of one such study~~. As a result of this limitation in scope, these studies are not as susceptible to the uncertainties inherent in broader studies which attempt to assess the total risk to loss of life from all causes.

There is a growing tendency within industry to use QRA studies to make design choices. Indeed, it has been suggested that one of the benefits of the heavy use of QRA in Safety Case studies is that it has shown design engineers the power of a QRA study to aid in making design choices.

Appendix B shows a case where QRA was used to determine if an increased expenditure to reduce the risk of a specific event from occurring was appropriate. This is typical of most of the QRAs which have been performed to date.

However, in many instances decisions to add cost to a design in order to reduce the risk associated with an identified event, may increase the total risks by making another event more probable. If the QRA is not done properly or completely the detrimental event whose risk was increased by the "fix" may actually add to overall

risk. For example, a fire in the process area of a typical Gulf of Mexico platform could cause secondary damage to the wellhead area if it is not protected by a firewall. However, a proper QRA must consider that the firewall will impede ventilation which could cause a small gas leak in the process area to become more dangerous and lead to an overpressure situation on ignition which could be more dangerous to the wellheads than a mere fire in the process area. Although such secondary conditions are often overlooked in the analysis, this is by no means an indictment of QRA as a valuable technique in making choices between alternatives. It is merely presented here to emphasize that the completeness of a QRA must be assured before the results are accepted.

It becomes even more difficult to chose between alternatives when human and organizational factors (HOF) play a major role in understanding the risk of one or more of the alternatives. For example, in analyzing alternative relief valve hookups as described in Section IIA, assessments must be made of the risks associated with failure to follow correct procedures in depressuring, isolating equipment, lifting and transporting the relief valve, installing blind flanges, communicating between operating, maintenance and instrumentation staff, etc. It is not sufficient to merely look at the decrease in risk due to the increased reliability of the relief valve which might result from removing it for servicing and bench testing.

Once again, QRA is a valuable tool for performing such an analysis. However, care must be used to assure that HOF factors are correctly included in the analysis before the results are accepted.

D. Using Historical Data to Infer the Probability of an Event

In a quantitative risk analysis, the probability of an event is calculated using one of the techniques described in the chapter on methodology, and consequence modeling is performed to assign an overall value for an individual risk, environmental consequence or economic loss associated with that event. Because of the difficulty in identifying all

possible significant events and of modeling the range of consequences associated with each event, there have been several attempts made to determine probability of a specified event **and overall risk using historical data for the industry as a whole.**

An example of this approach was undertaken by the MMS in a project entitled Facility Assessment, Maintenance and Enhancement (FAME) in 1992.[5] FAME analyzed the MMS data on fire and explosions on producing facilities. A data base of 383 fire and explosion accidents that occurred in the nine year period between 1981 and 1990 was developed, and an attempt was made to assign an initial cause from the one paragraph descriptions of each accident. This database was merged with platform population databases, which contained data on all current and removed platforms in the Gulf of Mexico including platform age, equipment listing, quarters size, operator, location, etc. The merged database permits detailed analysis of a number of risk factors on the basis of population data.

Unfortunately, the project was canceled before detailed analysis could be undertaken. However, the following preliminary conclusions can be drawn:

1. Initial causes are shown in Figure IIC-1. Further analysis of these causes was not undertaken.

2. The fire and explosion incident rate decreased significantly over the period as shown in Figure IIC - 2. Whether this is due to lower construction activity, change in platform equipment mix or better safety procedures was not investigated.

3. Figure IIC-3 indicated that probability of fire and explosion is not correctable to age. If anything, there may be a negative correlation.

[5] "Introductory Study to Develop the Methodology for Safety Assessment of Offshore Production Facilities, R. C. Visser, Belmar Engineering, 1992.

Figure IIC-1

Distribution of fire and explosion causes.

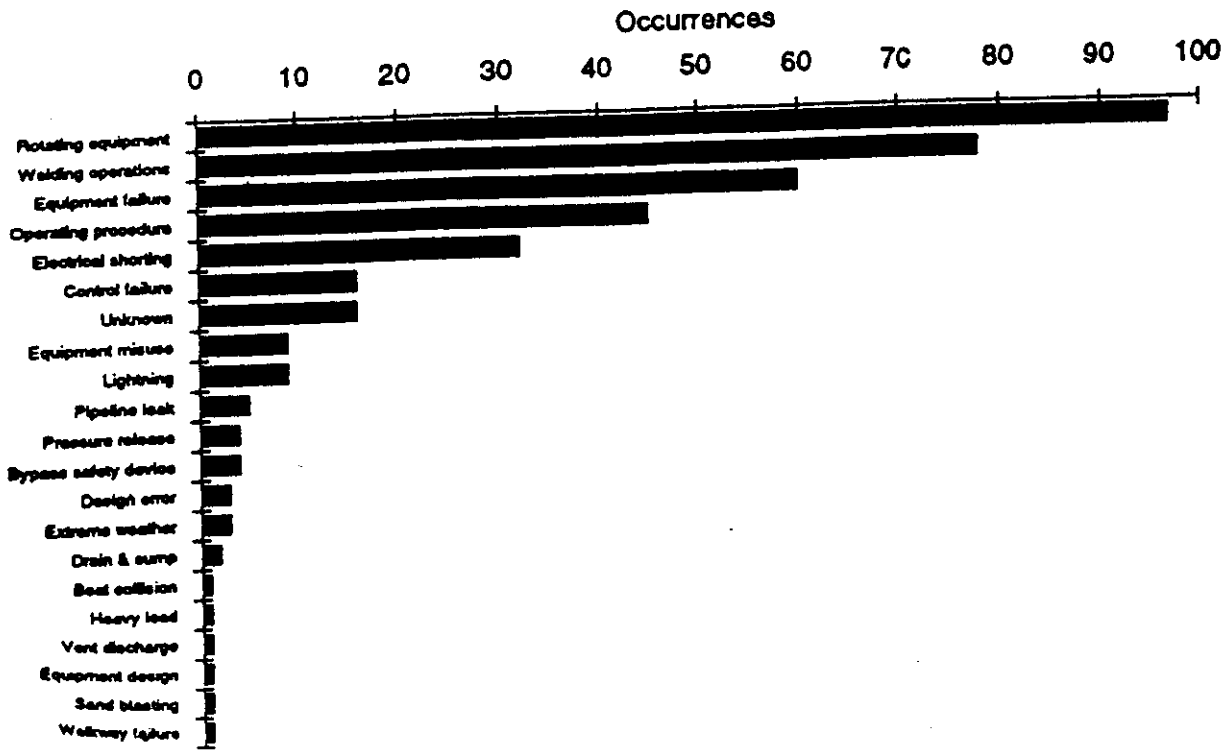


Figure IIC-2

Annual fire and explosion incident rate on Gulf of Mexico OCS platforms.

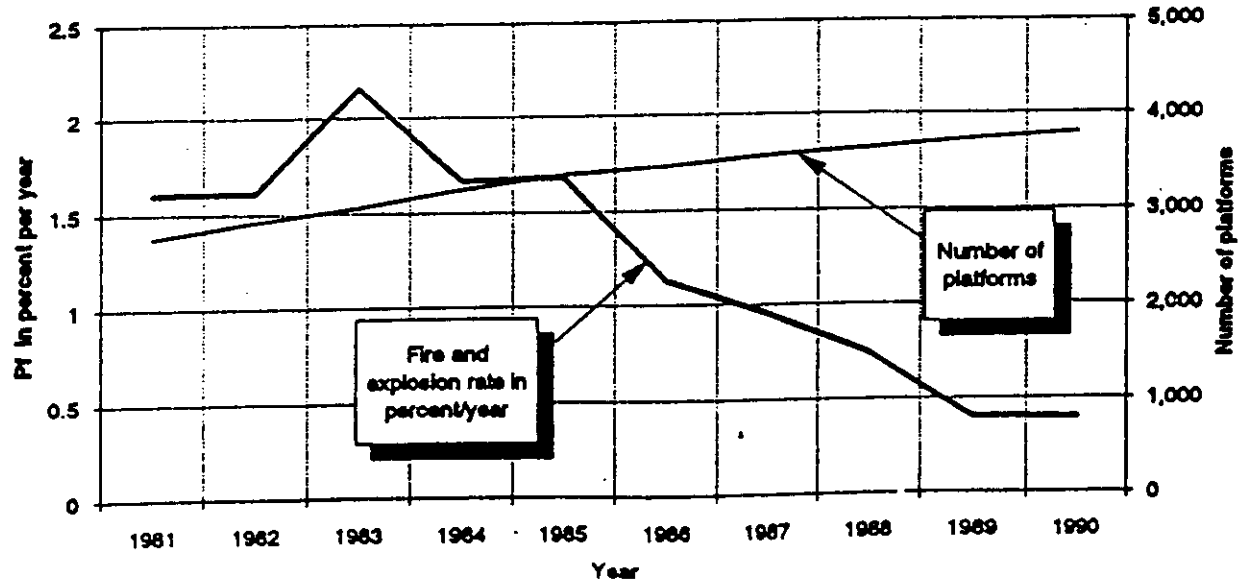
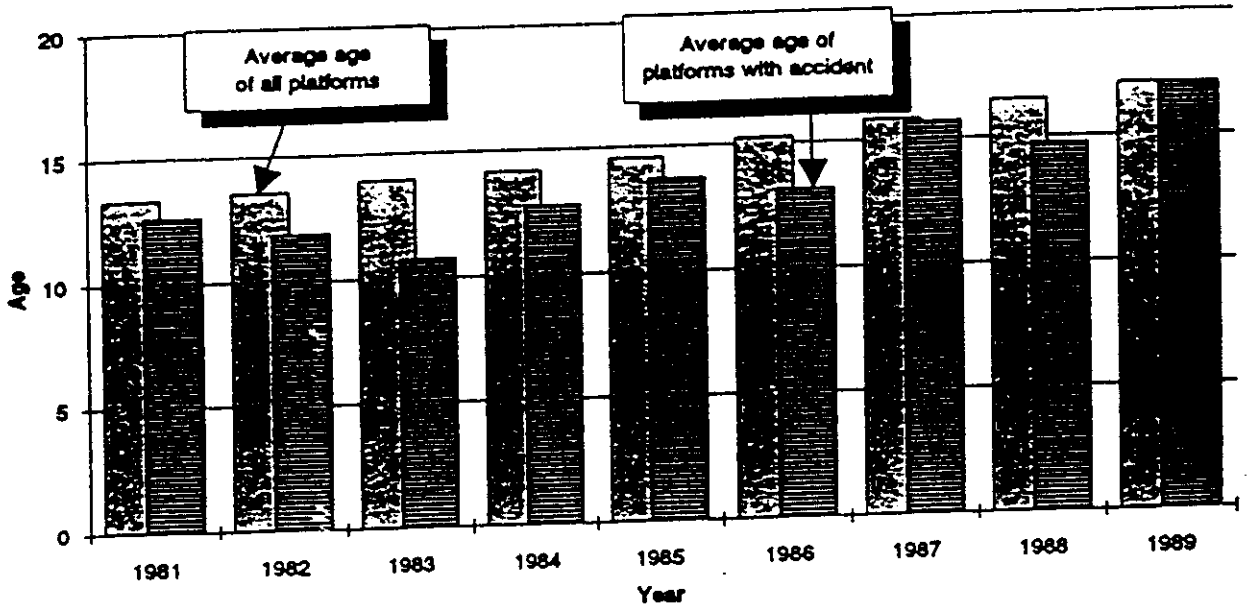


Figure IIC-3

Average age of all operating platforms and average age of platforms with a fire or explosion by year of occurrence.



4. Figure IIC-4 indicates that platforms with certain equipment types are more likely to experience fire or explosion than the average of 0.5 percent per year for all other platforms over the nine year period.

5. Table IIC-1 shows that many platforms with compressors have experienced multiple incidents, but whether this is correlatable to operatorship, type of compressor, facility size, equipment complexity, etc., has not been evaluated.

6. Between 1983 and 1990, there were eight process equipment related fires which resulted in "major damage" (over $100,000), which results in an incident rate of 3×10^{-4} per year. There was one total loss of platform from explosion or fire ~~which resulted in a rate of 4×10^{-5} per year~~.

Data from the FAME database has been used to evaluate probability of damage to a specific platform due to fire and explosion from the process equipment. This was done by determining the probability of (1) fire and explosion, (2) major damage, and (3) total loss for platform having similar equipment and modifying that for the experience of the operator.

Paul to provide write up on INC study

FAME indicated that platforms which had compressors on them were much more likely to have fires. However, this information was never evaluated to determine if there was some learning as to the design or operation of compression systems which could be derived from looking in more detail at these fires. Is it that platforms with compressors tend to be more complex and it is not the compression system itself that is causing these fires? Do some operators experience a higher rate of fires with their compressors than others? Is there a problem with engine starters, exhaust systems, electronic ignition systems, packing vents, etc., which could be addressed by revised codes and standards?

The use of historical data can provide insight as to overall risk due to industry activity such as oil spilled per barrel produced, fatalities per barrel produced, etc.

Figure IIC-4

Average annual fire and explosion incident rate on platforms with listed equipment.

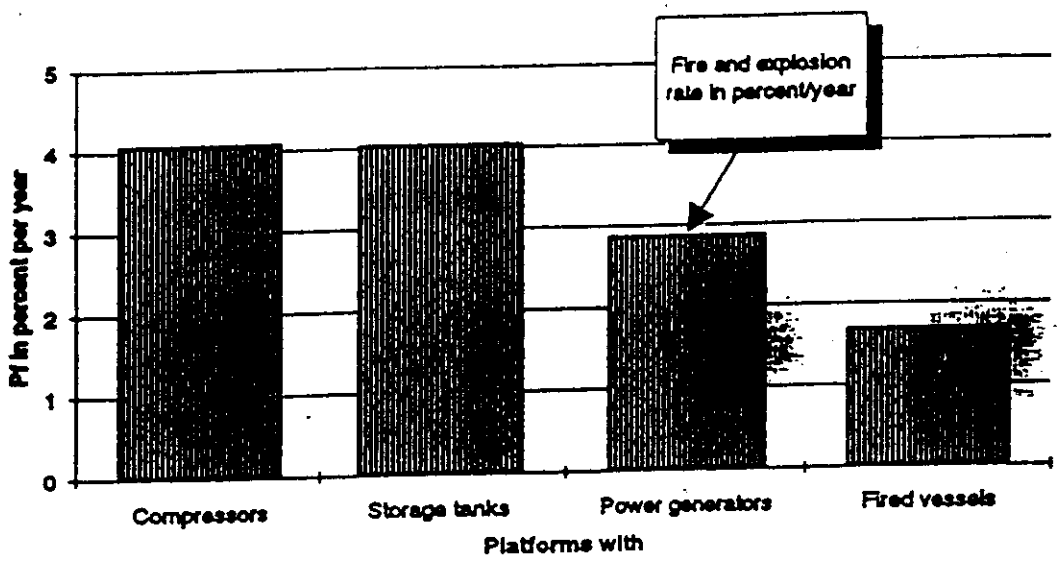


Table IIC-1

Distribution of fire and explosion incidents on platforms with compressors.

Incidents per platform	Number of platforms
1	97
2	42
3	13
4	3
5	2
6	0
7	1

This type of information has been valuable in understanding overall risks associated with oil production, However, formal studies of historical data have not been undertaken nor used as well as they could have been in developing codes of practice and standards by analyzing actual causes and consequences of accidents.

E. *Use of* Qualitative Risk Analysis

There are various scopes of risk assessment depending on the hazards involved, the threat to public and worker safety, and the complexity of the system. Due to the difficulty and time consuming nature of attempting to develop a quantification of risk, various studies have been performed to identify risk in a qualitative fashion. **Hazards analysis studies of process systems (Section IIG) are qualitative in nature, although they may lead to specific QRA studies to choose between alternatives. Indexing methods (Section IIF) are qualitative techniques which employ the mathematical manipulation of relative values or rank ordering lists to achieve mathematical consistency of interpretation.**

Qualitative methods are used to develop a solution to a problem via the expressed opinion of an experienced, knowledgeable, and credible authority figure or expert such as a Chief Engineer or group of advisors/consultants. Usually the problem is viewed to be complex and not easily susceptible to straightforward and complete objective analysis. The method, therefore, is characterized by the exercise of a high degree of judgment and the weighting of numerous imponderables to express the likelihood or probability of various outcomes. In practice, the usual method is framed by assessment of assumptions and is supported by quantitative analyses of elements of the problem. These are evaluated interactively by the expert (or a group of experts jointly) to yield a solution (or develop a consensus).

The solution is typified by the use of terms which are imprecise (for example: High, Medium, Low likelihood) or comparative (such as the probability of an incident is "similar to" that of some other incident). These methods may be expressed in

numerical terms having apparent precision. However, deeper analysis of the method will reveal a high judgmental content and/or an arbitrary, but perhaps reasonable, transliteration of an imprecise term into an apparently precise term.

~~Even though there may be considerable numerical content in the statement of the problem and in the supporting analyses, the solution is expressed in non-quantitative terms regardless that numerical assignments are made. For example, the likelihood of a particular oil spill event may be expressed as High, Medium, or Low and these terms stated or graded as numerical probabilities according to some corresponding scheme (e.g., High = >90%, Medium = 75-90%, Low = <75%). Or, a rank ordering of platform operations failure events is defined and the numerical position of the item in the ranking may be used as an input to some mathematical function (e.g., the development of a the relative cost-effectiveness of different mitigation actions~~

Several points are worth noting. All methods of analysis, including numerical methods, include in the analyses some aspects of ***a qualitative*** method. For example, **in the Australian Safety Case presented in Appendix D, the hazard identification portion of the work, including the severity ratings, occurrence frequencies, risk matrix (likelihood vs. severity), and selection of major accident events (MAE) for more detailed analysis, which support the quantitative analyses of risk were generated by a group of experienced personnel on a consensual basis using their experienced judgment applied to the situation at hand.**

Qualitative methods do not, in general, permit traceability within the analysis, i.e., the determination of the nature of the result as a specific function of the input. Consequently, its applicability and use for decisions of such matters as the relative or absolute cost-effectiveness of specific solutions to a technical operational, policy, or regulatory problem is very limited and must be done with great care.

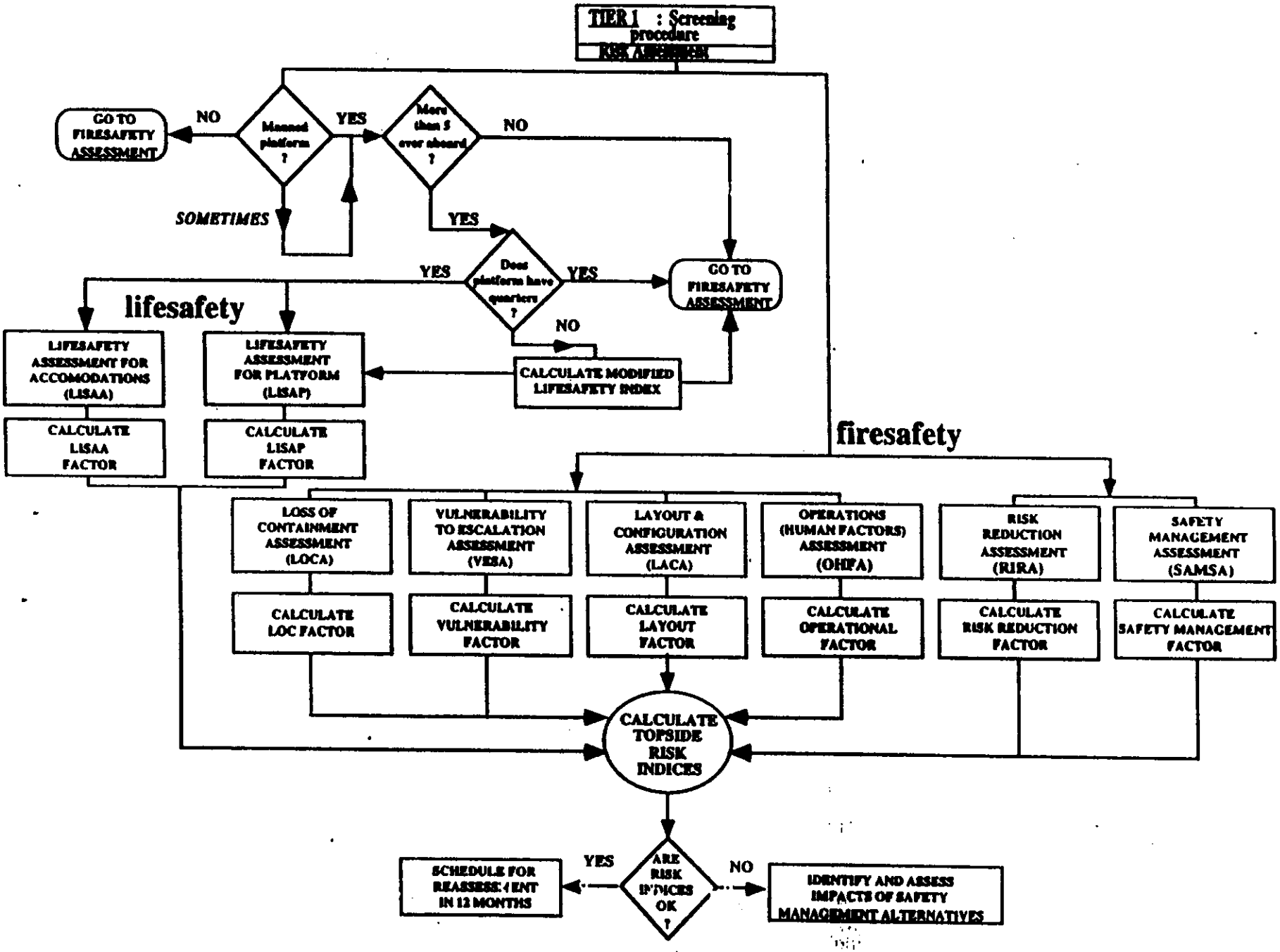
In seeking expert opinion and interpretation ~~of experience, the nature of the authority figure(s) must be evaluated~~ **the real issue is the evidence used by the expert in formulating an opinion.** It is likely that experts are biased and/or limited by the particular circumstances of their experience, customs, traditions, and standard practices. This ~~is of~~ **may be** particularly of concern when issues of Human Factors as a causative element are significant.

A major factor in the application of ***qualitative methods,*** requiring great care, is the influence of motivations and agendas divorced from the immediate problem. For example, an ~~authority figure's~~ **expert's** opinion may be strongly distorted by his desire to provide a solution which management might find to be pleasing, perhaps by overly weighting cost as an evaluation parameter. Such influences are not ordinarily perceptible. In addition, recent catastrophic and highly visible incidents usually have disproportionate influence on decisions. ~~especially those of policy and regulation. This is because a major concern of decision makers, who are generally less technically and operationally knowledgeable and experienced, is to satisfy the often poorly founded fears of their constituencies.~~

F. ***An Example of an*** Indexing Methodology

An example of an attempt to assess risk in a qualitative sense is the joint industry project FLAIM (Fire and Life Safety Assessment and Indexing Methodology) which was developed by University of California at Berkeley. ~~FLAIM can best be described as a qualitative risk assessment indexing methodology in which~~ Selected key factors relevant to fire safety and life safety are identified, assessed and assigned numerical (weighting values). Risk contributing factors are thereby indexed and ranked using a weighting system algorithm, keyed to relative (comparative) risk, to yield a set of risk indexes, and an overall risk index for the facilities. Figure IIF-1 serves as an overall 'road-map" to FLAIM's methodology. ~~Eight separate risk assessment modules, each of which yield individual risk indices used to calculate an overall risk index, drive FLAIM's algorithm. The adequacy of risk reduction measures and modifications to the platform Safety~~

Figure 11F-1


TIER 1 : Screening procedure
RISK ASSESSMENT
GO TO FIRESAFETY ASSESSMENT
NO
Manned platform ?
YES
More than 5 ever aboard ?
NO
SOMETIMES
YES
Does platform have quarters ?
YES
YES
GO TO FIRESAFETY ASSESSMENT
NO
lifesafety
LIFESAFETY ASSESSMENT FOR ACCOMODATIONS (LISAA)
LIFESAFETY ASSESSMENT FOR PLATFORM (LISAP)
CALCULATE MODIFIED LIFESAFETY INDEX
CALCULATE LISAA FACTOR
CALCULATE LISAP FACTOR
firesafety
LOSS OF CONTAINMENT ASSESSMENT (LOCA)
VULNERABILITY TO ESCALATION ASSESSMENT (VESA)
LAYOUT & CONFIGURATION ASSESSMENT (LACA)
OPERATIONS (HUMAN FACTORS) ASSESSMENT (OHFA)
RISK REDUCTION ASSESSMENT (RIRA)
SAFETY MANAGEMENT ASSESSMENT (SAMSA)
CALCULATE LOC FACTOR
CALCULATE VULNERABILITY FACTOR
CALCULATE LAYOUT FACTOR
CALCULATE OPERATIONAL FACTOR
CALCULATE RISK REDUCTION FACTOR
CALCULATE SAFETY MANAGEMENT FACTOR
CALCULATE TOPSIDE RISK INDICES
ARE RISK INDICES OK ?
YES
SCHEDULE FOR REASSESSMENT IN 12 MONTHS
NO
IDENTIFY AND ASSESS IMPACTS OF SAFETY MANAGEMENT ALTERNATIVES

~~Management System can be assessed by determining the effect these changes have on the overall risk index.~~

This procedure has not yet been applied and calibrated. It contains approximately 1,500 questions in the eight assessment modules. Currently there is a revised tool being developed by an industry program to enhance the human and organization factors analysis portions of the FLAIM program and to develop a more user friendly screening tool. ~~This effort is expected to result in field testing of several platforms and marine terminals in 1997. The effort is sponsored by the America Bureau of Shipping, Chevron, California State Land Commission - Marine Facilities Division, U.K. Health & Safety Executive, U.S. Minerals Management Service, National Energy Board of Canada, and Texaco.~~

G. ~~*Qualitative*~~ Hazards Analysis ***for*** Risk Management

Most of the higher level of risk analysis techniques start first with a process of hazard identification. Often the risks associated with the hazard and the solutions to mitigate the hazard are so well known that **a simple** hazard ~~identification~~ **analysis** technique by itself can be used as a risk management tool. The American Petroleum Industry has published Recommended Practice for Design and Hazards Analysis for Offshore Production Facilities (RP 14J) which provides guidelines for hazards analysis of offshore production facilities. ~~The following are quotes from RP 14J. Quotes were removed.~~

In reviewing the various techniques available for performing hazards analysis, the API concluded that "production facilities are generally simple, standard processes with vast amount of operating experience and a relatively low inherent risk." A series of "standard procedures, recommended practices, company standards and regulatory requirements" represent good practices based on lessons learned from "previous designs, hazards analyses, and accident and incident investigations... A high level of safety can be achieved by checking for compliance with these standard practices in design, construction, operation and maintenance."

The API recommends that a checklist approach be used to check the design for compliance for good practice. The use of more sophisticated techniques should be limited to analyzing "new processes, complex control systems, toxic material processes, [and] unusually high risks to personnel or environment," and even then these techniques should supplement and not replace a checklist or other technique which "checks for the same level of compliance with standard practice."

Typical problems identified in hazard analysis of offshore production facilities include: safety shut-down devices not installed as per API RP 14C, inadequately sized relief valves, tanks which can be subjected to overpressure if valves are inadvertently left open, drain systems which allow vapor to mitigate to unsafe areas, piping which fails to meet the pressure rating requirements spelled out in RP 14J, etc. In all these cases there is no need for a more elaborate risk assessment because the fix is well known and relatively inexpensive compared to the possible consequences. Modifying the equipment to comply with good design practices reduces the risk to what has historically been acceptable is a level as low as reasonably practicable concerning the particular risk scenario.

The SEMP system which is being encouraged by the MMS in the U.S. takes this approach for managing design risk. The approach does not preclude the use of QRA. Rather, it makes the assumption that there are many aspects of design which can be automatically provided that do not need a QRA to prove that they are cost efficient in reducing risk to people, the environment and assets. These include such things as providing relief valves, putting pipe specification breaks in the right location, providing fire and gas detection systems, separating ignition and fuel sources in the layout, providing escape paths, etc. On the other hand, there are many uses for QRA where standard practice is not definitive and QRA can be used to aid in making choices between alternatives. Two examples discussed above where QRA could be useful include the best way to hookup a relief valve and when to install a firewall. QRA could be used on a case by case basis or in a wider study such as the one suggested in Section III to develop new codes and standards by evaluating better ways to design compression systems.

III. ~~Conclusions and Recommendations~~ Findings

1. **The use of QRA has a number of potential benefits. QRA can be helpful in choosing among alternatives such as the example described in Section IIC, and for assessing the probability of a specific defined event such as described in Section IIB, particularly when new technologies or environmental conditions are encountered. Where a ~~simple preliminary estimate (e.g. via HAZOPS)~~ hazards analysis identifies potentially significant risks or consequences that demand more detailed understanding, QRA can also be valuable in identifying safety-critical components, systems, and processes.**

2. **At the same time, QRA's limitations should be recognized. Uncertainties in data and assumptions ~~(including scenario identification and consequence analysis)~~ may result in significant ~~errors~~ uncertainties in estimated risk which need to be identified in the analysis. The process requires significant effort in gathering data and understanding consequences and, as described in Section IIA, the resulting benefit may not justify the expense.**

   Assumptions should be clearly stated and uncertainties should be quantified, but because the calculation may be intricate and voluminous these may not be as easy to audit and understand. For example, to understand the risk associated with a leak from the HP Separator on Brae, the event tree (Figure 6 of Appendix C) must be understood. This contains many probability numbers which are in term backed by some combination of data and opinion which must be understood. It is then necessary to understand the basis for the most probable leak rate and how this is used in calculating the consequences for each of the final outcomes in the event tree.

3. **~~With the regard to~~ While the use of QRA to establish that a level of risk as low as reasonably practicable (ALARP) has been established is intuitively attractive, there are several ~~serious~~ problems with this approach.**

In implementing ALARP, the individual risk rate (IRR) is calculated as a function of the material or procedural change required to achieve that IRR. The cost of making this change is calculated and the monetary benefit of the change relative to the potential probabilistic failure consequences is subtracted. This leaves a cost increment associated with the change which is normalized to an individual life at risk - the Implied Cost to Avert a Fatality (ICAF). The ICAF is then compared with the value of **lowering risk to** life to provide the basis for a judgment regarding the acceptability of the IRR. **There may be a tendency on the part of the evaluator to** overestimate the cost of change and underestimate of the value of lowering the risk of human life. This, in turn may lead to a potential tendency to select a higher IRR than otherwise.

Finally, there is the problem of assuring that the right set of changes is hypothesized and tested to arrive at ALARP. As explained in Section IIA the way in which relief valves are installed could significantly impact IRR at a minimal cost, and yet this has rarely been considered in establishing ALARP.

4. **The U.S. practice avoids the calculation of individual risk rates. For novel structures, often a structural risk assessment is performed to assure that total loss of structure due to environmental loads and sometimes collisions meets a predetermined criterion, and QRA may be used to make a selection between specific design alternatives. However, for risks associated with process or drilling scenarios, it is assumed that following good engineering practice will result in an "reasonable" risk. The problem with not calculating individual risk rates for each installation is that while it may be possible to derive overall historic risk rates for the industry, the risk rate for any single installation is unknown.**

On the surface it is difficult to understand why this approach is used rather than relying on QRA to establish ALARP as is done in the U.K. However, from a practical standpoint, the differences may not be as great as they first appear. The U.K. regime was developed primarily for installations which are large, difficult to evacuate and, for

the most part, manned with large crews. The U.S. regime was developed primarily for installations which are much smaller, relatively easier to evacuate and, for the most part, unmanned or manned with much smaller crews. The size of most U.S platforms is such that it would be impossible to fight a major fire even if it were desirable to do so. In the U.K., on the other hand, it may be necessary to fight a major fire, or at least to survive in temporary safe refuge area until evacuation can be organized.

As a matter of custom the good engineering practice concepts of the U.S. have become a starting place for the design of U.K. installations, and the bulk of the risk analysis that goes into establishing ALARP has to do with calculating the risk associated with fighting a fire or surviving in a temporary safe refuge until evacuation can be organized. The procedures used in the design, operation and maintenance of wells, structure and process systems are very similar in both the U.S. and U.K. with the exception that as a general rule greater documentation of QA/QC in construction and more frequent inspection of pressure vessels is required in the U.K.

5. Prior to the adoption of Safety Cases in the U.K. and SEMP in the U.S., safety indices such as those shown in Tables ID-10 and ID-11 indicated that the level of safety in the U.S. was approximately the same as that in Europe. As shown in Table ID-12, there appears to be a significant improvement in safety in the U.K. as a result of adoption of the Safety Case regime. Clearly the adoption of SEMP will focus attention on managing safety in the U.S. and should therefore increase safety. However, it is too early to prove this from available data. Some anecdotal evidence (such as Table ID-13) indicates that significant improvements in levels of safety may be possible and a SEMP-based system in the U.S. may result in safety levels which continue to be comparable to those in the U.K.

6. Benefits in design and operational processes might be achieved by describing potential risks and mitigations along the lines of the U.K. and Norwegian Safety Cases. Participants in such analyses have generally agreed that the endeavor is helpful by forcing structured thought about accident scenarios and mitigation measures. Such

analyses might be particularly valuable for the few large, remote deepwater U.S. facilities that present significant risks of fire or other hazard and from which timely evacuation would be difficult.

IV. Conclusions

1. The design and safe operation of an offshore platform relies heavily on engineering knowledge and company culture.

2. The UK Safety Case approach provides text-book oversight of how to organize to design and safely operate an offshore installation. It does not provide the detailed guidance needed to actually carry out the design, nor does it provide a tool to a capture experience so that mistakes shall be avoided in the future.

   It would be of concern if the idea were to take hold that the Safety Case approach and the use of risk assessment were together all that is now required for the safe design and operation of offshore platforms.

3. The ability of regulations to ensure safe operations should not be overestimated. The main advantages of regulations are (a) to provide a structure within which sound design and operating decisions will be made, and (b) to ensure that safety considerations are given due weight in the design and operating process.

   Regulations should be goal-setting, but they also provide legitimacy and support to the engineer who is challenging a ranking of risk or what may appear to be an unsafe practice.

4. The detailed engineering knowledge to which designers and operators must refer for all except prototype designs and new operations is properly captured in industry codes and standards which must be kept up to date.

"Failure to learn" has been identified as one of many contributors to the Piper Alpha disaster (Pate-Cornell, 1992). Ensuring that failures and near misses get properly recorded so that this knowledge is readily available to future engineers and designers is essential. Keeping industry codes and standards up to date is one way to achieve this for design and material and equipment failures.

For instance, many learnings from the Piper Alpha disaster have been recorded (inter alia by Pate-Cornell, 1992), but at least until now few of these seem to have been incorporated into revisions of industry codes and standards. It is hypothesized this is due to the disenchantment with prescriptive guidance which immediately followed after Piper Alpha. While this is understandable, the real problem is that codes and standards are guidelines of good practice which must be available for reference, are ignored at ones peril but certainly should not be slavishly followed. Engineering is as safe as the understanding each individual engineer has of the principles underlying requirements in regulations, codes and standards. Blindly to follow requirements simply because they are written down is a recipe for disaster. However, not to have the guidelines available for reference means that past mistakes are bound to be repeated.

5. Risk assessment using qualitative and quantitative methods as appropriate is an engineering tool which should have high visibility and be used appropriately during design, operations and modifications (a) to ensure that the most serious risks are considered and mitigated (b) to ensure proper consideration of linkages, and (c) "proper design of safety redundancies" (Pate-Cornell, 1992).

Risk Assessment is not in and of itself a design check, nor should it be regarded as a substitute for establishing and recording in industry codes the need for back-up requirements for emergency and safety features, and sufficient prescription so that these do not always have to be designed from first principles for each new facility. Codes and Standards also provide legitimacy and support to the engineer challenging a ranking of risk or an apparently unsafe practice; to make such judgments based solely on risk assessment relies heavily both on individual expertise (which can not always be

guaranteed) and on establishing and then being able to maintain the proper company culture.

On the other hand, regulations and codes and standards cannot alone be relied upon as being sufficient. Acceptance and appropriate use of risk assessment helps guard against the equally inappropriate and equally dangerous situation of "everything being permitted unless explicitly forbidden" (Pate-Cornell, 1992).

6. QRA is an appropriate tool to evaluate and allow waivers from prescriptive requirements in regulations, codes and standards, where such requirements may not be appropriate for a specific intended use. This is a use of QRA which should be encouraged.

   It is not possible to write prescriptive requirements to cover every eventuality. Requirements as written may not be applicable to a particular situation, may be more costly than necessary to safeguard a specific situation, or may in fact be dangerous if strictly applied to a particular case. A case in point is whether or not to permit block valves in vent lines, which is specifically prohibited in some codes, but which might arguably have prevented the particular disaster which occurred on Piper Alpha. Whereas meeting the requirements of industry codes and standards may be "deemed to satisfy," the requirements of regulations, codes and standards should never be directly written into legislation and regulations. Regulations must also be given the ability to waive unsuitable prescriptive requirement where this is appropriate.

7. Risk assessment should consider organizational as well as engineering outcomes. There were, for instance, a number of organizational failures which contribute to the severity of the Piper Alpha disaster (Pate-Cornell, 1992), and the contribution of human factors to risk and disaster should not be overlooked.

8. The use of the UK Safety Case approach is most suited to large, complex facilities with couplings which could cause smaller incidents to escalate into major disasters. Large

North Sea platforms obviously fall into this category, as may a number of large fixed and floating facilities in other areas around the world. Whether the use of QRA to calculate an IRR is necessary in such cases depends upon the specific installation. Calculation of IRR may not be necessary for those installations whose hazards, and operations are not unique, and where results of previous studies and historical data are adequate to assess risk.

Out of a total of more than 7000 fixed platforms installed around the world since the offshore industry started in 1947, no more than 100 presently fall into this category. However, as industry moves worldwide into deeper water and more inhospitable areas, this number may be expected to increase.

9. There are a large number of platforms in the US and around the world properly built to existing (non probabilistic) codes and standards, for which the UK Safety Case and additional risk analysis is unnecessary and uneconomic. The structures are properly designed, built and operated to prescriptive industry codes and standards, which should be kept up to date.

10. Target reliabilities should not be set. The potentially different uses of risk assessment for design and operation, and for regulation should be recognized at this time, and any possible conflict between possibly conflicting objectives should be avoided.

    If the full benefit of risk assessment to improve safety and reduce risk is to be realized, then target reliabilities should not be imposed by regulation since (a) what can sensibly and realistically be achieved is still being determined, (b) there is a danger that target reliabilities become a goal beyond which it is not considered necessary to improve, and (c) risk assessment becomes a numbers game rather than a tool to improve general safety and to seek out and mitigate the highest risks.

11. High technology solutions must be designed, built and operated by informed technical persons taking into account regulations, industry codes and standards, tools such as

risk assessment and a wide personal background of knowledge and experience. On the other hand, low technology solutions are repeats of previous practice, and are appropriately designed from up to date codes and standards. Often, the difficulty is distinguishing between the two, and then appropriately staffing projects and operating groups.

12. The MMS should use the historical data in their data base to evaluate whether accident data indicates that changes in what is considered good design and operating practices are necessary. For example, a study of past compressor related fires could be undertaken. If trends are uncovered, QRA techniques could provide valuable insights in evaluating design or operational changes.

13. There is no basis to conclude that requiring a Safety Case approach to safety in the U.S. would result in a higher level of safety than will be obtained with the current SEMP approach. It has been demonstrated that requiring individual safety cases for each installation will be more expensive than the SEMP approach and it is possible that such a requirement could divert attention from the more important effort of improving codes and standards.

While the goal of making SEMP voluntary appear to have the laudable effect of focusing the operators attention on their responsibility for safety (as opposed to their responsibility to comply with a regulation), it is of concern that some operators are apparently making a minimal attempt at implementing SEMP. The SEMP concept is endorsed by every major industry committee. Therefore, it may be possible to conclude that unless an operator is actively implementing SEMP, the operation is not being "performed in a safe and workmanlike manner" (PINC G-110) and the necessary precautions are not being "taken to correct any oil and gas accumulation or other health, safety or fire hazards" (PINC G-112), and thus the operation violates 30 CFR 250.20. By issuing warnings, the MMS can help encourage compliance.

Appendix A

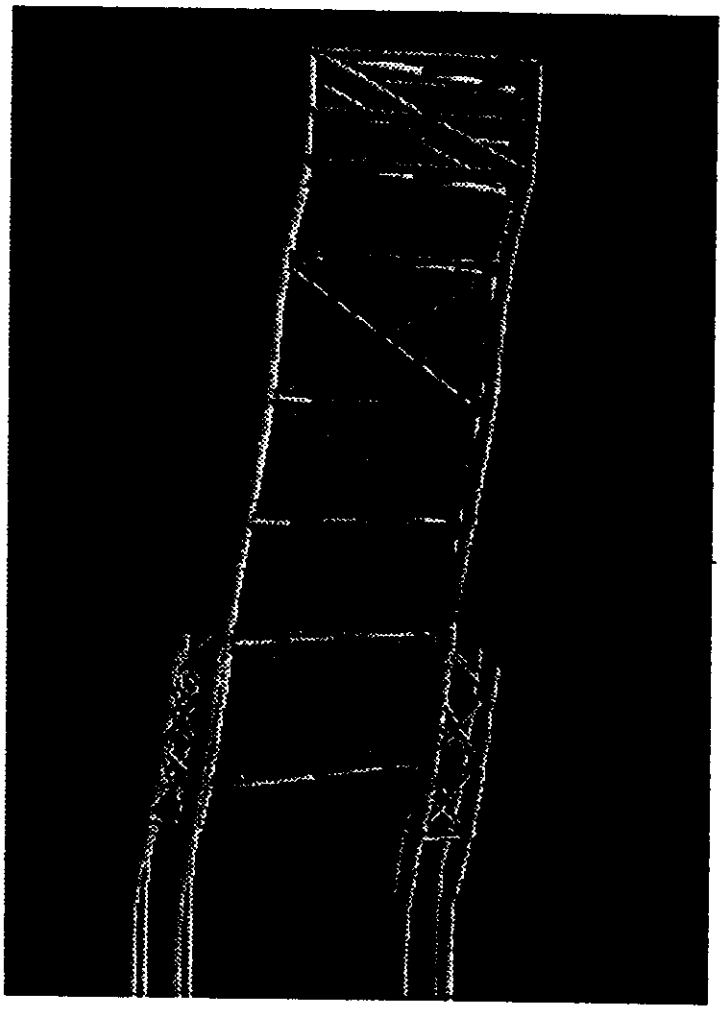
An Example Case of Using QRA for Structural Risk Assessment

To illustrate the application of structural reliability analysis, a study of a North Sea platform (Ref. 1) is presented. The study involved deterministic push-over analyses, and component and system reliability analyses of the platform under extreme loading and fatigue conditions. The variation of reliability of the platform with time was estimated, taking into account the deteriorating effects of fatigue.

Structural and Load modeling

The structure considered is a four legged, X-braced jacket supported on four leg piles and eight skirt piles. The computer model of the structure is shown in Fig. 1 in a near collapse condition. The jacket structure was modeled as a 3-D frame while the deck was modeled as a rigid, closed box at the cellar deck level, with the width (transverse to the wave approach direction) of the box chosen to provide an exposed area equivalent to the area of the cellar deck support structure, piping and processing equipment.

Figure 1: View of a North Sea platform in a state of stress



The tubular members were modeled as 2-nodded beam-column elements, the response of which includes hardening in tension and softening in compression. Joint strength modeling was based on empirical formulae with post-critical behavior assumed to be perfectly plastic. The pile foundation model involves a combination of calibrated linear elastic springs with non-linear axial pile elements.

Initially, the design-basis environmental loading was calculated based on a 50-year return wave combined with 50-year return current. A response surface for base shear due to environmental loading was developed by increasing systematically the wave height and current intensity. When the wave impinges on the deck, the loading on the deck was calculated as a function of the crest elevation.

Assessment of the Ultimate Strength

A deterministic collapse analysis of the structure was performed by systematically increasing the wave height and current intensity and including the loading on the deck. This approach provides a realistic load pattern and a non-proportional increase in loading. As the wave height is increased, initially some piles developed plastic hinges but the global failure of the jacket is caused mainly by brace failures in frames parallel to the wave approach direction. The collapse of the jacket occurs at a wave height of 39.9 m with the corresponding Reserve Strength Ratio (RSR) of 2.92.

Results of Reliability Analysis Under Extreme Environmental Condition

The jacket reliability analysis under extreme environmental loading is carried out using a failure tree approach. A number of load and resistance parameters are treated as basic random variables, with appropriate probability distributions as given in Table 1.

TABLE 1: PROBABILISTIC MODELING FOR THE EXTREME LOAD RELIABILITY ANALYSIS

Parameter	*Distribution type*	*COV*
Member capacity	*Lognormal*	*0.12*
Joint capacity	*Lognormal*	*0.15*
Pile capacity	*Lognormal*	*0.25*
Wave height	*Lognormal*	*0.15*
Wave period	*Function of wave height*	-
Current speed	*Lognormal*	*0.15*
Marine growth	*Normal*	*0.10*
Jacket wave force model uncertainty	*Lognormal*	*0.15*
Deck wave force model uncertainty	*Lognormal*	*0.35*

A number of dominant failure sequences leading to collapse of the jacket are identified using a failure-tree enumeration approach. It is observed that the most likely failure sequence does not include any pile failures, which confirms previous deterministic results that the failure of piles does not influence the ultimate capacity of the jacket significantly. The results of system reliability analysis for the extreme loading condition are summarized in Table 2.

From the results of sensitivity factors of basic variables it is seen that the system reliability is highly sensitive to the uncertainty in loading variables. This results in high correlation between failure sequences.

Results of Reliability Analysis Under Pure Fatigue Conditions

The system reliability analysis under pure fatigue condition is carried out using the approach described earlier. The basic variables considered and their probability distributions are given in Table 3.

TABLE 2: SUMMARY OF RESULTS FOR RELIABILITY ANALYSIS UNDER EXTREME LOADING

Description	*Annual Prob. of failure*	*Reliability Index (Annual)*
Any first failure	*3.47E-03*	*2.7*
Most-likely failure path	*5.88E-07*	*4.86*
System failure	*2.02E-06*	*4.61*

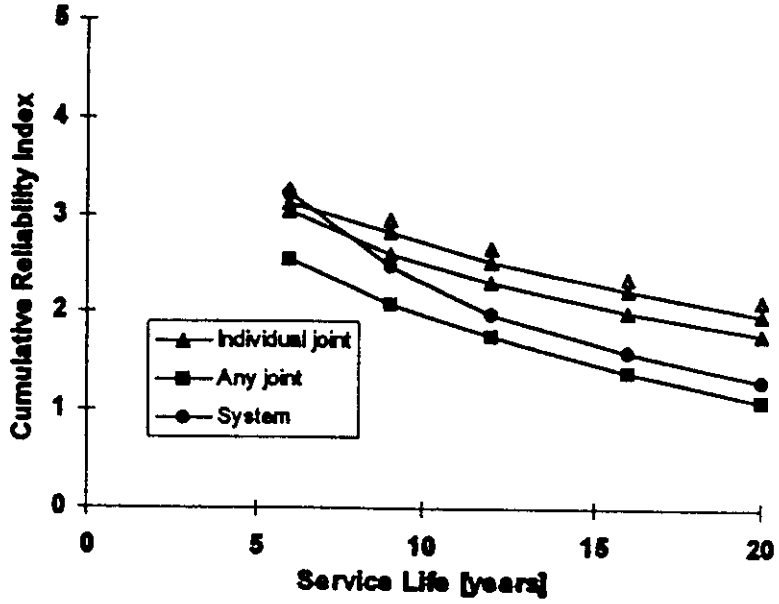
TABLE 3: PROBABILISTIC MODELING FOR FATIGUE RELIABILITY ANALYSIS

Parameter	*Distribution*	*Mean*	*COV*
Model uncertainty in global response	*Lognormal*	*1.0*	*0.20*
Model uncertainty in S.C.F.s	*Lognormal*	*1.0*	*0.15*
S-N curve parameter	*Lognormal*	*Bias=3.38*	*0.58*
Miner's damage sum at failure	*Lognormal*	*1.0*	*0.25*
Ratio of life-to-complete joint failure to life-to-through thickness cracking	*Lognormal*	*1.2*	*0.15*

The component reliabilities under pure fatigue conditions are calculated for a number of critical joints and for a range of service life periods. The results for the three most critical joints (upper curves) are shown in Fig. 3. Also shown is the reliability corresponding to any one joint failure, evaluated as the union over individual joint failure events. The significant difference between individual component reliabilities and that for any one joint indicates a prominent system effect (negative) as a result of the low correlation between joint failure events under fatigue condition.

Next, a failure tree enumeration approach is used to identify dominant failure sequences under pure fatigue conditions. The enumeration is limited to the failure of a maximum of four joints in sequence. None of these sequences resulted in the collapse of the structure. The variation of system reliability under fatigue, which represents the union over a number of failure sequences, is shown in Fig.2. It can be seen that the system reliability is higher than the reliability corresponding to any one joint failure (positive system effect).

Figure 2: Variation of fatigue reliability with service life

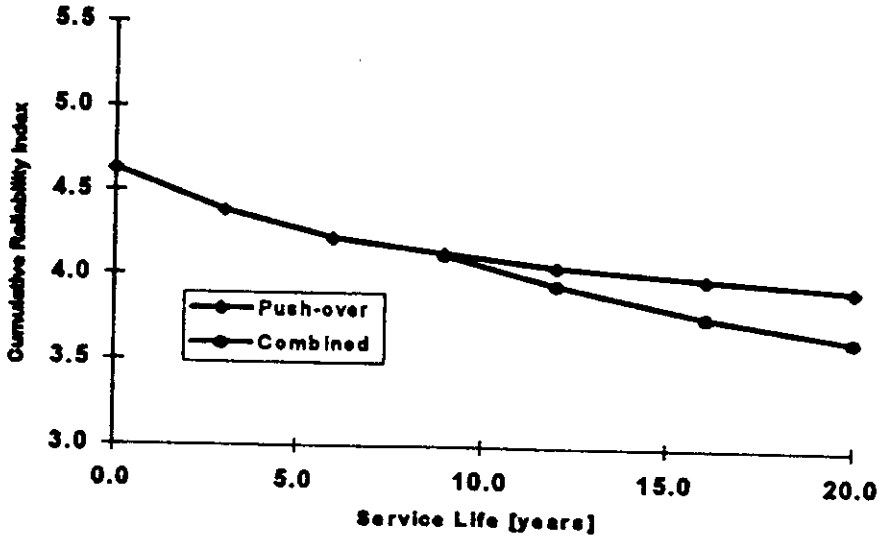


Results of Reliability Analysis Under Combined Fatigue and Extreme Loading

The system reliability analysis of the structure is then extended to consider the combined actions of fatigue and extreme environmental loading. Fig. 3 shows a plot of cumulative reliability index for extreme loading alone and combined fatigue and extreme loading conditions over the service life of the jacket.

These calculations are carried out under the assumption that failure of up to four joints in fatigue can occur and no mitigation action is undertaken. The contribution of pure fatigue sequences to system failure probability is not included as they do not result in the collapse of the structure. These results indicate strong dominance of the system reliability under the push-over conditions, in particular during the first half of the service life. In the second half, some effect of fatigue deterioration can be observed. The upper curve represents the system reliability under extreme conditions only, thus assuming that no damage is present. This curve can be interpreted as corresponding to "full inspection and repair" strategy. The lower curve represents the system reliability for the combined conditions, which can be interpreted as "no-inspection" strategy.

Figure 3: Variation of cumulative system reliability index over service life



The above results indicate a strong dominance of the system reliability under the push-over conditions, particular during the first half of the service life. This dominance is strongly influenced by the probability of the waves impinging on the deck. After the 10-th year of the service life some effect of fatigue can be observed, but only when no inspection and no repair is carried out. Based on these observations, a very limited maintenance program should be adequate to eliminate fatigue deterioration effects.

The results for cumulative probability of failure were used to calculate annual failure probabilities. This was done according to the formula

$$P_F(ann, t+ys/2) = (P_F(cum, t+ys) - P_F(cum, t)) / ys$$

where t is time during the service life at which the annual failure probability is calculated is the interval over which the annual probability is calculated. A summary of results is given in Table 4.

TABLE 4. SUMMARY OF SYSTEM RELIABILITY ANALYSIS RESULTS FOR COMBINED CONDITIONS

Service life [years]	*Annual failure probability*	*Reliability index β_{sys}*
0	*2.02E-06*	*4.61*
3	*2.02E-06*	*4.61*
6	*2.02E-06*	*4.61*
9	*2.02E-06*	*4.61*
12	*6.77E-06*	*4.36*
16	*1.13E-05*	*4.24*
20	*1.34E-05*	*4.20*

These results can be used for evaluation of the initial service period during which no inspection is required. In the present case, the annual failure probability for combined conditions increases only seven-fold, from 2.02E-06 to 1.34E-05, over the service life of twenty years. Assuming that the target failure probability for the system is 1.0E-04, it can be concluded that no inspection is required. Of course, a minimal level of inspection, e.g., periodic flooded member detection (FMD) and remote operated vehicle (ROV) inspection, would be desirable to capture the unanticipated failure events.

REFERENCES

N. K. Shetty, J. T. Gierlinski, J. K. Smith, and B. Stahl, "Structural System Reliability Considerations in Fatigue Inspection Planning," Proceedings, Int. Conf. on Behavior of Offshore Structures, BOSS-97, July 1997, Delft, The Netherlands.

Appendix B

Example of Using QRA to Assess Relative Risk Between Two Alternatives

An example application of QRA to assess alternatives is described in Ref. 1. A study was undertaken for the Marlin deepwater development to determine the risks and benefits associated with the use of dual casing risers, compared to single casing riser design. The study involved carrying out and linking 1) Failure Modes and Effects Analysis, 2) Fault Tree Analysis, 3) consequence severity ranking by experts, 4) cost (risk) / benefit assessment, 5) decision analysis, and perhaps most importantly, the study led to 6) team building and buy-in.

Amoco is the designated operator of the Marlin deepwater development, located in the Viosca Knoll area 85 miles ESE of Venice, LA in 3240 feet of water. The Marlin design team's conceptual design basis assumed that the wells would be tied back from the seafloor to the surface vessel with dual casing production risers, capable of carrying full shut-in tubing pressure. These risers are essentially dual concentric, redundant risers surrounding the production tubing running from 200 feet below mudline to the surface wellhead. A number of potential hazards during production and workover can prompt a requirement for this level of redundancy in barriers. The purpose of this study was to determine the risk-benefit associated with the use of dual casing risers, compared to single casing riser design.

System Description

The Marlin riser systems consist of two similar designs of production riser system. The two designs are similar in most aspects except for the second (concentric) riser casing string in the dual riser case.

A system definition and boundaries were developed for the study. The system configuration for the normal production mode is represented in the simplified completion diagrams shown in Fig. 1 for the single and dual riser cases.

The system configuration changes when the system is operating under either a workover or development drilling mode. The primary changes to the system are that, as part of the workover or development drilling procedure, the surface tree is changed out for a Blowout Preventer (BOP) and the well is generally operated in a mode with Kill Weight Fluid (KWF) in the system. The purpose of the KWF is to provide a hydrostatic overbalance of fluid to prevent the well from flowing. In addition to the overbalance of the fluid there will be either one or more mechanical barriers in the system which can be used to close off flow from the well if the overbalance of KWF is lost.

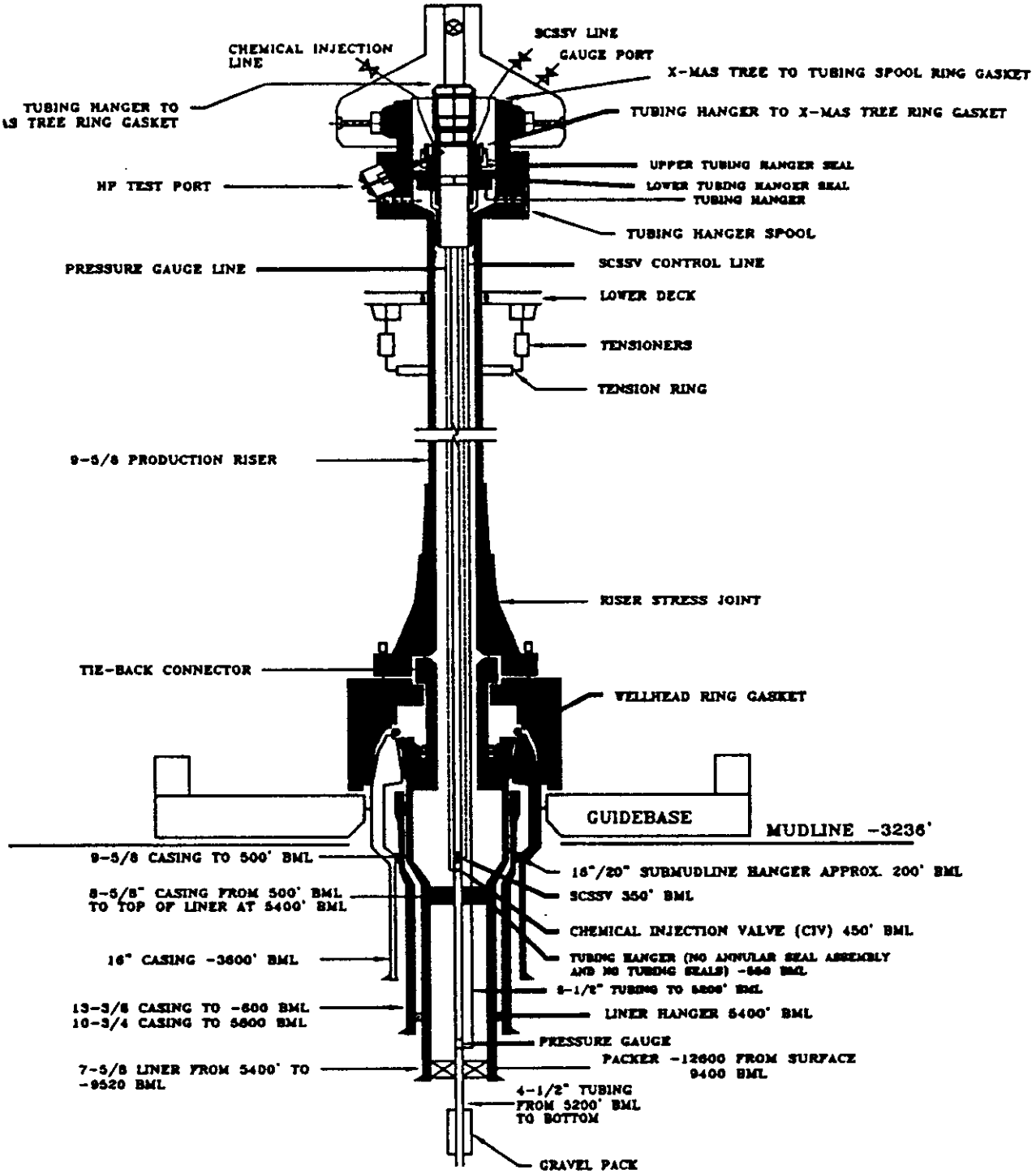


Fig. 1(a) Single Casing Riser Configuration

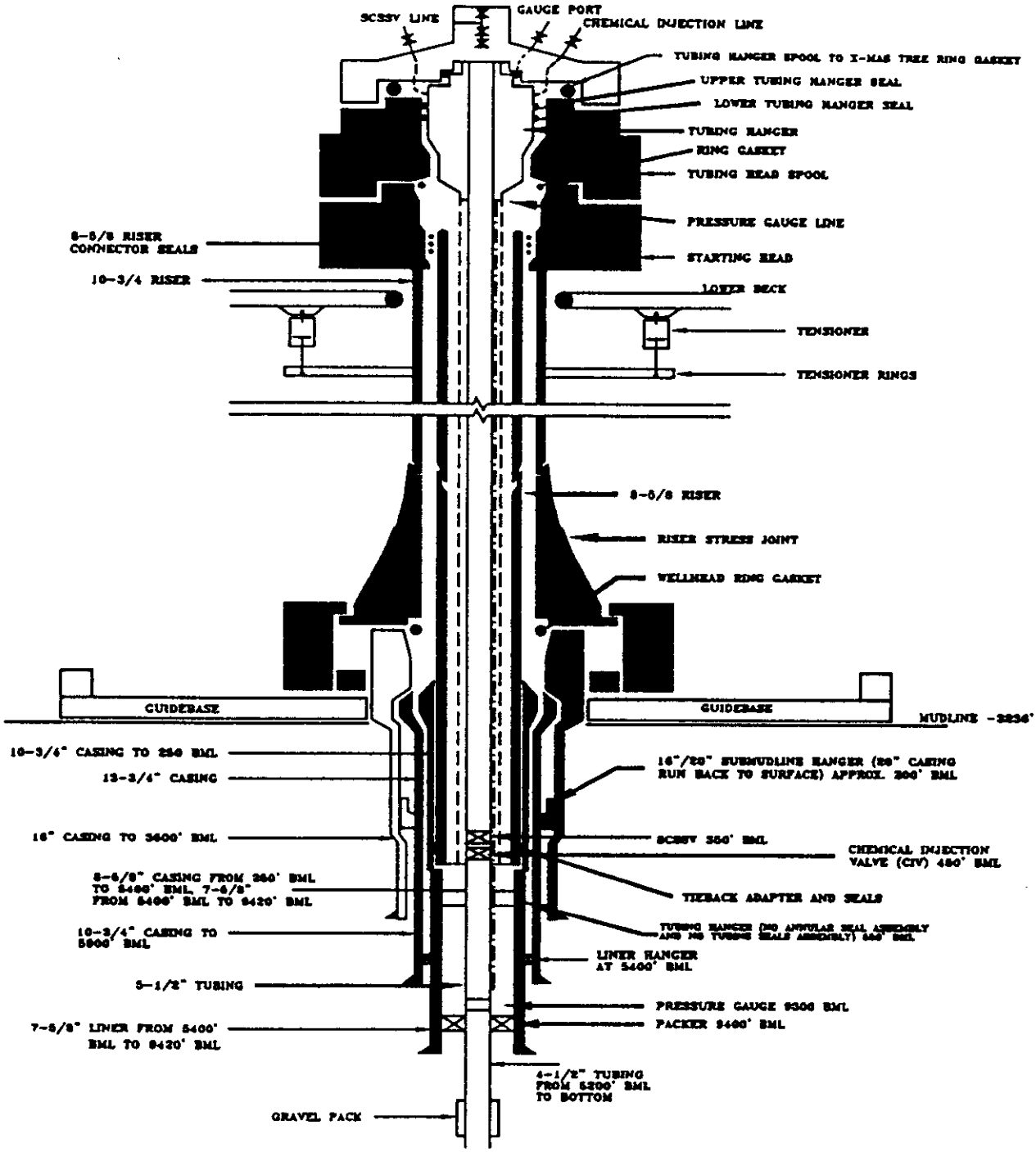


Fig. 1b Dual Casing Riser Configuration

Technical Approach

The study process is shown graphically in Fig. 2. The process illustrates the interaction of the tasks: Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), Failure Frequency Analysis and Risk Assessment within the risk analysis process. Consequence severity categories were developed and defined by the Marlin team for use both in the FMEA task and the overall study process. These categories included safety, economic loss, and environmental impacts.

The FMEA provided a comprehensive identification of the hazards that could occur in each mode of operation. This was the primary source for the development of the risk scenarios.

The fault tree analysis produced the fundamental model for identification of critical failure combinations, determining distribution of event frequency by cause and for calculating the quantitative risk values. In addition to computing the frequency of loss of containment events (the top event), the frequency events leading up to loss of containment (leaks and barrier failures) were also generated. The workover trees were used for all operating modes envisioned for Marlin; therefore, many of the fault tree branches were included or excluded according to the operating mode.

Failure data used to quantify the FTA models were taken from a variety of sources including proprietary studies and expert opinion. Where estimates based on expert opinion were used, sensitivity analyses were performed to determine the effects of these estimates.

Risks were determined by summing over the probability, consequence combinations where consequence impacts were measured in dollars. This calculation gave rise to what is termed risk (consequence cost times its probability of occurrence). The risk includes both loss of containment (severe) and less severe failure events. Additionally, cost estimates are given for the differences in capital and operating costs for the alternative systems. These costs can be compared to the risk of the system, thereby obtaining a benefit to cost ratio for the proposed "upgrade" beyond a single riser alternative.

A decision analysis was conducted using a software tool for decision making under conditions of uncertainty. The software tool was used to perform formal decision analysis taking uncertainties into account and to determine the implied costs that would be appropriate to spend on the upgrade of the system from single to dual to reduce the risk.

The purpose of the FMEA is to provide a comprehensive method for the identification of the hazards that could occur in each mode of operation. The FMEA utilized the system design basis and the workover and other procedures that were developed for the Marlin riser project.

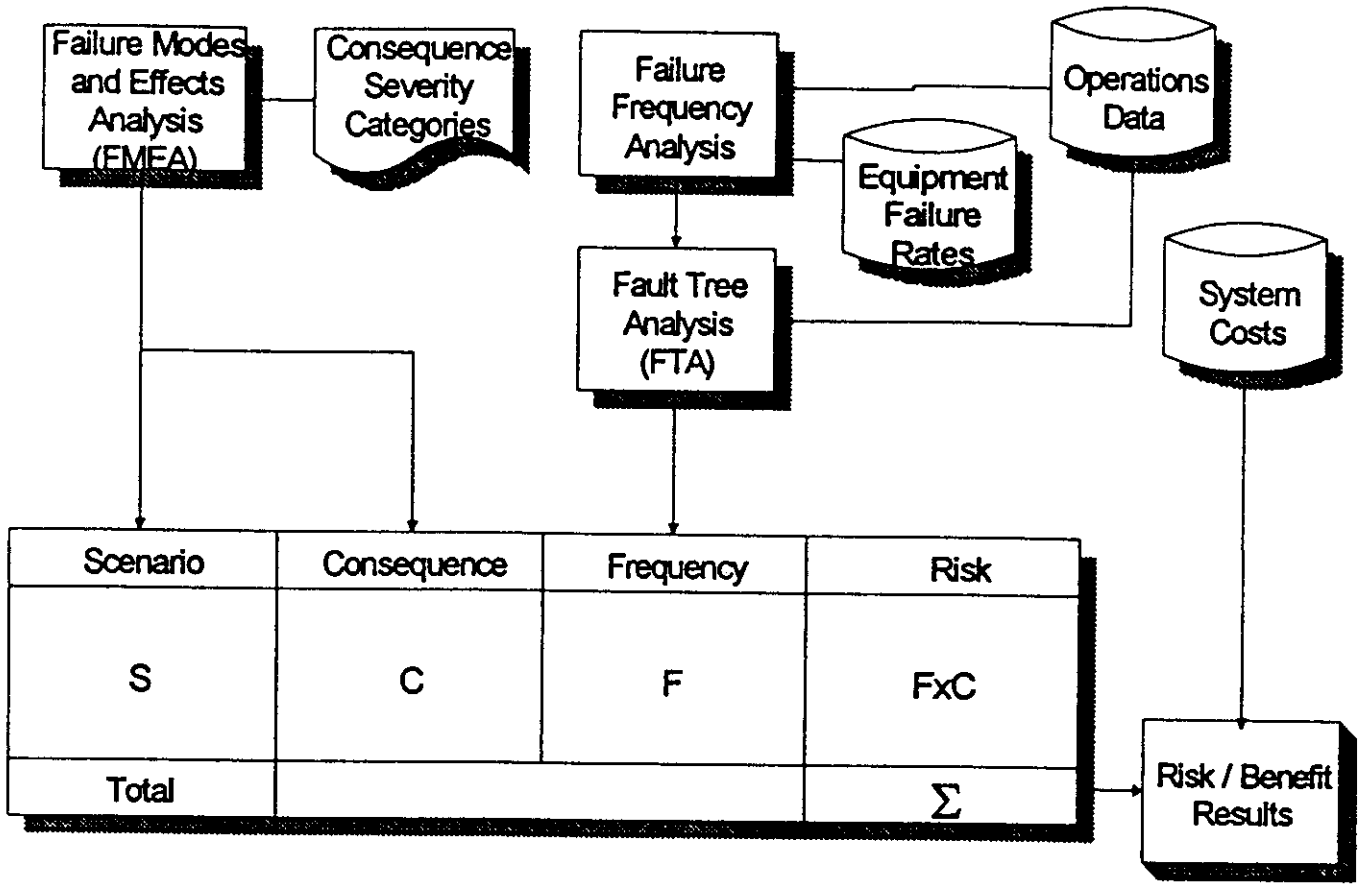


Fig. 2 - Study Process

The FMEA considered the following modes of operations of the equipment:

Normal Production
Workover by Pulling Completion
Up hole re-completion
Sidetrack
Installation
Riser repair

For each failure mode identified in the FMEA a consequence "Severity" category (Table 1) was assigned to ranking of failures.

Further details concerning the technical approach can be found in Ref. 1.

Risk Results

Risk is defined as the sum of the consequences of failure times their respective probabilities of occurrence. Using this measure allows direct comparison of the risks predicted for a particular design alternative, in financial terms, to the capital and operating costs associated with the reduction of risk.

Total risk was estimated for each of the alternatives. Risk consists of three components: a reliability (probability) assessment which was described previously, a failure or consequence cost, and investment (capital and operating) costs.

Although the initial position was to utilize a dual riser configuration for Marlin, for purposes of this discussion, a single casing riser (at all times) configuration will be referenced as the base case. This was assumed because it is the lowest investment scenario, and all other investment alternatives will be viewed incrementally. The other alternatives considered were: 1) providing the provisions to be able to run a second (or inner) riser, but expecting not to utilize this capability; 2) providing the provisions to be able to run a second (or inner) riser and planning on installing it during all well interventions; 3) having dual risers at all times. Alternatives 1 and 2 were assumed to be temporary installations, which could only be implemented on one well at a time, although all wells would have the capability.

Incremental investment costs range from a low of $ 2.1 MM for the temporary, but not expected to be installed inner riser alternative, to a high of $ 8.4 MM for the temporary and installed during all intervention activities. The permanent dual riser alternative has a cost of $ 6.9 MM, which falls between the first two alternatives but toward the high end. This suggests that if the decision is made that a dual riser configuration is required for interventions, it should be installed initially as a permanent system for the Marlin Project.

Table 1 Consequence Severity Categories

Type	*Description*	*$ Value*
Catastrophic		
Safety	*Multiple serious injuries*	*$100MM*
Economic Loss	*Total asset loss of $100 million*	*$100MM*
Environment	*Long term damage to an environmentally sensitive area*	*$100MM*
Major		
Safety	*Serious injury*	*$30MM*
Economic Loss	*Asset loss of between $1 million and $100 million*	*$30MM*
Environment	*Possible threat to wildlife, spill requires mobilization of clean up equipment*	*$30MM*
Minor		
Safety	*Occupational / workplace accident*	*$1MM*
Economic Loss	*Asset loss of $1 million*	*$1MM*
Environment	*Reportable spill which can be contained on site*	*$1MM*

Table 2 presents the probability of a blowout during production, during workover and of leak / component failures leading to an unplanned workover. The table also presents the total consequence impact (safety, economic, environmental) for each type of event. The risk, expressed in dollars, is the total expected loss due to all events of the type listed (e.g. workover blowout) for the entire platform life, 29.75 well years for all well/risers.

Upgrading to the hybrid design reduces the lifetime risks on Marlin, at a cost of $8.4MM, by $170,000, because it provides prevention only during workover activities. Upgrading to the permanent dual riser for all wells, at a cost of $6.95MM, reduces the lifetime risks on Marlin by $486,000, as it provides prevention for all phases of operation. In both of these cases, the reduction of risk is not sufficient to justify the cost of upgrading.

To determine an appropriate cost for the engineering changes to the facility, a "payback ratio" of from 3 to 10 was selected. This means that $1 invested to reduce risks on Marlin should reduce risks over the lifetime in the amount of $3 to $10. The implied cost to avert the risks, for the recommended payback ratios of from 3:1 to 10:1, and also 1:1 for a conservative viewpoint is shown in Table 3. For the hybrid option the costs should be in the range of $17,000 to $170,000 and for the permanent dual option from $49,000 to $486,000. The justifiable costs are considerably lower than the estimated upgrading costs indicated in the previous paragraph.

As these values depend on management policy and there are uncertainties about the predicted risk, formal decision analyses were undertaken.

The results of the decision analysis (based on a simplified model with deterministic capital and operating cost estimates as well as deterministic consequence estimates) agreed with the result already presented, indicating a clear preference for the single casing riser design. A more advanced decision analysis model was also constructed, in which probability distributions to represent capital, operating, and consequence costs were introduced. The results indicated two primary conclusions: First, extreme risk values were predicted to occur, with extremely remote probabilities of extreme risk. The extreme predictions were influenced by the probability distributions of costs. Second, the decision policy predicted by the enhanced decision analysis model remained fully consistent with the above conclusions. The enhanced model indicated that the single casing riser design is the alternative of choice unless the initial investment in the dual casing riser can be by about $6.5MM from its estimate of $6.95MM. This is equivalent to justifying an incremental cost of about $450,000 for the dual casing design ($6.95MM - $6.5MM), which is close to the $486,000 indicated in Table 3 at a benefit to cost ratio of 1:1.

Table 2 - Risk Results

	Production Mode		Intervention Mode	
	Leak (Single Barrier Failure)	Blowout (Loss of Well Control)	Blowout (Loss of Well Control)	Total
Single Riser				
Probability	6.31E-01	1.52E-03	2.09E-03	
Consequence $MM	3	230	230	
Risk $MM	1.908	0.350	0.481	2.738
Temporary Riser				
Probability	6.31E-01	1.52E-03	1.35E-03	
Consequence $MM	3	230	230	
Risk $MM	1.908	0.350	0.311	2.568
Incremental Risk (Temp vs. Single) $MM	0	0	0.170	0.170
Dual Riser				
Probability	6.23E-01	3.18E-04	1.35E-03	
Consequence $MM	3	230	230	
Risk $MM	1.869	0.073	0.311	2.253
Incremental Risk (Dual vs. Single) $MM	0.039	0.276	0.170	0.486

Table 3 - Justifiable Costs ($M) of Upgrading at Various Benefit/Cost Ratios

	Benefit / Cost Ratio		
	10:1	3:1	1:1
Dual Riser	49	162	486
Temporary Riser	17	57	170

Conclusions

Results of the study are: upgrading to the permanent dual riser for all wells, at a cost of $6.95MM, reduces the lifetime risks by $486,000, as it provides prevention for all phases of operation. Upgrading to a hybrid design which would allow a dual riser to be run during all workover activities reduces the lifetime risks by $170,000, at a cost of $8.4MM. In both of these cases, the reduction in risk was not sufficient to justify the cost of upgrading.

The risk and decision analysis process described in this paper was considered to be highly successful by the participants of the process. Risk analysis provided the framework for discussion and evaluation of many dissimilar issues involved. It provided the necessary vehicle for communication among the participants, including project management, design engineering and consultants, and provided a rational basis for decision making.

References

1. *Andrew J. Wolford, Stephen R. Perryman, F. Jonathan Deegan, Stuart W. Gosch and Bernhard Stahl, "Marlin Riser Deepwater Alternatives Risk Assessment," OTC Paper No. 8518, Proceedings, Offshore Technology Conference, Houston, 5-8 May 1997.*

Appendix C

Example U.K. Safety Case

The Brae B platform

Brae B is one of three platforms and a subsea template which together develop Marathon's Brae Field in the UK North Sea. The Brae Field is 125 miles offshore the east coast of Scotland. The B platform is a single, integrated platform consisting of a drilling rig and production, utility and accommodation facilities (Fig. 1), installed in a water depth of 325 ft. The jacket weighs 18,500 tonnes, and the topsides operating weight is 39,000 tonnes.

The Brae B platform develops a condensate reservoir, and handles a peak condensate production of 75,000 bpd and recycles 400 mmscfd of gas by compression to 6,500 psi and reinjection into the reservoir for later gas sales. Production started in 1988.

General description of the Brae B safety case

The Brae B safety case was prepared in 1993, at a time when the precise requirements and a preferred format were still being discussed and decided. A later case might be formatted differently. The Brae B safety case seeks to follow the guidance given in the HSE publication A Guide to the Offshore Installation (Safety Case) Regulations 1992 (HMSO, London).

The safety case is in six principal parts in two volumes, with 356 pages of text and 129 illustrations. The detailed index is shown at Figure 2. More than half of the Brae B safety case book is devoted to company policy and organization and operating procedures in the Health, Safety and Environmental (HSE) area, to the Brae safety management system, and to an engineering description of the Brae B platform and process facilities.

FIGURE 1 - Brae B Platform

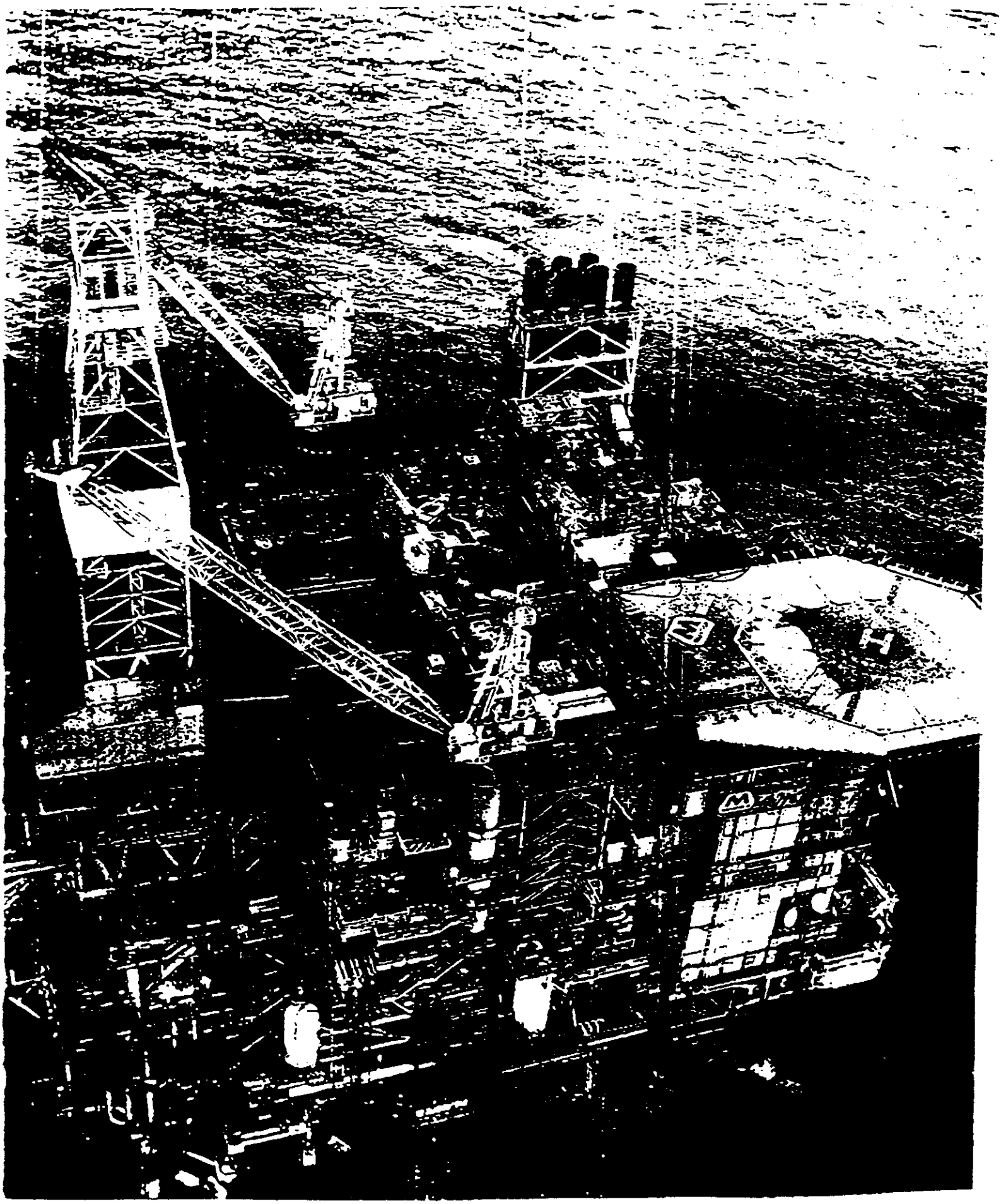


Figure 2

Brae B Safety Case

Index

Preface

1: Introduction
- **1.1 Background and Scope**
- **1.2 Marathon Oil Company Environmental Health and Safety Policy Statement**
- **1.3 Marathon Oil UK relationship to Marathon Oil Company**
- **1.4 Objectives**
- **1.5 Accident causes and prevention**
- **1.6 Summary of contents**
- **1.7 Responsibility for issue, review, updating and compliance**
- **1.8 Development of the Safety Case**

2: Corporate Management of Safety
- **2.1 Introduction and Scope**
- **2.1 Organisation**
- **2.3 Management structure**
- **2.4 Department overviews**
- **2.5 Management Safety Committee**
- **2.6 MOUK management of Safety, Health and Environment systems**
- **2.7 Company standards**
- **2.8 Risk management**

3: Description of the Installation
- **3.1 General description**
- **3.2 Location**
- **3.3 Environmental conditions**
- **3.4 Reservoir development**
- **3.5 Design concept**
- **3.6 Primary functions**
- **3.7 Hazardous substances and inventories**
- **3.8 Marine activities**
- **3.9 Installation safety systems**
- **3.10 Temporary refuge**
- **3.11 Escape, evacuation and rescue**

Part 5 (54 pages of text and 24 illustrations) deals with identification and control of major hazards. This section describes the risk assessment process Marathon used, to demonstrate that the requirements of the Safety Case Regulations have been satisfied relating to (a) the identification of major hazards and (b) the evaluation and control of their risks. Detailed studies carried out are not included in the actual safety case submitted to the HSE, but have been referenced in the safety case document (Fig. 3).

Part 6 (29 pages of text and 17 illustrations) confirms, by reference to the safety case itself, that all the requirements of the Offshore Installations (Safety Case) 1992 Regulations have been met and that (a) the operator does have in place an adequate safety management system (b) that all hazards with the potential to cause a major accident have been identified, and (c) that risks to personnel have been (and are being) reduced to the lowest level that is reasonably practical.

Identification and control of major hazards

The identification and control of major hazards was carried out to:

(i) Identify those hazards associated with the Brae B platform operations which have the potential to develop into major accident events.

(ii) Analyze each of these major hazards, to determine the likely frequency of occurrence and severity of consequence in terms of loss of life

(iii) Examine in detail the risk from each major hazard and, where appropriate, implement measures to reduce it to as low as reasonably practical (ALARP).

(iv) Evaluate the temporary refuge impairment from major hazards

(v) Examine the evacuation, escape and rescue arrangements and ensure their adequacy for all identified major accident events.

FIGURE 3 - List including References to Risk Assessment Studies carried out for the Brae B Safety Case

Safety Case Reference	Document Title	Document Reference
5.1	The Public Inquiry into the Piper Alpha Disaster	HMSO Cm 1310, ISBN 0-10-113102-X
5.2	The Offshore Installations (Safety Case) Regulations 1992	Statutory Instrument 1992/2885
5.3	Company Standard 'Management of Systematic Risk Assessment'	MOUK Number 0000-M-95-Z-M-0008-00
5.4	Guidelines for Systematic Risk Assessment	MOUK Number 0000-M-00-Z-P-1701-00
5.5	Management of Safety, Health & Environmental Systems 'Hazop Procedure'	MOUK Number 0000-A-95-Y-P-0001-00
5.6	Guide to Failure Mode Effects and Criticality Analysis FMEA/ FMECA	BS 5760 : Part 5:1991
5.7	Brae 'B' Integrated Study Report	MOUK Number 7080-A-95-Z-T-0001-00
5.8	Audit Report on Process Hazard Analysis	MOUK Number 0000-A-95-Y-T-0004-00
5.9	Essential Systems Reviews - Fire & Gas Detection	MOUK Number 7080-A-95-Y-T-0001-00
5.10	Essential Systems Reviews - Emergency Shutdown Systems	MOUK Number 7080-A-95-Y-T-0007-00
5.11	Essential Systems Review - Blowdown System	MOUK Number 7080-A-95-Y-T-0008-00
5.12	Emergency Systems Review - Fire Pumps and Firewater	MOUK Number 7080-A-95-Y-T-0004-00
5.13	OREDA - Offshore Reliability Data	DNV Technica, 2nd Edition 1992
5.14	Essential Systems Review - HVAC System	MOUK Number 7080-A-95-Y-T-0019-00
5.15	Essential Systems Review - GPA/PA Systems	MOUK Number 7080-A-95-Y-T-0020-00

/080-A-95-Y-M-0001-00-I
Part 7

Safety Case Reference	Document Title	Document Reference
5.16	Essential Systems Review - Telecommunication	MOUK Number 7080-A-95-Y-T-0021-00
5.17	Essential System Reviews - Emergency Power System	MOUK Number 7080-A-95-Y-T-0016-00
5.18	Brae 'B' Fire Risk Assessment	MOUK Number 7080-A-95-Y-T-0005-00
5.19	BCL Assessment of Potential Explosion Effects on the Brae Alpha and Brae Bravo Platforms	MOUK Number 0000-A-95-Y-T-0005-00
5.20	'GAS-UP-2' Computer Model	Propriety product of Burgoyne Consultants Ltd
5.21	Computer Modelling of Gas Explosion Propagation in Offshore Modules, Hjaerteger et al	Journal of Loss Prevention Process Industries, 1992 Volume 5, No 3 pp 165-174
5.22	'FLACS' Computer Model	Propriety product of Christian Michelson Inst.
5.23	'CHAOS' Computer Model	Propriety product of British Gas plc
5.24	'FRAT1A' Computer Model	Propriety product of Burgoyne Consultants Ltd
5.25	The SFPE Handbook of Fire Protection Engineering	National Fire Protection Association, 1st Edition 1988
5.26	Hydrocarbon Leak and Ignition Database	E & P Forum, 1992
5.27	'TECJETT' Computer Model	Propriety product of DNV Technica
5.28	Smoke & Gas Ingress Study	MOUK Number 7080-A-95-Y-T-0002-00
5.29	Guidelines for Smoke and Gas Ingress Assessment	UKOOA 1992
5.30	Safety Alert	Issued by HSE - 16/8/1991
5.31	DNV Technica TR Impairment Review for Brae 'A' and Brae 'B'	MOUK Number 0000-A-95-Y-T-0006-00

Safety Case Reference	Document Title	Document Reference
5.32	EERA Summary Report - Brae 'B'	MOUK Number 7080-A-95-Y-T-0022-00
5.33	EERA - Brae 'B'	MOUK Number 7080-A-95-Y-T-0003-00
5.34	DNV Technica Brae 'A' and 'B' Qualitative Escape Study Report	MOUK Number 0000-A-95-Y-T-0007-00
5.35	DNV Technica Rescue Analysis Brae Alpha	MOUK Number 7000-A-95-Y-T-024-000
5.36	Quasar Study Brae 'A' and 'B'	MOUK Number 0000-A-95-Y-T-0008-00
5.37	The Offshore Installations (Emergency Pipeline Valve) Regulations 1989	Statutory Instrument 1989/1029
5.38	Hazard Analysis Brae 'B' Pipeline Emergency Shutdown Valves	MOUK Number 7080-A-90-N-T-0012-00
5.39	Assessment of the Need for the Installation of Sub Sea Isolation Valves	MOUK Number 0000-A-95-Z-T-0001-00
5.40	RM Consultants SSIV Reliability	MOUK Number 0000-A-99-N-M-0002-00
5.41	The Update of Loss of Containment Data for Offshore Pipelines	Advanced Mechanics & Engineering Ltd August 1990 (Job No.226.1)
5.42	Classification of Hazardous Locations	Institution of Chemical Engineers, 1990
5.43	Evaluation of Condensate Releases from East to North, and North to South Brae Platforms	MOUK Number 7016-Z-99-N-T-0011-00
5.44	Source Identification, Behaviour and Modelling of Oil	Joint Industry Project, Warren Spring Laboratory
5.45	Pipeline Report	MOUK Number 7080-A-95-Y-T-0013-00

Part 7

Safety Case Reference	Document Title	Document Reference
5.46	Assessment of the Risk of Helicopter Crash	MOUK Number 7080-A-95-Y-T-0012-00
5.47	Ship Collision Study	MOUK Number 7080-A-95-Y-T-0006-00
5.48	'COLLIDE 2' Computer Model	Propriety product of SAFETEC
5.49	Dropped Object Study	MOUK Number 7080-A-95-Y-T-0011-00
5.50	East Brae Development Dropped Objects Study	MOUK Number 7016-Z-99-N-T-0019-00
5.51	Topsides Survey - Dropped Objects	MOUK Number 7080-A-99-Y-T-0005-00
5.52	Wordwide Offshore Accident Databank Statistical Report	Veritas Offshore Technology & Services 1990
5.53	Escape and Evacuation Study - East Brae Production Phase	MOUK Number 7016-Z-99-N-T-0025-00
5.54	North Sea Seismicity - Summary Report	Department of Energy, OTH 86219
5.55	Piper Alpha Technical Investigation Final Report (Annex 9)	Department of Energy, 12/88
5.56	Global Marine Failure Mode and Effects Analysis Diving System Brae 'B'	MOUK Number 7080-A-95-Y-T-0024-00
5.57	Nomenclature for Hazard and Risk Assessment in the Process Industries	Institution of Chemical Engineers, 1985

Safety Case Reference	Document Title	Document Reference
6.1	MOUK Management of Safety, Health and Environmental Systems	MOUK Number 0000-M-95-Z-M-0001-00
6.2	Well Control Procedures and Guidelines	MOUK Number 0000-A-99-Z-P-0016-00
6.3	Well Service Manual	MOUK Number 0000-A-95-Z-M-0002-00
6.4	Basis of Design for Temporary Refuge on Brae 'B'	MOUK Number 7080-A-99-S-S-0001-00
6.5	A guide to the Offshore Installations (Safety Case) Regulation 1992	HMSO L30, ISBN 0-11-882055-9
6.6	Offshore Installations: Guidance on Design and Construction and Certificaiton, 4th Edition, 1990	Department of Energy, HMSO ISBN 0-11-412961-4

The Brae B risk assessment process

Figure 4 shows a general overview of the risk assessment process followed by Marathon.

Full HAZOP studies were carried out on selected drilling, process and utility systems. Initiating studies were carried out to identify potential hydrocarbon leaks in hazardous areas. The independent studies each dealt with a separate, external risk such as ship collision or helicopter crash. The results of the studies were integrated into the safety case using the systematic risk assessment process described in the Marathon procedure Guidelines for Systematic Risk Assessment (SRA), essentially following steps (i)(ii) and (iii) outlined in Section 3 above.

The risk assessment carried out for the Brae B safety case relies on well established reliability and risk management techniques. Appropriate use is made of hazard identification, frequency analysis and consequence analysis techniques. Hazard identification techniques used include HAZOP, Hazard Identification (HAZID), Initiating Event Analysis, and Failure Mode and Effect Analysis (FMEA). Frequency analysis techniques used include Fault and Event Tree Analysis and Reliability Analysis. Consequence analysis included: gas release rate and dispersion models; module gas-up and jet and pool fire models; explosion models; impact models for collision and dropped objects; and escalation studies.

Some examples of the input to and output from these studies are shown by: the HAZOP risk importance matrix (Fig. 5); typical event trees (Fig. 6); overview of an essential systems review (Fig. 7) and a fire risk assessment (Fig. 8), and a typical gas-up curve (Fig. 9).

FIGURE 4 - General Overview of Brae B Safety Case Risk Assessment Process

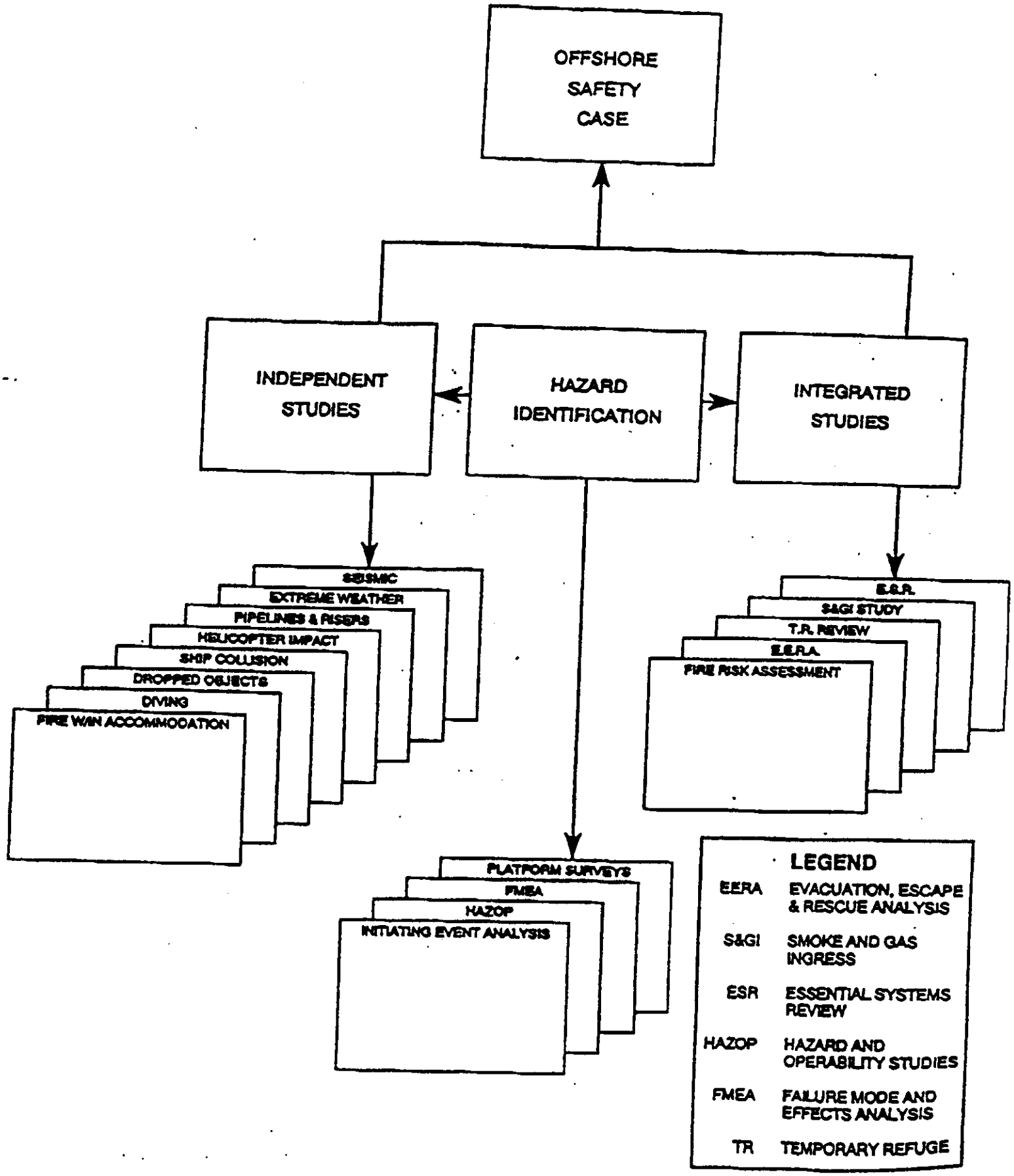


FIG 1.1 OVERVIEW OF RISK ASSESSMENT PROCESS

FIGURE 5 - HAZOP Risk Importance Matrix

Consequence Severity	A	Negligible
	B	Minor
	C	Serious
	D	Major
	E	Catastrophic
Consequence Likelihood	1.	Improbable (<0.001)
	2.	Potential (0.001-0.01)
	3.	Possible (0.01-0.1)
	4.	Probable (0.1-0.2
	5.	Highly Probable (>0.2)
Consequence Category	P	Personnel Injury
	F	Facilities/Production Loss
	E	Environmental Impact

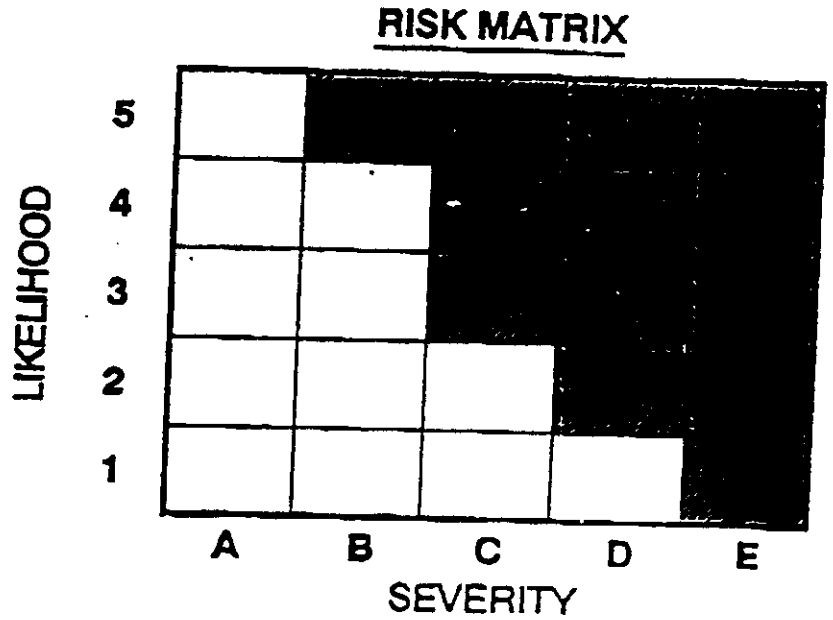
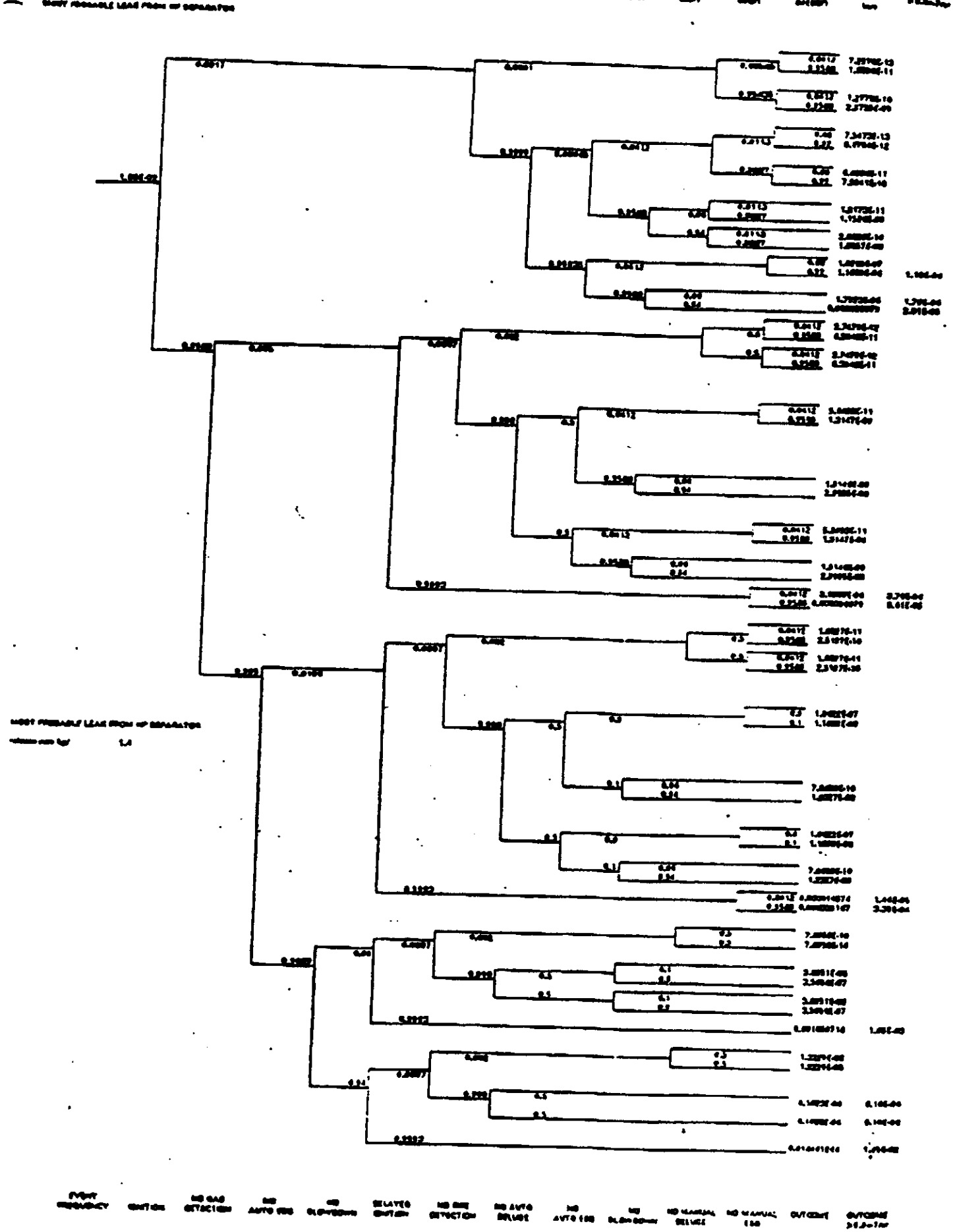
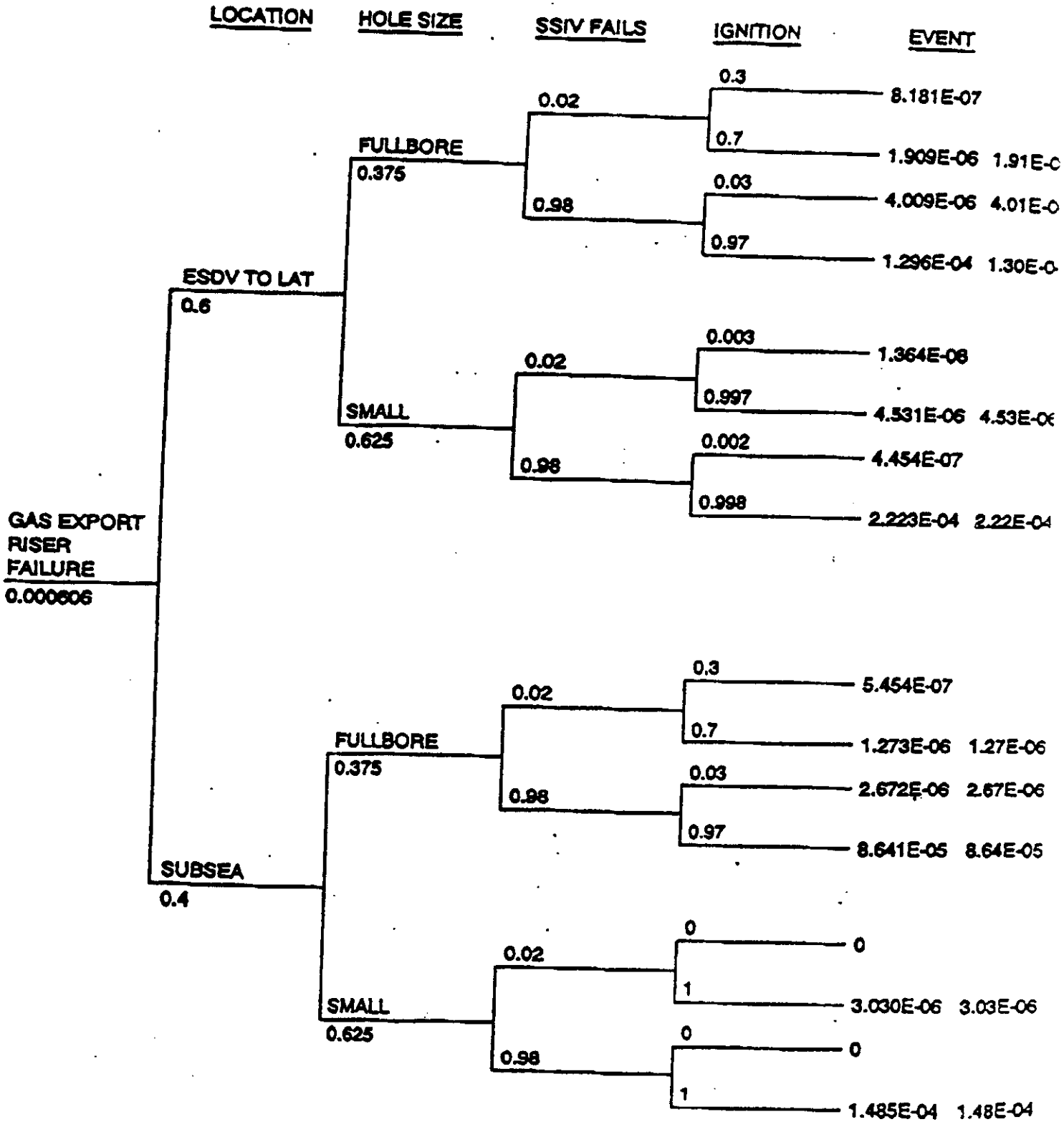


FIG 3.1 HAZOP - RISK IMPORTANCE MATRIX

FIGURE 6 - Typical Event Trees





RATIONALISED OUTCOMES FOR THE GAS EXPORT RISER	
Topside ignited full bore release, SSIV operates	4.01E-06
Subsea ignited full bore release, SSIV operates	2.67E-06

FIG 5.2 BRAE 'B' RISER FAILURE

FIGURE 7 - Overview of an essential systems review

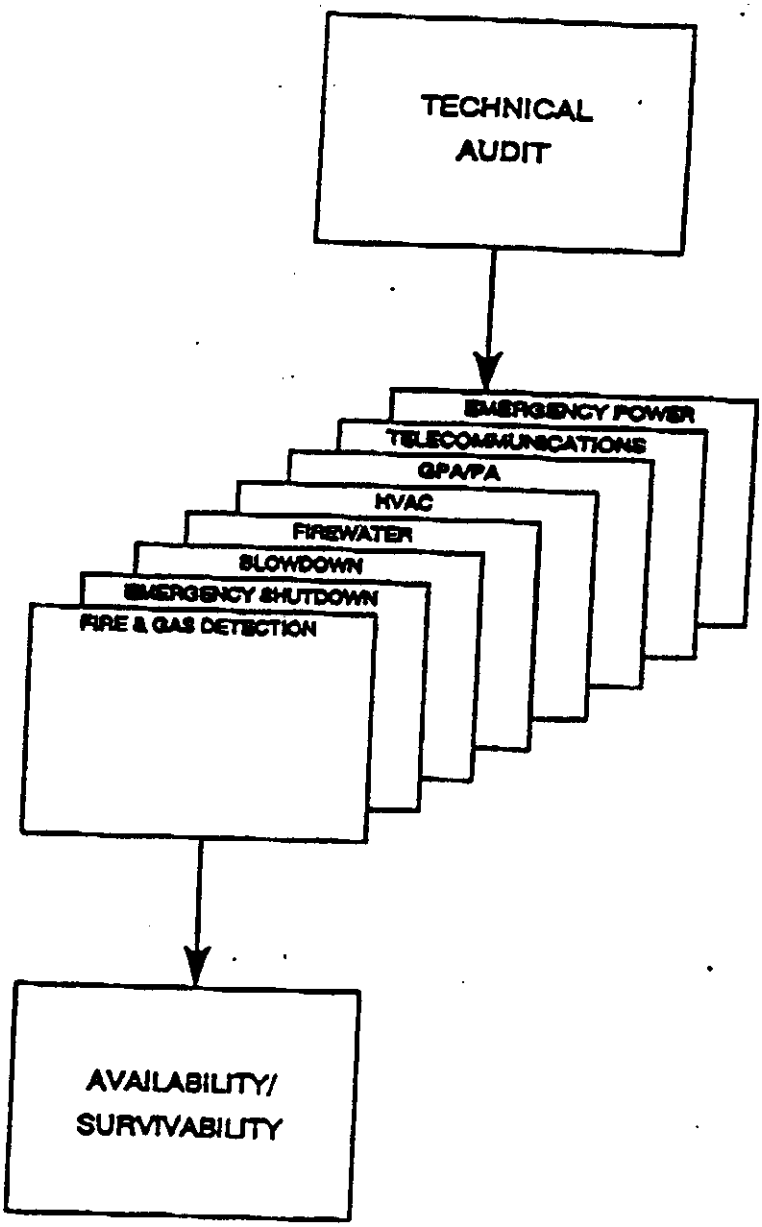


FIG 4.2 ESSENTIAL SYSTEMS REVIEW

FIGURE 8 - Fire Risk Assessment Overview

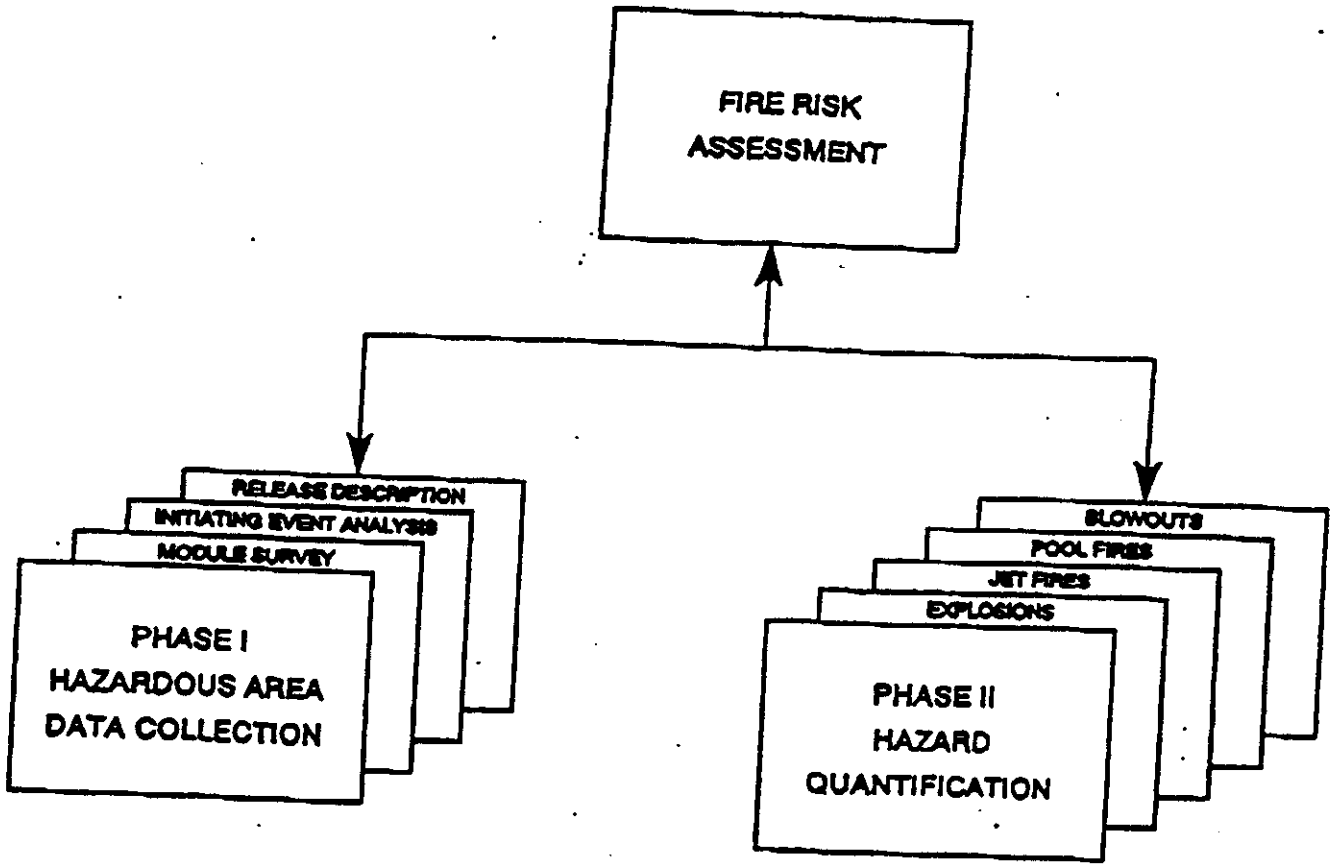


FIGURE 9 - Typical Gas-Up Curve

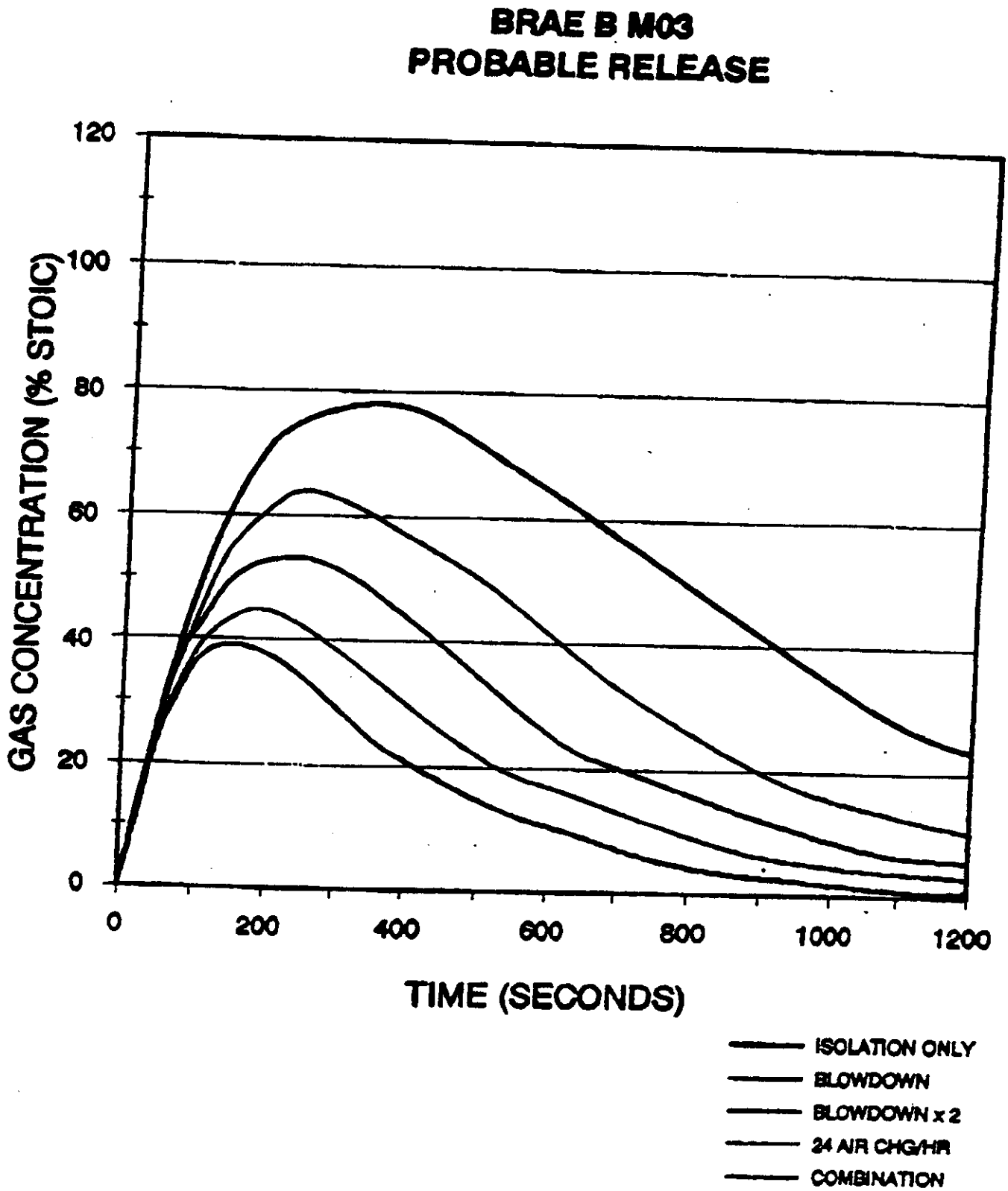


FIG 4.4 GAS UP CURVE

Qualitative and Quantitative Risk Assessment

The Brae B safety case seeks (Part 5, Section 2.3) to make a clear distinction between qualitative and quantitative assessment of risk:

'Qualitative assessment of risk requires the application of experienced judgment to identify and assess potential hazards. In some cases, the application of this judgment alone is sufficient to determine whether the risk is either unacceptable or that existing controls reduce the risk to acceptable levels.....

'Quantitative Risk Assessment (QRA) is recognized as a useful tool to define and describe risk and provides a numerical expression of risk level. The accuracy of available data, assumptions and the applicability of formal assessment techniques may mean that there is no benefit in performing QRA (which is therefore) performed where the value of the information generated justifies the effort....."

Risk acceptance criteria.

For the Brae B safety case, the current acceptance criteria for individual risk (expressed in terms of frequency of death per year) are defined by a three zone system (Figure 10). Risk at a frequency greater than 10E-3 (1 in 1000 years) is unacceptable. Risk at a frequency less than 10E-5 (1 in 10,000 years) is broadly acceptable. Risk between these frequencies is tolerable if it has been reduced to a level as low as reasonably practical (ALARP). QRA is required to provide these quantitative data.

Individual risk

The risk calculated for MOUK assumes a typical individual working to an offshore pattern of 12 hours per day on a two-in-four week rota. To avoid calculating an average which might conceal a certain group of personnel at particular risk, individual risk was calculated

FIGURE 10 - Risk Acceptance Criteria

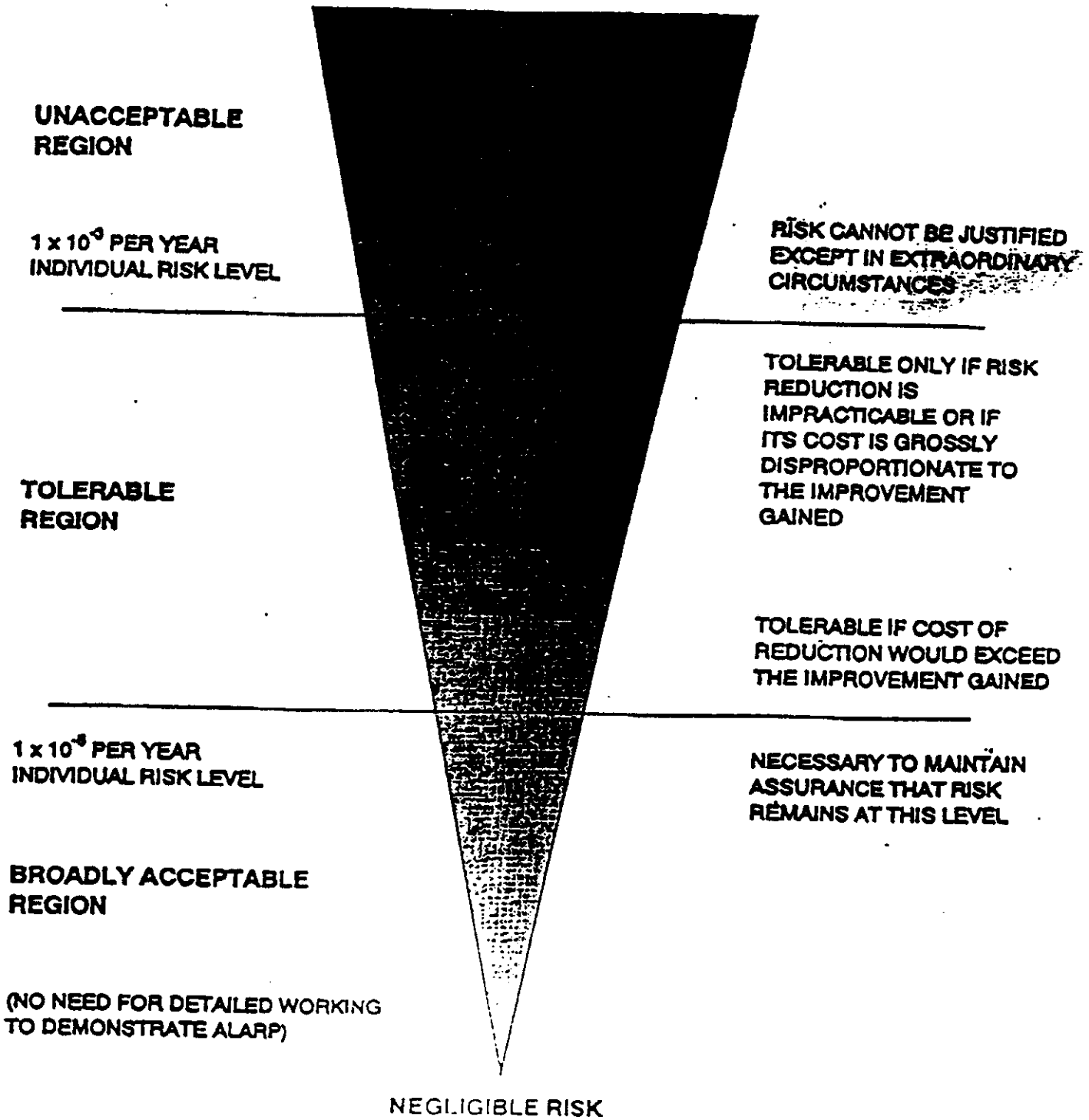


FIG 6 : RISK ACCEPTANCE CRITERIA

for (i) personnel who normally work in the accommodation (ii) personnel who normally work in the process and utility modules (iii) drillers and well completion personnel.

The overall platform average for individual risk is the proportional average of the three groups. Implicit in the calculation of individual risk is the assumption that the process and drilling personnel spend their off-duty time in the accommodation.

For expected normal manning levels, averaged over a year, the contribution of major hazards to risk to personnel was calculated. The calculated overall individual risk for Brae B is 4.32 x 10E-4, which is within the tolerable zone when assessed against the acceptance criteria. The highest individual risk event is the chance of a process leak (Figs. 11 and 12).

Group risk

Group risk accounts for the probability of multiple fatalities in a major accident event. It takes no account of the risks imposed on individuals but assumes personnel are present at the location 24 hours a day 365 days per year. Group risk was used to construct F-N curves which illustrate the cumulative frequency F of events resulting in N or more fatalities (Fig. 13).

Results of the safety case review

Part 6 of the safety case includes a summary of the preventative and protective measures in place for each identified risk category, assesses their reliability and effectiveness, and discusses additional measures adopted or under consideration for further reducing risk for each category. It is not intended to review these matters in great detail in this summary, which is primarily directed to the use of risk assessment, but the following information is considered pertinent.

FIGURE 11 - Individual Risk Table

INDIVIDUAL RISK - NORMAL MANNING POB

EVENT	ACCOMMODATION (freq/yr)	PROCESS (freq/yr)	DRILLING (freq/yr)	OVERALL (freq/yr)
Riser Failure	1.8×10^{-5}	1.9×10^{-5}	2.4×10^{-5}	2.0×10^{-5}
Process Leak	1.38×10^{-4}	1.92×10^{-4}	1.36×10^{-4}	1.73×10^{-4}
Blowout	4.3×10^{-5}	4.3×10^{-5}	8.7×10^{-5}	5.0×10^{-5}
Structural Failure*	1.00×10^{-4}	1.00×10^{-4}	1.00×10^{-4}	1.00×10^{-4}
Ship Collision	1.9×10^{-5}	1.9×10^{-5}	1.9×10^{-5}	1.9×10^{-5}
Helicopter Impact	7.0×10^{-5}	7.0×10^{-5}	7.0×10^{-5}	7.0×10^{-5}
Total	3.88×10^{-4}	5.96×10^{-4}	4.36×10^{-4}	4.32×10^{-4}

Note. * consists of seismic and extreme weather events.

FIGURE 12 - Individual Risk Profile

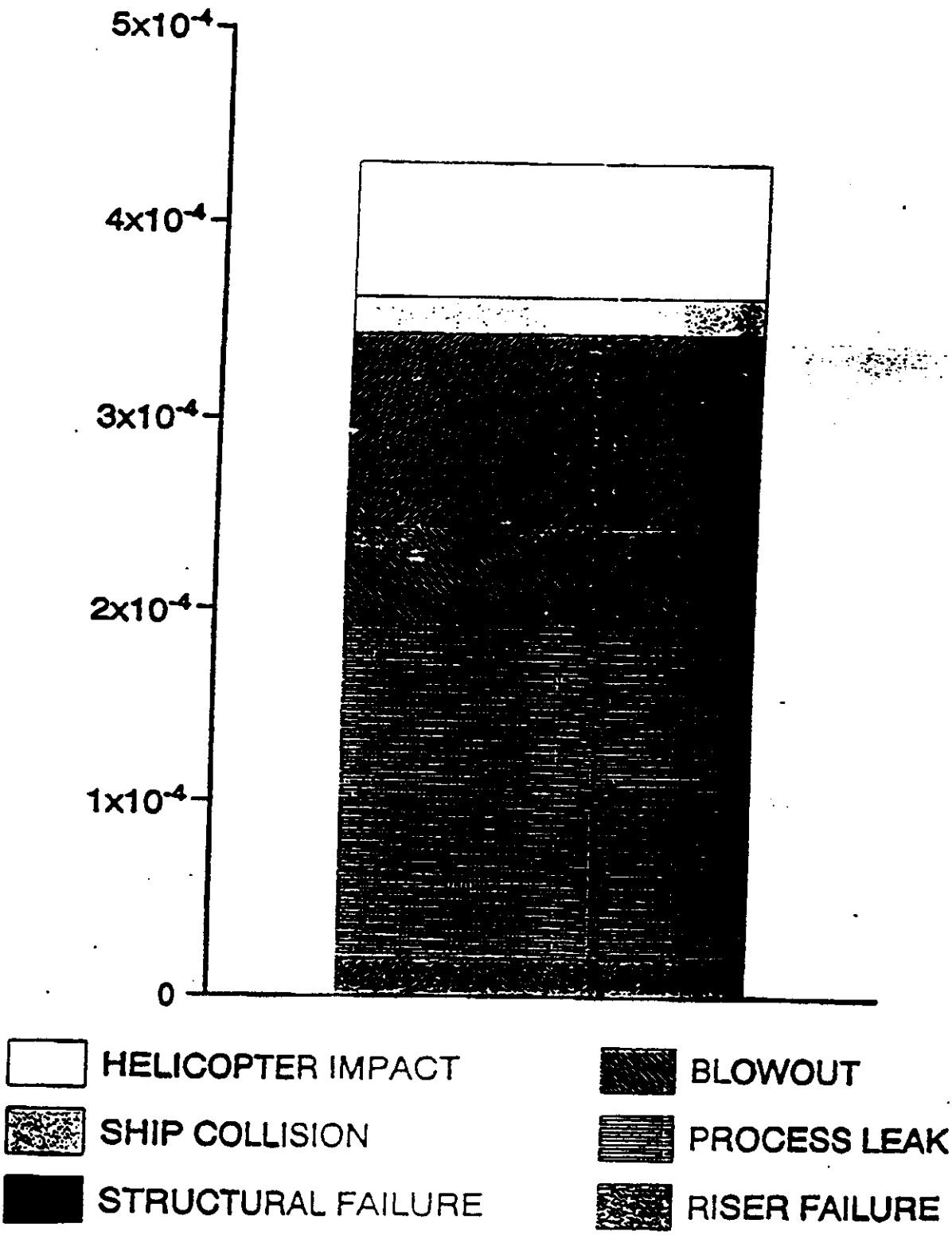


FIGURE 13 - P-N Curve

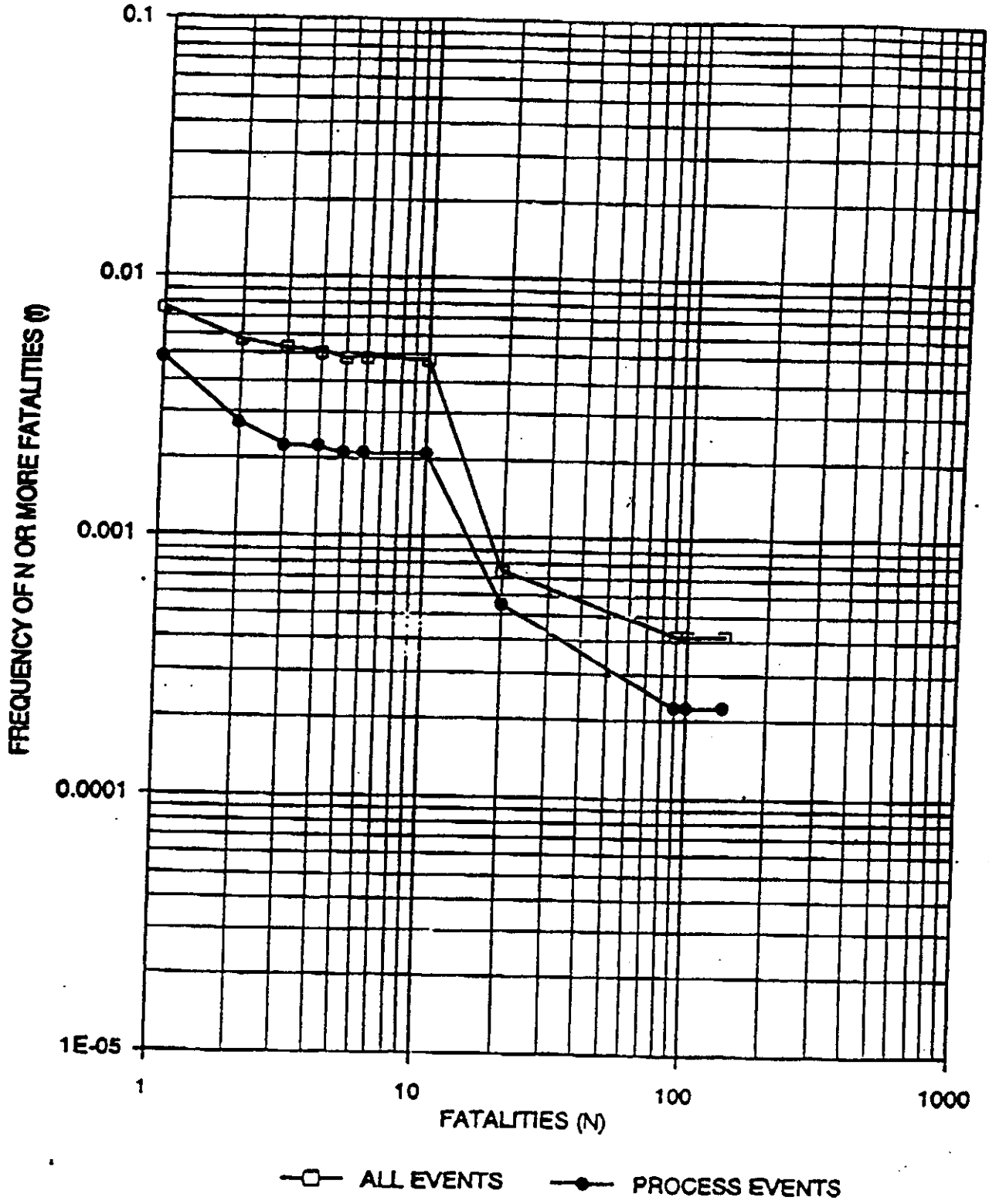


FIG 6.2 FN CURVES

Reliability of the systems in place to prevent and mitigate against the consequences of a hazard were assessed from records and from discussion with operating personnel. The reliability of some key systems was determined to be as follows:

(i) firewater pump system >99%

(ii) gas and fire detection systems >99%

(iii) HVAC (safe air) system >98%

(iv) emergency shutdown system >95%

(v) emergency venting and blowdown system >94%

Additions and changes made to the platform following the safety case review include:

(a) Tensioning or torque equipment is used to ensure that correct flange tightness is achieved, and tightening of large flanges on process pipework is now carried out by specialist contractors.

(b) A comprehensive review was carried out of small bore connections in pipework carrying hydrocarbons, and where possible such connections have been eliminated.

(c) Since fatigue failure due to harmonic vibration of pipes is recognized as a potential source of leaks, vibration surveys and on line stress analysis techniques were used to identify potentially vulnerable piping sections and supporting arrangements modified accordingly.

(d) Blast relief and protection has been improved, since it is not possible to completely eliminate the possibility of an ignition of hydrocarbon gas within process modules.

(e) A skyscape personnel evacuation system was added, so that personnel could easily reach water level in the case of an emergency.

(f) A safe module was modified to meet the requirements of the temporary refuge required in the Safety Case legislation, which based on the Brae B hydrocarbon inventory include a self-contained endurance period of 90 minutes.

~~Risk Analysis and Quantitative Risk Assessment~~

~~Finally, some limited further discussion on the stated intent of the UK Regulations may be useful for a full understanding of the Brae B risk assessment process, and the use Marathon made of QRA while preparing the Brae B safety case. The HSE publication A Guide to the Offshore Installation (Safety Case) Regulations 1992 (HMSO, London) defines terms, and provides substantial guidance on risk assessment techniques and their application. Based on these guidelines, the HSE:~~

~~(i) defines Quantitative Risk Assessment (QRA) as: "....the identification of hazards and the evaluation of the extent of risk arising therefrom incorporating calculations based upon the frequency and magnitude of hazardous events." (Regulation 2).~~

~~(ii) requires "a demonstration, by reference to the results of suitable and sufficient quantitative risk assessment, that the measures taken (in relation to the hazards) will reduce risks to the health and safety of persons to the lowest level that is reasonably practical." (Guidance on Schedule 2, #11).~~

~~(iii) defines reasonable practicability, as:~~

~~"Under the HSW Act, as interpreted by the courts, duty holders discharge their responsibilities when they can show that there would be a gross disproportion between the cost (in money, time or trouble) of additional preventive or protective~~

measures, and the reduction in risk they would achieve." (Content of Safety Cases: General Guidance #77).

(iv) makes the following distinctions between Engineering Analysis, Risk Analysis and Quantitative Risk Assessment:

"*Analysis*....refers to the objective process which produces information about the risks as its result. *Assessment*....is the process by which the results are considered against judgment, standards and criteria, to show that measures in place are adequate. Maintenance by the duty holder of a clear distinction between the two terms will improve the quality of the assessment presented in the safety case..." (Ibid #83).

"*Engineering analysis* includes the application of deterministic engineering and scientific calculations and qualitative judgment to indicate the safety margins available and the extent of defense in depth against hazardous events. Such analysis will often be implicit, where engineering codes and standards are used which have been derived from experience and prior analysis. Much of the physical design justification will depend on this approach. However, there is scope for *risk analysis*, which includes formal analytical methods such as failure modes and effect analysis (FMEA), and fault and event trees, to show the relationships between initiating events, affected systems or components and final outcomes. These analyses will identify hazards for explicit consideration; further engineering and risk analysis may then be required to evaluate such hazards and their potential consequences, in an iterative process". (Ibid #84).

"*Quantitative risk assessment (QRA)* (formally defined in regulation 2) otherwise known as probabilistic risk assessment is a discipline capable of giving further insight into the levels of risks and the adequacy of safety related systems. QRA begins with a formal qualitative risk analysis, which itself can reveal weaknesses which could be rectified there and then. It also allows the various components of

~~risk, and possibly the overall risk, to be quantified where input data are available on failure rates and consequences. Considerable effort may be needed to quantify, but it should be done where the value of the information generated justifies the effort." (Ibid #85).~~

Appendix D

Example Australian Drilling Safety Case

~~The Reading & Bates~~ *An* Australian *Drilling* Safety Case *presented to the panel* is an example of a complex and sophisticated non-quantitative risk assessment analysis with apparent high credibility. It employs mathematical techniques to analyze a rank ordered list of hazards coupled with historical databases and modeling assessment of consequences. It is viewed to be non-quantitative in that the approach is heavily based upon ~~opinion and~~ *expert* judgments at all stages of the analysis.

~~R&B is an international offshore drilling contractor operating a fleet of twenty four rigs. These comprise 12 Jackups, 8 semi-submersibles, 2 tender assist vessels, 1 dynamically positioned drillship, and 1 dynamically positioned construction vessel. R&B has conducted 7 United Kingdom and 2 Australia Vessel Safety Cases. The personnel conducting the current Australian Safety Case are experienced middle management and technical personnel working out of the R&B Perth office. The particular analysis discussed herein was performed during May - June, 1996.~~

The ~~R&B~~ risk assessment methodology and process is comprised of 4 main components:

- Hazard Identification: identifies hazards peculiar to a specific rig; ranks the hazards qualitatively and groups them according to type; and selects major accident events (MAE) for assessment.

- Risk Assessment: evaluates frequency and consequences of occurrence; and assesses sensitivity of assumptions.

- Results and Risk Acceptance Criteria: This is the basic mathematical portion of the work; combines frequency and consequence to determine risk; determines risk results for individual at-risk worker groups; and sorts major risk contributors.

- Risk Control Measures: This proposes actions based upon the analytic results; identifies risk reduction measures (upgrades to the rig) and evaluates benefits of such measures using the concept of "As Low As Reasonably Practicable-ALARP", and develops a plan for implementation.

Identifying the hazards involves both the rig and the area management work force through data base search and interviews with an approximately one week rig visit by the analytic team. Compartment surveys were conducted, scenarios of accidents were prepared and investigated, and the overall system response and vulnerability to MAEs were specified. A total of 204 hazards were identified during the team sessions. The hazards identified were ranked for potential Severity of Consequences, and Frequency of Occurrence according to the qualitative guidelines presented in ~~R&B's~~ Tables D-1 and D-2.

Table D-1 Hazard Identification Severity Ratings

Rank	Description	Comments
5	Extremely Severe	Major Accident Event (MAE). More than one fatality, and/or loss of MODU.
4	Severe	One fatality, possible loss of MODU.
3	Significant	Multiple LTAs or one very severe LTA, significant damage to MODU.
2	Minor	One LTA, or multiple non-LTA injuries, possible slight damage to MODU.
1	Very Minor	One first aid or no injuries expected, no damage to MODU

Table D-2 Hazard Identification Frequency Ratings

Rank	Rating	Comments	Examples
5	High	Could be expected to occur once or more during a year of operation. Equivalent to 1+ in 1 years, or about 1000+ / 1000 years.	LTA accident - 0.5 to 2 per year First aid accidents
4	Possible	Could be expected to occur 2 to 3 times in the lifetime of a MODU. Equivalent to about I in 10 years or about 100 / 1000 years.	370/1000 minor engine room fire 297/1000 crane dropped object
3	Remote	Could be expected to occur once in the lifetime of 3 to 4 MODUs. Equivalent to about I in 10 years or about 100/ 1000 years.	25/1000 blowout with 14 wells/yr 9/1000 large engine room fire 7/1000 well testing year round 5/1000 serious lost tow line
2	Very Remote	May occur once in 3 years in the worldwide jackup fleet (335 units), or once in 8 years in the semi fleet(125 units). Equivalent to about 1 / 1000 years.	4.9/1000 blowout one explo. well 1 .8/1000 serious crane drop 1.7/1000 dropped BOP 1/1000 accommodation fire 0.9/1000 shale shaker fire 0.7/1000 well testing 10% of year 0.7/1000 dropped block
1	Extremely Remote	May occur once in 30 years in the worldwide jackup fleet (335 units), or once in 80 years in the semi fleet (125 units). Equivalent to about 1 in (80 x 125) years or 0.1 / 1000 years.	0.65/1OOOship collision on station 0.5/1000 tow collision w/platform 0.03/1000 sunk by tow collision 0.02/1000 helicopter crash 1 flight

Finally, a 5 x 5 Risk Matrix of Severity Rank vs Likelihood of Occurrence (Frequency) was constructed combining the two tables, ~~above~~. The Matrix entries ***in Table D-3*** were arbitrarily assigned values (rank) from 1 to 25 with judgmental definitions according to ~~R&B's~~ Table D-4.

Major Accident Events were then selected in the Risk Ranking category 18-25 where potentials for more than one fatality were thought to exist. Initial event frequencies and event escalation probabilities for each MAE were assigned using interpretations of the World Offshore Accident Database (WOAD), the Blowout Database, the Offshore Reliability Database (OREDA), and ~~R&B~~ Corporate Accident Statistics. Rig and area specificity for frequencies was accomplished by applying modification factors based on the data with Australian data preferred (sparse), and North Sea data made acceptable "if properly justified". Assessment of the specific consequence impacts was achieved by modeling the impacts of fire, explosion, gas dispersion, and structural collapse. Impairment criteria were defined and applied to the models. Survival of persons was based on initial event impacts on escape and evacuation difficulties. Survival of structures was based on endurance time under the event environment. The number of fatalities to workers were estimated considering all relevant stages of the event from the initial event through rescue to sanctuary.

The computation of specific fatality risks used the previously discussed frequencies of occurrence, consequences, and emergency responses for the modeled events and applied an Event Tree approach. The Event Tree enabled specification of "all possible" outcomes and escalations, considered a variety of emergency responses, and considered a range of wind and sea state conditions. The calculation of fatality risks was made in a standard manner by summing the results for all event branches and all stages of an accident. Risk results were assigned to specific worker groups through analysis of relevancy of the tree branches to each of the major groups. The

Table D-3

Severity	Frequency				
	1	2	3	4	5
1	1	2	3	4	5
2	6	7	8	9	10
3	11	12	13	14	15
4	16	17	18	19	20
5	21	22	23	24	25

Table D-4 Risk Matrix Levels

Risk Ranking	Ranking Description
1 - 8	The risk is safe by any criterion, no further action required.
9 - 12	The risk is not serious. It does not require immediate action, but should be periodically revisited to ensure that risks remain acceptably low. Events to be captured in hazard register.
13 - 17	The risk is moderate. It requires further review of causes, preventive measures, and controlled responses to determine the potential for escalation and to ensure risk is within acceptable limits. Events to be captured in hazard register.
18 - 25	The risk is high. It requires further management action and prompt review of control and mitigation measures, and may require quantitative risk assessment and ALARP measures.

overall results aggregated the risks for all MAEs, and the rig and worker groups. Additionally, the major risk contributors were identified. The final measure of risk was 'Individual Risk per Annum - IRPA" for the major risk contributors. These were compared with the Fatality Risk Acceptance Criteria based upon the criteria developed during the UK Safety Case process wherein 10^{-3} per year is viewed to be the maximum tolerable and 10^{-5} per year is broadly acceptable. The region between is tolerable if it conforms to ALARP criteria.

The analysis included a demonstration of ALARP for the top 80% of risk contributors with equipment or design changes and procedural and/or training enhancements. Potential rig upgrades, included hazard identification exercises and satisfaction of specific regulatory requirements, both involving the workforce. Cost-Benefit analysis was conducted using the method of 'Implied Cost of Averting a Fatality - ICAF". A plan was developed for implementation of the risk control measures with agreement with the DME.

While the results of the ~~R&B~~ Australian ***Drilling*** Safety Case are numerical, appear to be quite precise, and may be interpreted to accurately represent the safety issues, considerable uncertainty exists due to the high content of non-objective judgment involved. Further, while it was asserted that sensitivity analysis was conducted, no evidence of the latter was contained in the methodology and results presented. Specific observations are:

Hazard Identification, potential severity of consequences, and frequency of occurrence was done subjectively.

No verification of completeness or inclusiveness was accomplished for hazard lists and scenarios was done (i.e., "a sanity check") except via analysis team discussion.

Risk Ranking was admittedly qualitative, based on the experience and judgment of the personnel.

The MAE selection was also done on a subjective, non-quantitative basis. The various categorizations and rating schemes are coarse and may be expected to hide important fine

structure. (However, one must constrain the size of the analysis for various practical reasons.)

The use of historical databases is, perhaps, as useful as could be expected; however, most of the data is less applicable to the circumstances than desirable and too anecdotal and coarse to give good insight into cause and effect. Further, historical data selection was subjective.

The techniques of modeling of consequence impacts are suspect in terms of the overall effort given to this work.

The determination of impacts to workers was subjective.

The event tree approach may or may not consider "all possible outcomes and escalations".

The elimination of other than the defined MAEs causes uncertainty in the applicability of the results.

The acceptability and use of ALARP is subjective.

~~The basic Fatality Risk Acceptance Criteria as a basic standard is a matter of policy, the values for which appear in the UK Safety Case to have been determined in a non-traceable, trial and error manner by interchange between the regulatory authority (subjective interpretation of public policy) and the enterprise operators (acceptable anticipated incurred costs).~~

Potential Rig Upgrades and Cost-Benefit Analysis results are suspect because of the fundamental non-quantitative basis for the analysis and uncertainties associated with the "benefits" to be achieved (i.e., the value put on a human life).

It appears that causative factors, principally human factors, have been ignored. The event tree analysis begins with the occurrence of an event assumed to happen.

~~The DME, as the designated authority, is an equal partner to the Safety Case outcome with the enterprise operator.~~

4: Installation Safety Management System
- **4.1 Introduction**
- **4.2 Organisation**
- **4.3 Personnel**
- **4.4 Communications**
- **4.5 Procedures and document control**
- **4.6 Activity control**
- **4.7 Expert Safety, Health and Environmental support**
- **4.8 Verification and audit**
- **4.9 Emergency response**
- **4.10 Maintenance**

5: Identification and Control of Major Hazards
- **5.1 Introduction**
- **5.2 Systematic risk assessment**
- **5.3 Hazard identification**
- **5.4 Integrated studies**
- **5.5 Independent studies**
- **5.6 Risk assessment- criteria and results**

6: Concluding Summary and Follow-up Plans
- **6.1 Introduction**
- **6.2 MOUK management of safety**
- **6.3 Risks, prevention and protective measures and remedial plans**
- **6.4 Conclusions**

7: References