TNO-TUD Report
TNO BI-92-123
TUD 6.92.26

FORMAL SAFETY ASSESSMENT of Offshore Structures

Prepared by:

J. Jongebloed
J. Wardenier
A.C.W.M. Vrouwenvelder

Offshore Engineering Major
Section Steel and Timber Structures
Faculty of Civil Engineering
Delft University of Technology
The Netherlands
1992

Preface

In this report Formal Safety Assessment (FSA) is presented. The report is the result of a (literature-)study to FSA. The main difficulty with FSA is the lack of substantial available information, since this is a new feature in the offshore industry. Intention is made by governments to adopt in their regulations the obligation for an operator to carry out an FSA for each of its installations.
This report deals with the various aspects concerned with FSA. Important aspects are a demonstration that the company has a suitable Safety Management System (SMS) and a demonstration by Quantitative Risk Assessment (QRA) that the risks from potential major hazards have been minimized.

Acknowledgement
The authors want to thank F.S.K. Bijlaard (TNO) and A.H.M. van der Pal (Protech International) for their assistance in the preparation of this report and their critical review.

Note
References to literature, including literal adopted parts, are made by [].

Contents

Abbreviations

ALARP	As low as is reasonable practicable
CBA	Cost Benefit Analysis
CIMAH	Control of Industrial Major Accident Hazards (UK)
CSE	Concept Safety Evaluation
DEn	Department of Energy (UK)
EFFECTS	PC software package for effect calculations (TNO)
ESD	Emergency shutdown
ESV	Emergency shutdown valve
EZ	Economische Zaken (Ministry of Economic Affairs, The Netherlands)
FACTS	Failure and ACcidents Technical information System (TNO)
FMEA	Failure Mode and Effect Analysis
F-N curve	Group risk curve
FSA	Formal Safety Assessment
GoM	Gulf of Mexico
HARIS	PC-based data system to support risk and reliability studies (Elsevier, UK)
HAZAN	Hazard Analysis
HAZOP	Hazard and Operability study
HAZOP-PC	PC software package for HAZOP documentation
HSC	Health and Safety Commission (UK)
HSE	Health and Safety Executive (UK)
MHIDAS	Major Hazard Incident Data Service (AEA Technology, UK)
MSC	Management Safety Committee
NPD	Norwegian Petroleum Directorate
OREDA	Offshore Reliability Databank
Protech	Stork Protech bv (The Netherlands)
PTW	Permit to Work
QRA	Quantitative Risk Assessment
REAGAS	PC software package for gas cloud explosion calculations (TNO)
RISKCURVES	PC software package for risk analysis calculations (TNO)
SMS	Safety Management System
SodM	Staatstoezicht op de Mijnen (State Supervision of Mines, The Netherlands)
SPC	Safety Program Committee
SSIV	Subsea safety isolation valve
TESEO	Method for human factor analysis
TNO	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (The Netherlands Organization for Applied Scientific Research)
TRA	Total risk analysis
TSR	Temporary safety refuge
TUD	Technische Universiteit Delft (Delft University of Technology, The Netherlands)
UK	United Kingdom
UKOOA	United Kingdom Offshore Operators Association Ltd
WOAD	World Offshore Accident Databank (Veritec, Norway)

Abstract

The Cullen Report will have a significant and long lasting impact on the worldwide offshore industry, and especially for the North Sea area.
In the near future, an operator will be required to submit a Safety Case to the regulatory body in respect of each of its installations. The Safety Case is a matter of ensuring that an FSA has been carried out, the purpose of which is to demonstrate that the potential major hazards of the installation and the risks to personnel thereon have been identified and appropiate controls provided. The Safety Case should demonstrate that certain objectives have been met. The Safety Case should be made for all mobile and fixed installations and should apply to both planned and existing installations. The two key points are the Safety Management System (SMS) and Quantitative Risk Assessment (QRA).
The SMS of the company is expected to set out the safety objectives, the system by which those objectives are to be achieved, the performance standards which are to be met and the means by which adherence to those standards is to be monitored. Features of SMS are presented. QRA, a very important aspect of FSA, is a method of performance with respect to safety objectives. QRA provides the basis to identify major hazards that could arise from offshore activities and the precautions required or proposed to prevent or limit their consequences. QRA in the decision making process, acceptance standards and the role of Cost Benefit Analysis are discussed. QRA provides a structured, objective and quantitative approach. QRA involves identification of failure cases, frequency estimation, consequence modelling and risk summation and evaluation. The techniques involved are presented.
It should be noted that the description of FSA in this report is a rational, but nevertheless arbitrary choice. In this report SMS and QRA are seen as the two key points of the Safety Case. Companies, however, may have a different approach dealing with safety and may use a different terminology from a company policy point of view. The Safety Case would sit well with regulations which set goals rather than prescribe solutions. It is recommended to move to a more flexible safety system that emphasizes the need for concentrated, active management of safety by every individual involved. The situation in the Netherlands differs a lot from the situation in the UK. This applies to the offshore situation itself as well as the regulatory body.
A short inventory of accidents with mobile and fixed installations worldwide is presented. Most attention, however, is focussed on accidents on the North Sea.

Through FSA studies several benefits can be gained. Concluding remarks are made.

1. Introduction

1.1 General

On the evening of 6 July 1988, the Piper Alpha platform on the English Continental Shelf was completely destroyed by fire, which broke out after an initial explosion in one of the modules. The disaster claimed the lives of 165 of the 226 persons on board of the platform and 2 of the crew of a fast rescue craft, while it was engaged in the rescue of persons from the installation. The death toll was the highest in any accident in the history of offshore operations. [1].
On 13 November 1988, the Hon Lord Cullen was appointed to hold a Public Inquiry to report on the circumstances of the accident and its cause together with any observations and recommendations with a view to the preservation of the life and the avoidance of similar accidents in the future.
On 12 November 1990, the final report about the the Public Inquiry was published in the United Kingdom, generally refered to as the Cullen Report.

The contents of this Report and in particular the 106 recommendations will have a significant and lasting impact on the offshore industry. One of the most important recommendations refers to the obligation of an operator to submit to the regulatory body a Safety Case in respect of each of its installations. Part of the Safety Case will be a demonstration by Quantitative Risk Assessment (QRA) of major hazards that the acceptable standards have been met.
The British government has adopted most of the recommendations from the Cullen Report and has converted these into her regulations concerning offshore installations. Suchlike procedures are already implemented in Norway. The Dutch government cannot stay behind in these new developments and there will almost certainly be adoption of the recommendations, as far as relevant to the Dutch situation, [2]. Large operators have already started to implement these new safety methods. So, the offshore industry must be prepared to satisfy these new requirements.
The Netherlands Organization for Applied Scientific Research (TNO) and Stork Protech bv have decided to combine their relevant strength and expertise and are now in a position to offer a comprehensive service in the field of Formal Safety Assessment (FSA) for offshore installations. For this a special FSA project group has been established. TNO offers a wide range of specialist services to the industry in the field of risk analysis, fire and explosion protection, failure analysis, etc. Protech is a leading engineering and consultant company providing design, engineering and management services to the oil and gas industry.

1.2 Aim

The thesis with subject Formal Safety Assessment (FSA) is being carried out under the supervision of the FSA group TNO-Protech. This report aims to give an introduction of FSA in all its aspects. Both safety management and risk assessment are dealt with. However, most attention is focussed on the 'technical' side of FSA (i.e. QRA).
The description of FSA in this report is a rational, but nevertheless arbitrary choice. SMS and QRA are seen as the two key points of the Safety Case. Some companies, however, may have a different approach. SIPM, for example, considers the SMS to be the key point, which incorporates QRA as a technique to highlight the areas requiring

particular attention.

Except for the difficulty mentioned in the Preface, there is another (main) difficulty. This is the terminology used in the divers literature. Many times different terms are used for the same or almost the same aspects. This latter applies especially for the methods/techniques involved in QRA. This is very confusing. In this report attemps are made to provide a clear explanation of the QRA techniques and the 'correct' use of the terminology.

2. Safety Assessment

2.1 Introduction

The Piper Alpha disaster involved the realisation of potential major hazards, [1]. There was a hydrocarbon leak and an explosion inside the gas compression module followed by the rupture of gas risers, which added very large amounts of fuel to the fire. Although such remote but potentially hazardous events had been envisaged Occidental (the operator) did not require them to be assessed systematically; nor did the offshore safety regime require this. There was for major projects no comprehensive system of safety assessment and management did not appear to appreciate fully the contribution which it could make.
In the near future, an operator will be required to submit a Safety Case to the regulatory body in respect of each of its installations, figure 2.1. The two key points are the Safety Management System (SMS) and Quantitative Risk Assessment (QRA).

2.2 Safety Case or FSA

Safety is 'control of accidental loss'. This includes both preventing accidents and keeping losses to a minimum when accidents occur. An accident is 'an undesired event that results in harm to people, damage to property or environment and loss of supporting capability'. Thus the word safety covers it all, [3].
Safety is crucially dependent on management and management systems. The Safety Case should show among other things that the company has a suitable Safety Management System (SMS). A Safety Case is a matter of ensuring that a Formal Safety Assessment has been carried out to assure safe operations. The SMS should give the start to carry out an FSA. FSA involves the identification and assessment of hazards over the whole life-cycle of a project from the initial feasibility study through the concept design study and the detail design to construction and commissioning, then to operation, and finally to decommissioning and abandonment, [1].
It is suggested to use the term 'Formal Safety Assessment' or FSA to describe the process of assessment and the term 'Safety Case' to mean the output from this process, [1], [4]. See figure 2.2.

The QRA being part of the FSA will demonstrate that potential major hazards of the installation and the risks to personnel thereon have been identified and assessed, and are under control and that the exposure of personnel to these hazards has been minimized. QRA involves identification of failure cases, frequency estimation, consequence modelling and risk summation and evaluation. The techniques used include hazard and operability (HAZOP) studies, event- and fault tree analysis, effect modelling and human factor analysis.

The need for FSA arises because of the combinations of potential hardware and human failures are so numerous that a major accident hardly ever repeats itself, [1]. A strategy for safety management must therefore address the entire spectrum of possibilities.

The FSA structure is shown in figure 2.3.

2.3 Objectives

The offshore Safety Case should demonstrate that certain objectives have been met. The undermentioned list does not have the intension to be complete, but rather gives an impression of the kind of objectives. For each installation (or project) specific objectives will be listed depending on:

- type of installation (fixed/mobile, exploration/production)
- age and lifetime of the installation (new/existing)
- requirements from the operator
- regulations from the regulatory body
- etc.

Objectives of the offshore Safety Case should include the following, [1]:

- a demonstration that the Safety Management System (SMS) of the company and that of the installation are adequate that the design and the operation of the installation are safe.
- a demonstration that the potential major hazards of the installation and the risks to personnel thereon have been identified and appropiate controls provided.
- a demonstration by Quantitative Risk Assessment of major hazards that acceptance standards have been met in respect of risks to the integrity of the temporary safety refuge (TSR), escape routes, embarkation points and life boats from the design accidental events, and that all reasonable practicable steps have been taken to ensure the safety of persons in the TSR and their safe and full evacuation, escape and rescue.
- a demonstration that the inventory of hydrocarbons on the installation and in the risers and pipelines connected to the installation have been minimized.
- a demonstration that a fire risk analysis has been carried out.
- a demonstration that adequate provisions have been made against hazards arising from risers and pipelines. This involves a demonstration that the vulnerability of emergency shutdown valves (ESVs), and if necessary subsea safety isolation valves (SSIVs) to severe accident conditions has been minimized and to assess their ability to survive such conditions.
- a demonstration that the ingress of smoke and/or gas into the accommodation module and control room is minimized and that the quality of breathable air is maintained, when the external firewall is subjected to severe hydrocarbon fire. This involves smoke and gas detectors and arrangements for automatic ventilation shutdown on the detection of smoke or gas.
- a demonstration that all emergency systems, including communication, control (like fire water deluge, shutdown, etc.) and protection, are available during, and have the ability to survive, severe accident conditions. Severe accident conditions, for example, are fire, explosion, collision and strong vibration.

2.4 Main tasks

The above mentioned objectives can be best achieved by performing different tasks. The following main tasks are distinguished, see also figure 2.3:

- description of the Safety Management System (section 3.5)
- description of the installation (section 3.6)
- carry out a QRA-study (section 3.7 and chapter 4)
- documentation (section 3.8 and section 4.6)

3. Offshore Safety Case / FSA

The Cullen Report, [1], and especially chapter 17, was the basis for this chapter and is not refered to in the text.

3.1 Current use of FSA

Some companies operating in the North Sea require the use of safety assessment for major projects, and did so prior to the Piper accident. Nowadays more and more companies produce FSAs although this has not been required yet by any offshore regime. However, the Norwegian Petroleum Directorate made a big move on this with their Regulations on Risk Analysis.
BP International, for example, uses a formal Project Review Procedure conducted at 6 distinct stages of a project, starting with definition and feasibility and going through operation, in which audit teams seek to identify any outstanding safety issues. There is a formal requirement to carry out HAZOP studies at the detailed design stage and the results are scrutinised by the audit team. Conoco (UK) Ltd has also carried out an FSA at the conceptual stage of a project, based on the Norwegian Concept Safety Evaluation (CSE). The objectives were to demonstrate the safety and reliability of the design, to detail the operational requirements and limitations and to provide the basis for continuing safety assurance after handover. The outcome of the work was a systematic, documented review of all significant accident scenarios and the associated precautions. This year, the FSA group TNO-Protech started to carry out safety assessments on the Dutch Continental Shelf for 17 Amoco platforms, including 2 production units.

The CIMAH model (Onshore Safety Case)
Onshore major hazard installations in the United Kingdom are subject to the Control of Industrial Major Accident Hazards (CIMAH) Regulations, 1984. There is a regulation that the operator should provide the Health and Safety Executive (HSE) with a written report on the safety of the installation. This written report is commonly called the Safety Case. The four main headings of this report relate to information on every dangerous substance involved in the activity, on the installation itself, on the management system and on the potential major hazards.
Some other Regulations are the requirement for a demonstration of safe operation, notification of major accidents, updating of the Safety Case, an obligation to supply the HSE with further information, preparation of an on-site and off-site emergency plan and provision of information to the public.

In the first instance the Safety Case is a means by which an operator demonstrates to itself the safety of its activities. The Safety Case is concerned with management and software as well as with hardware. In practise Safety Cases submitted are for the most part prepared by the operator's personnel, although some use is made of consultants for specialised work such as consequence modelling, particularly by smaller companies. The Safety Case also serves as the basis for the regulation of major hazard activities. On receipt of a Safety Case the HSE first checks to ensure that all information required is provided and to identify any matter of immediate concern. The report is then assessed by a multi-disciplinary team including specialists from HSE's Technological Division, the local area inspectors and as necessary local specialists in the Field Consultant Groups. Any matters of concern are then taken up by letter or by visit.

Following this initial response, the report constitutes an important input into the inspection strategy and provides a basis for selecting areas which should receive priority attention.
A CIMAH site is normally visited annualy by inspectors. Inspectors are required not only to look at the hardware, but also to look closely to the management of that hardware and the hazards associated with it. They have to ensure that a company is setting the appropriate standards, that they know what potential problems they have and that they are monitoring and assessing what they are and what they are doing. Inspectors have the skills in identifying quickly the failings that are leading to inadequacies on the ground and identifying where in the overall management structure the weakness is, and homing in on it as quickly and effectively as possible.

The Safety Case is not a licensing or approval system. It does not transfer some of the responsibility to the licensing authority. The Safety Case works out well and so does the role of quantification. Many operators have reported that they found the exercise of producing a Safety Case valuable. Many stated that the exercise had led them to make changes in their approach and improvements to systems and procedures. The CIMAH Regulations are believed to have largely achieved their aims.

The Norwegian model
The Norwegian offshore regime has developped in the same general direction. The Regulations Concerning Safety Related to Production and Installation in 1976 contained a requirement that if the living quarters were to be located on a platform where drilling, production or processing of petroleum was taking place, a risk evaluation should be carried out. A more quantitative approach from the Norwegian Petroleum Directorate (NPD) came with the Guidelines for Safety Evaluation of Platform Conceptual Design published in 1981. These centered around the provision of a shelter area, required the conduct of a Concept Safety Evaluation (CSE), and specific numerical acceptance standards. This CSE was based on QRA ideas. Events required to be evaluated, where relevant, were: blow-out, fire, explosion, falling objects, ship collision, helicopter crash, earthquakes, all other possible types of accidents, extreme weather conditions and combinations of these accidents. It was required that based on the defined accidental events a set of design accidental effects should be specified, expressed in terms of heat flux and duration, impact pressure, impulse or energy and acceleration. Explicit numerical acceptance criteria were stated.
Many formal safety assessments and risk analyses for offshore installations were carried out in the Norwegian Sector to comply with NPD regulations, [5]. If a regulation laid down a particular requirement, but risk analysis indicated that this was not necessary, an exemption from the regulation could be granted. Conversely, the analysis might show that the minimum requirement in the regulation was not sufficient.
Statoil performs a total risk analysis (TRA) at the detail design stage in addition to carrying out a CSE at the conceptual stage. This TRA is developped by Statoil itself.

The 1981 Guidelines were replaced by the NPD Regulations on Risk Analysis, which came into force in January 1991, [5]. These new Regulations require that safety analysis should be carried out through all phases from the concept to operation, but the choice of the methods would be left to the operator. The new Regulations no longer contain a stated numerical acceptance criterion. Instead, the operator is required to establish its criteria before the start of the conceptual design. However, the acceptance criteria required are not less stringent. The philosophy underlying the legislation is one of progressive improvement.

DEn practise and UKOOA submission on an FSA
The Department of Energy (DEn), United Kingdom, presented a discussion document on FSAs of offshore installations. The document was in 2 parts. The first dealing with the principles of FSA listed installations to be covered, hazards to be considered, techniques which might be used and project stages at which assessments should be carried out. It stated that there should be written procedures for undertaking FSA and that the outcome of the FSA should be documented and subject to independent regulatory review. The second part covered both hardware and management aspects and gave more details of the techniques, including HAZOP and QRA.
The document created a requirement for something analogous to the onshore Safety Case. However, it was perceived to be weak on management and human factor aspects. The FSA envisaged in the discussion document would apply to mobile as well as fixed installations, in fact to all installations, including floating production vessels and multi-purpose vessels.

UKOOA (United Kingdom Offshore Operators Association Ltd) submitted that the operator should be required to carry out an FSA, equivalent to a CIMAH Safety Case, in a planned manner at specific stages of the project such that the findings could be incorporated into the design or any proposed change in operating activity. The operator should define the design accidental events and the acceptance criteria. Quantitative methods should be used where appropriate. This FSA should be done by the company personnel with the help of outside consultants confined to specialised work, such as consequence modelling. FSA should be applicable to both new and existing installations.

Offshore Safety Case / FSA
Cullen is convinced that an FSA is an essential element in a modern safety regime for major hazard installations and that it has a crucial role to play in assuring safety offshore. FSA should take the form of a Safety Case. The regime should have as its central feature demonstration of safe operations by the operator.
There should be a requirement for an offshore Safety Case, based broadly on the CIMAH model for onshore installations.

3.2 Nature and purpose

Primarily the Safety Case is a matter of ensuring that every company produces an FSA to assure safe operations. Only secondarily is it a matter of demonstrating this to a regulatory body. The Safety Case should demonstrate that certain objectives have been met, see section 2.3.
The Safety Case should demonstrate that the company has a suitable Safety Management System. The offshore Safety Case, like that onshore, should be a demonstration that the potential major hazards of the installation have been identified and assessed, and are under control and that the exposure of personnel to these hazards has been minimized.
An installation needs to be self-sufficient in providing protection for personnel. The Safety Case should demonstrate that it possesses a temporary safe refuge (TSR) and escape routes which will endure for a sufficient time to allow safe and full evacuation, escape and rescue. It is difficult to see how those demonstrations should be done other then by QRA. Accordingly it is proposed that QRA is required, and this goes beyond what is required onshore. It is clearly practical, since it is included in many onshore

Safety Cases and is the basis of the Norwegian CSE. It is considered justified for offshore installations, because large number of people not only work but also live on them and the risks on the installations are relatively high.

The Safety Case should normally be prepared primarily by company personnel. A company which is competent to operate an offshore installation should be competent to produce the Safety Case. Involvement of the company's own personnel is the best way to obtain the full benefits within the company and for the purpose of dialogue with regulators. It is desirable that the operator should deal itself with the QRA aspects of the Safety Case rather then contract them out. Consultants have a role in bringing in an independent perspective and assisting with novel and specialist techniques.

Positive effects of a Safety Case, [6]:
- It stimulates a systematical approach of safety during all the phases of a project.
- The management system has the central role it deserves.
- It gives the oportunity for flexible changes in specific situations.
- Improved insight in risks and risk determining factors.

The main purpose of the offshore Safety Case is to assure safe operations, and to improve and maintain the safety in such a way, that acceptable standards have been met during an offshore installation's life-cyle.

3.3 Application of Safety Case / FSA

The offshore Safety Case should apply to both fixed and mobile installations. Cullen recommends that a Safety Case should be required for both planned and existing installations as is the case onshore.
The Safety Case should not be seen as a one-off exercise, but as a part of a continuing dialogue between the operator and the regulatory body. The Safety Case needs to be kept up-to-date. It should be updated at regular intervals or if there is any material change affecting it. The most fundamental change will be a change in operator. An updating should also be required if their is a major emergency on the installation (with or without precautionary evacuation), if there are major modifications or if there is some major technological innovation or the discovery improved understanding of a major hazard which might justify it.
Given that the Safety Case should be updated if there is a major modification, there will be a need for the regulatory body to define what constitutes a major modification for this purpose. Provision should be made in order to avoid the need for more than one Safety Case to be updated by an operator at the same time and to enable the regulatory body to postpone the automatic updating where it has recently required a discretionary updating.
As regards modifications to the installations or their equipment or procedures, the operator should, before putting the modification into effect, ascertain what effect it has on the relevant components of the Safety Case. An operator should be required to report to the regulatory body all intended modifications which meet criteria set by the regulatory body, with a view to the discussing with the regulatory body whether and to what extent a review of the Safety Case is required.

The offshore Safety Case should be, [6]:
- made for new installations

- made for existing installations
- updated after every change affecting it
- updated every five years

Installations which fall under FSA:
- fixed units
- mobile units
- subsea systems
- risers and pipelines
- all other exploration and/or production installations

3.4 FSA practise for new and existing installations

In keeping with the concept of the FSA being a living process encompassing all stages of the life of a development, the Safety Case should be reviewed and updated at key stages, [4]. The key stages envisaged are: Concept, Detailed Design and Review during operation.
At the Concept stage the Safety Case will provide a broad overview of the engineering determining the eventual layout and configuration, and the management philosophy to be adopted. All design options considered should be discussed, and the reasons identified for the final concept selection.
The next stage of the Safety Case at the Detailed Design is essentially the core document upon which reviews are based. At this stage the operator will have an in-depth understanding of the mode of construction, operation, maintenance and inspection. Therefore these aspects should be fully addressed within this stage.
The Reviews during operation will concentrate upon any substantial differences, such as engineering modifications, procedural and management changes, simultaneous operations and abandonment.

FSA for new installations
Timescale for preparation of the various stages of a Safety Case for a new installation will be governed by the development schedule for that installation. Therefore it is essential that the FSA is incorporated as an integral part of a 'project safety plan', [4]. This clearly involves an extensive workload and perhaps a very different approach to project management and procedures for some companies. The safety plan should detail the program of studies, reviews and audits to be undertaken throughout all phases of the development. Early management commitment and the development of a strategy to meet the FSA objectives will be required.
The initial form of the Safety Case should have a CSE character. As the design develops so should the Safety Case, taking on more the aspect of a total risk analysis (TRA). It is intended that in the final form in which it is submitted the Safety Case should be based on detail design information. The specific ways in which risk analysis can be used to improve plant design are described in [7].
It will be for the regulatory body to specify the precise stage in the project for submission of the Safety Case. It is clearly desirable that some preliminary assessment of matters related to the Safety Case be submitted early in the project.

FSA for existing installations
It is not acceptable that installations are operated without a thorough assessment of what the risks are. While certain options are foreclosed once an installation is built,

there will generally be a variety of measures, both hardware and software, which can be taken to improve safety if the risks justify them. The range of installations to be addressed retrospectively will vary from those which have been in operation for many years to those which are currently under design/construction/commissioning. Since in in most cases the full detail design information is available, the Safety Case will have the character of a TRA. However, the information available for some of the oldest installations will not be as comprehensive as that for a future installation, and the quality of that information is likely to be variable. Furthermore, certain of the current techniques have only been developped and accepted offshore over the last few years and engineering standards may have advanced in the intervening period. Nevertheless for all these installations the major hazards and their means of control should be identified. However, this may necessitate a different approach to that taken for a future installation where FSA principles will be adopted from early concept development. This was further discussed during a syndicate study 'the application of FSA to existing installations', [4].
For existing installations, the question of how to ensure an appropriate level of safety is significantly different from the case of a new built, [7]. Firstly, the degrees of freedom are very much more restricted, at least with respect to major features such as layout. Secondly, the installation may be approaching the end of its useful life, so that the utility of any upgrades may be limited. Thirdly, the implementation of upgrade measures on an active installation may itself be hazardous. Fourthly, the costs and weight penalties of upgrades may be significant.
The way in which the problem presents itself is, in fact, as a large set of possible options (of which the 'do nothing' option is one). The decision to select a particular upgrade should therefore be seen in context of its alternatives. Cost and weight penalties are factors which should be considered alongside risk reduction, because the decision is really about optimal use of resources. See [7] for techniques used for identification of potential upgrade measures.
Safety Cases for existing installations should be brought in as rapidly as practicable, on a schedule to be determined by the regulatory body.

Potential problems
Potential problems, [4]:
- delays to future projects introduced by approval at the concept stage and certification prior to commissioning, which may become contingent upon submisssion of a satisfactory Safety Case.
- it could prove both difficult and expensive to recover and demonstrate a satisfatory Safety Case at the detailed design, if the concept design is poor.
- the preparation of Safety Cases for new projects and retrospectively for the large number of existing installations represents a formidable task. Not only may operators lack sufficient resources of suitable expertise, but there is evidence that this is widespread throughout the industry, i.e. consultants, contractors, regulatory bodies and certifying authourities.
- some of the benefits that an operator could accrue from a thorough review of its own activities could be lost if the major part of the FSA is not performed in-house.
- the integrated nature of the FSA demands that a single body, competent in assessing both the engineering and management control aspects, should be responsible for its regulation. It will be exceedingly difficult, if not impossible, to seperate the engineering and management controls.

3.5 Safety Management System

An important part of the Safety Case will be a description of the operator's Safety Management System (SMS). The SMS should be in respect of the design (both conceptual and detailed) of the operator's installation and the procedures (both operational and emergency) of these installations. In the case of existing installations the SMS in respect of design should be directed to its review and upgrading so far as is reasonably practicable. Safety Management is simply the management of safety and should use the same concepts as are being used in all other areas of management, [8]. The word Safety in the SMS should overlap quality, environmental care and productivity.

Scope of SMS
The SMS must ensure the identification and assessment of hazards throughout all offshore activities (i.e. exploration, production and abandonment) at all stages of development (i.e. planning, design, construction and operation), [9]. It has to demonstrate that all practicable measures are taken to prevent, control and mitigate those hazards. The operator should be required to satisfy itself by means of regular (internal) audits that its SMS is being adhered to. The SMS should be adequate for the purpose of ensuring that all activities, they are engaged in or contract other companies to carry out for them, are safe.
The Safety Management System is expected to set out:
- the safety objectives of the operator
- the system by which those objectives are to be achieved
- the performance standards, which are to be met
- the means by which adherence to those standards is to be monitored

Finally the SMS must ensure that the information in the Safety Case is factually correct, and how the operator will continue to observe the critical safety practices and the features described. Safety Management is in essence the elimination of the gap between intention and achievement, [5].

Safety of activities is to be achieved through, [8],[9]:
- responsibilities in the organisation
- setting standards for personnel in positions of authority critical to safe operations
- training personnel for operations and emergencies
- applying safety assessment or activities with risks
- setting up (critical task) procedures for design, operations, maintenance, modifications, concurrent operations and emergencies
- regular inspections Top-Down-Bottom-Up, with the help of checklists
- management of safety by contractors in respect of their work
- organisation of formalised involvement of the workplace (operations and contractors) in safety
- regular meetings of MSC and SPC
- setting up structured and sound system of accident and incident reporting, investigation and follow-up
- setting up monitoring and auditing of the operation of the system
- having a systematic reappraisal of the system in the light of the operator and the industry

The standards, procedures and work methods set by the SMS involve for example, Permit to Work procedures (PTW), Safe Control of Scaffolding and procedures for Concurrent Production and Drilling Operations.

Features of SMS

A good SMS should narrow the gap between what should and what is being done. All too often management think things are safe because they have issued a procedure but never check to see if it is being done correctly until there is an accident. [8], [10]. First you must have management commitment before you can start any really effective Safety Management System. It must start at the top, at General Manager level. Once you have that commitment, you can start. Features of SMS, [8], are described below.

The starting point is the improvement/change Integrated Safety Care. The system starts with the **plan**. This is the point where an audit is carried out to set a base for improvement. From this an action plan is developped.
An **audit** is carried out to verify whether activities comply with planned arrangements and to determine the effectiveness of the system. Audits shall be scheduled on the basis of the status and importance of the activity. The audits and follow-up actions shall be carried out in accordance with documented procedures. The results of the audits shall be documented and brought to the attention of the personnel having responsibility in the area audited. The management personnel responsible in the area shall take timely action on the deficiencies found by the audit. Safety audit as 'tool of management' is discussed in [11].

Training is an important feature. All relevant people should receive training for any new skills required of them and also to motivate them to carry out the required work. Two levels of training are necessary:

- a general introduction to put everyone on the same track and to explain why and how to do it.
- specific training courses on the items highlighted in the action plan, e.g. accident/incident investigation. To make an offshore staff appreciate that near misses and incidents should be reported and investigated just as fully as an accident is trying at times as people tend to think of 'witch hunts' where the persons involved are automatically to blame. It is important, proving that this is not the case, so that all incidents are reported and investigated.

Do is when you carry out your improvement plan making sure that a Top-Down and a Bottom-Up approach is used, e.g. the men on the platform should write critical task procedures. These follow a job inventory which highlighs critical tasks that require procedures.

Inspections are carried out with the help of an offshore inspection **checklist**.
The offshore orientation checklist is another usefull tool in making sure that everyone who works on the floor is aware of all the rules and regulations associated with working on the platform.

Top-Down-Bottom-Up is the term used to show how the management system works. It starts at the top with the General Manager deciding to put a management system in place. He can't do it all himself, and that is where committees come in. Committees form the backbone of the system, with good communication between them they can set up and monitor the program.

There should be a **Management Safety Committee** (MSC) made up of all the heads of the departments of the company, not just safety and production but also accounting, reservoir, etc. Along with this there should be a **Safety Program Committee** (SPC)

made up from both offshore and onshore personnel.
The MSC decides on the direction that they wish to go in and the SPC should decide how best to carry it out, after due consulation with the people who's work it will effect.

One learns from incidents and near misses due to the investigation and change, write procedures or carry out retraining to stop it before it becomes an accident.

Final remarks
The management has the prime responsibilty for safety. Safety is not standing on itself, [12]. Finance plays a big role, the company needs to make money. Quality, quantity and cost-price also have to be taken care of in order to not run the risk of discontinuation of the company. The mangement has the difficult task to weigh all these aspects with the right priority. In practice, many times conflict situations will occur. Then, management will have to make the right and justified decisions.

3.6 Description of the installation

The description of the facilities will include sufficient information to enable a clear understanding of the installation, this with an emphasis on the aspects relevant for safety and emergency management. Design features for safety enhancement will be clearly documented, including description of purpose. The external circumstances of the installation will be described, like metereological conditions, shipping lanes, etc.
At least the following safety sytems will be described:
- seperation and segregation
- blast relief and protection
- fire protection (active/passive)
- fire and gas, detection and alarm systems
- well systems
- isolation, emergency shutdown (ESD) and venting
- heating, ventilation and air conditioning
- emergency power, communications and lightning
- pipeline communications and control
- temporary safety refuge (TSR)
- escape routes and evacuation
- livesaving appliances
- standby boats

3.7 Role and status of QRA

Quantitative Risk Assessment (QRA) is a method of obtaining a measure of performance with respect to safety objectives, which has been developed primarily for the assessment of large scale accidents, which by their nature are very rare, and therefore not easily observable, [7]. In particular, the frequency of these events cannot be obtained directly from statistics. QRA synthesises an estimate of their frequency by a structured process of reasoning, based on statistics of equipment failure rates, human errors, accidental impacts, extremes of weather and similar 'precursors' of potential major hazards. QRA is presented in Chapter 4.
Engineers and decision makers like to use risk assessment to make the decision for them. For this purpose they would like to see well defined acceptance criteria for risk

and a calculation resulting in one number to tell them whether their design is right or wrong. Several regulatory bodies also promote the use of QRA for establishing that acceptance criteria are met. However, in general, they also promote the use of QRA to identify improvements as a means of communication between professionals, [31].

QRA in the decision-making process
QRA is only one input in the decision-making process, though an important one. Its strength is that it provides a structured, objective and quantitative approach. It gives a better understanding of the hazards and of the measures needed to control them. See figure 3.1 for the role of QRA in the decision-making process. QRA is a prime means for the operator to demonstrate firstly to itself and secondly to the regulator that it has taken all reasonable practicable measures to ensure safety, and thus provides a good basis for the dialogue between operator and regulator. It should not be used, however, in isolation or as an automatic mechanism for decision-making. The point is made in one of the documents on QRA published by the HSE: 'QRA is an element that cannot be ignored in decision-making about risk since it is the only discipline capable, however imperfectly, of enabling a number to be applied and comparisons of a sort to be made, other than of a purely qualitative kind. This said, the numerical element must be viewed with great caution and treated as only one parameter in an essentially judgemental exercise'.

Acceptance standards for QRA
The practise of QRA requires acceptance standards. There is more than one form of acceptance standard. Examples are accommodation endurance times, equipment availability targets and risk criteria. One approach to the setting of risk levels has been proposed by the HSE and has met with general acceptance, at least in principle, if not as to the precise numbers to be used. This splits risk into three bands, figure 3.2. The top band represents an intolerable risk level and action must be undertaken, the lower band represents a negligible risk and no action is required, while in the middle area the requirement is to reduce the risk 'as low as is reasonable practicable' (ALARP). If the calculated risk falls into the ALARP region, it must therefore be reduced as low as is reasonable practicable, and in order to do this it is necessary to demonstrate that to reduce it further would incur 'grossly disproportionate' costs. This then entails the use of Cost Benefit Analysis (CBA), [7].
A CBA approach is used to investigate the risk reduction per unit resource spent. The risk measure utilised in the CBA approach must obviously represent global (group, or occupational) risk rather than individual risk, to be compared with the global costs. The deriviation of a suitable single-valued measure is considered in [7]. This latter discusses the representation of the total risk impact of the installation, in pairs of numbers f_i, N_i which represent the frequency and the number of fatalities for each accident case (i) in the modelled set. The whole of the information content of this table of f-N pairs can be represented in an "F-N curve", in which is plotted the frequency of all events F in which N or more fatalities occur. The F-N curve is , therefore, a complete index of risk, and in principle it can be used for decision-making. The only drawback of the use of the full F-N curve is that the criteria of acceptability are somewhat hard to define, since they must also take the form of a line or curve drawn in the F-N plane.
Some oil-companies usually don't use F-N curves for their workers. Their safety policy is based on the fact that every individual employee should be safe. SIPM, for example, considers F-N curves to be only of real interest when dealing with risk to the public (societal risk). Instead of these curves, the use of overall Potential Loss of Life (PLL)

over the project life-cycle and Individual Risk (IR) to the most exposed workers are the preferred measures of the risk to employees, [31].

It is normal practise that acceptance standards for QRA are set by the operator. This accords the fact that QRA is generally an activity undertaken voluntarily to demonstrate compliance. Regulatory documents on risks and risk criteria should be used as guidance. In order to provide at least one fixed point in the regime, both the minimum endurance and the frequency with which their is a failure of the endurance of the accommodation, or TSR, should be specified by the regulatory body. This is proposed by Cullen.
Acceptance standards, including risk criteria, should be interpreted with flexibility by the regulatory body. However, they should be tough and set sufficiently high to result in real improvements in safety. In particular, there needs to be a reduction of the risks from major accidents.

Although QRA will almost always result in meaningful recommendations, the use of QRA in an absolute sense is not promoted by e.g. Shell for a number of reasons, [31]. It is stated that by it's very nature QRA accuracy is not very high. Also there is no single way of doing it. Therefore Shell considers that the absolute risk values resulting from QRA's should only be used as guidelines. The real benefit from QRA is in the comparison of options and the identification of the areas contributing most to the overall risk, so as to be able to focus attention on these.

QRA and the role of Cost Benefit Analysis
In a Cost Benefit Analysis (CBA), the costs of additonal protective measures are balanced against the resulting benefits in terms of reduced hazards and potential economic loss, [13]. A principal reason for extending risk quantification studies to include CBA is to provide direct inputs to aid consistency in resource allocation decisions. In addition to risk parameters concerning both 'critical' individuals and population groups, such analyses should address the likelihood of occurence of financial costs arising from accidents involving material damage both on and off-site and production losses during shutdown periods for repairs. This may then be employed in evaluating the worth of further safety measures, where statistically expected reductions in such costs can reflect an 'insurance' value.

Clearly, where these values exceed the costs of the proposed safety measures, there is a direct economic case for their implementation. In other cases, the residual or net costs will typically be set against the associated reductions in individual or occupational risk, thereby providing a measure to rank the cost effectiveness of alternative options in terms of their respective expenditure per statistical fatality averted. However, in order to utilise this in a cost benefit approach to the implementation of ALARP, it is necessary to compare these measures with appropriate monetary valuations of risk reductions, expressed in, say, $ per statistical fatality averted. This analytical framework for determining an 'optimum' level of protection which maintains residual ALARP, may be illustrated as in figure 3.3.
Whilst the apparent simplicity of this cost benefit framework is clearly attractive, its practical implementation may encompass a series of complex value judgements, involving both the monetary 'valuation of life' and the evaluation of other cost components. Some of the most relevant factors underlying these value judgements are dicussed seperately in [13].

Some companies, e.g. BP, use the cost for avoidance of a fatality as a basic criterion, [31]. However, they only apply it if the risk to personnel is below a specific threshold value. Shell E&P companies do not express the value of life in monetary terms. QRAs usually lead to clear recommendations without this valuation. Nevertheless, to assess the effectiveness of safety measures, it is recommended to calculate the amount spent to avert a fatality, [31]. However, if high values are found this should never necessarily lead to acceptance of the status quo. It should be used as a stimulus to develop more innovative and cost effective safety measures.
It is further stated that the use of the cost to avert a fatality as a rigid and absolute yardstick should be avoided. There is no amount of money that can compensate the loss of life. However, if the cost to avoid a fatality exceeds US$ 50-100 million the suggested means and measures should be considered rather ineffective and possibly counterproductive. Efforts are required to develop more effective alternatives.

Observations
The QRA technique is today in widespread use in the offshore, nuclear and chemical industries, being applied to fundamental questions of conceptual design, siting official approval and detailed design. The QRA will provide the basis to identify major accident hazards that could arise from offshore activities and the precautions required or proposed to prevent or limit their consequences.
The QRA provides a systematic and fully documented safety analysis, and will serve as part of the living process which assesses safety over the whole life-cycle of a project.

3.8 FSA report or Safety Case

The FSA report is the submitted evidence, that a full and systematic check has been made for hazards and that any potentially significant hazards have been analysed in terms of associated risks, [14]. It demonstrates that an adequate level of safety has been achieved and records the provisions that will exist in order to ensure compliance with the Safety Case throughout the installation's life-cycle.
In practise, the Safety Case submitted will be a summary of work undertaken by the operator, [4]. The Safety Case does not need to contain the detailed documentary evidence which supports the conclusions reached, but it should include sufficient detail of them to enable an independent assessor to judge whether the conclusions are sound. It should also contain precise references to where the supporting documentation can be consulted if necessary.

4. Quantitative Risk Assessment

4.1 Introduction

QRA is a powerful tool in the decision making process which can assist in the selection of acceptable solutions to safety problems. The objective of QRA is to improve safety by:

- allowing the main risk contributors to be identified; and
- by comparing alternative designs or methods of operation from a risk point of view.

QRA also provides an indication of the relative safety of the alternatives and an input into economic evaluation.

QRA involves identification of failure cases, frequency estimation, consequence modelling, risk summation and evaluation, [5], [7]. Identification of failure cases involves identification of hazards and postulating of accidents. Failure case identification is crucial to the overall quality of the analysis.
The following tasks are distinguished when carrying out a QRA-study:

- hazard identification
- identification of accident scenarios and effect-/consequence modelling
- risk analysis study
- risk management
- final evaluation and documentation

The QRA-study structure is shown in figure 4.1.

Compared to ten years ago, there is now no serious problem in obtaining the data required to estimate frequency or models to estimate consequences. The area of human factors is acknowledged to be one where improved techniques are desirable. It is also desirable to be quite open about the uncertainties inherent in QRA and to take these into account in its conduct and evaluation, using methods of sensitivity analysis.

4.2 Hazard identification

An inventory of hazards, failure modes and failure effects for the installation (system) and for individual components is called a Hazard Analysis (HAZAN), [15]. The best known hazard identification technique used within the chemical process industry is the Hazard and Operability study (HAZOP) for systems and sub-systems. The Failure Mode and Effect Analysis (FMEA) is used for components and accessory parts. [16].

HAZOP study
A HAZOP is carried out by a team of experts, [14], [16]. The team consists of members with a HAZOP-background as well as people from the company, for the need of specific company and process knowledge. HAZOP applies to new and existing systems. The HAZOP team systematically checks through all the components (equipment, pipework and instrumentation) of a system design, at the pipework and instrumentation drawing stage. Deviations from the intended method of operation are assessed for consequences and causes in order to produce an action list to prevent, minimize or allocate unacceptable occurences. This is an equipment orientated assessment.

The steps to follow when carrying out a HAZOP, [16], are described below. The HAZOP team should become familiar with the company. The team should have the disposal of information of the following items , before a complete and correct analysis can be carried out:

- an up-to-date flowdiagram
- control diagrams
- process and instrument diagrams
- process-descriptions and certifications
- instruction books
- start/restart procedures

Guidewords are used when carrying out a HAZOP. First, the installation is divided into part-processes by choosing so called 'analysis-points'. Afterwards, the team tries to find out, with the help of guidewords, wether it is possible that a specific part-process is able to work different from that what the designer had in mind. Guidewords help to find deviations from the design-functions in a systematically way, for example: *no* flow, *more* or *less* pressure, *partly*, *reversed*, *different from*, etc.
The next steps are gone through:

- formulation of the destination-function of a part-proces
- use the first guideword
- work out a usefull deviation
- check the consequences in a qualitative way
- work out the next deviation
- choose the second guideword
- etc.

A HAZOP can be carried out with the stream as well downstream. The part-processes are analysed step by step, from the incoming streams to the end-fase, or from the main-processes back to the incoming streams.

The use of guidewords creates a positive way of thinking for the HAZOP-team. It leads to discussions which are focussed to come to agreements about the most important problem-areas and recommendations for process or design improvements.
HAZOP can become very comprehensive by its systematic tackling. The HAZOP team consists of experienced people. This furthers systematic tackling of a problem and results in an choice of adequate guidewords and avoidance of the analysis of fully unlogical events.
Everytime, HAZOP seems to be able to find out the shortcomings, which somehow were slipped into the design. This makes HAZOP a cost effective instrument.
The results of the HAZOP study will be documented with the help of the widely spread software package HAZOP-PC.

FMEA
The Failure Mode and Effect Analysis (FMEA) is comparable with HAZOP, but is used for analysis of components and accessory parts, [16]. FMEA is also carried out by a team of experts. The functions, possible failure cases, and the causes and effects of every possible failure are assessed for every specific part of a component. Failures are analysed by using so called failure-causes and failure-mechanism modelling. These mechanisms are the key to resolve failures. The following failure mechanisms are distinguished in a FMEA:

- mechanical
- thermo/mechanical
- chemical

- chemical/mechanical
- filthiness
- change in material properties

Good descriptions and maintenance schedules are absolute conditions.

Observations

A failure mechanism is defined as the manner in which the structure responds to a hazard. A combination of hazards and failure mechanisms leads, with a given probability, to failure or collapse of the structure or its components. In assessing the safety of the structure it is important not to forget one of the major hazards or failure mechanisms. The mere fact that one lists the various phenomena is often more important than the complete analysis that follows, [15].

Important aids in preparing an inventory of causes of failures are data banks, literature studies, interviews, studies of actual instances of damage, brainstorm sessions, experience with simular systems, and so on.

4.3 Scenario identification and consequence modelling

This part of the QRA study will form the basis for the risk analysis and specific studies required. The following aspects are dealt with:

- identification of initiating events with possible cause of the event and location on the installation, with help of the above mentioned HAZOP/FMEA studies.
- description of accident scenarios, in which the safety provisions are taken into account.
- type of effects/consequences, by using a number of models for calculation of effects and damage. EFFECTS and REAGAS, for example, are software packages for the calculation/modelling of effects and consequences.

For offshore platforms, the initiating events generally fall under the following headings:

- spills/releases of hydrocarbons from process equipment
- blowouts
- releases from risers
- ship collisions
- structural failures
- environmental loads
- helicopter accidents
- dropped objects
- utilities failures

In practise, the above list of events is expanded into a much longer and more detailed list, specific to each platform. Typically, several hundred of initiating events might be defined, [7]. In real life, events may very in size or intensity of effect. In a QRA model, only a selection of representative events can be analysed, so it is important that the selected events are truly representatives of the real ones and that the frequency values assigned to each selected event equals the total frequency of the real events which it represents.

For complex systems it might be helpful to make a graphical presentation on how component failures and systems failures are connected, [15]. Standardized presentations are Fault trees, and Event or failure trees.

It is important to consider the system as a whole, [15]. Systems are composed of many

components, each of which may be prone to hazards and failure mechanisms. Malfunction of some component may in turn pose a hazard to some other component. The malfunctioning of one component may sometimes lead directly to failure of the system (series arrangement), in other cases components may compensate for one another (parallel arrangement). Fault and Event trees are useful aids to establish an ordered pattern in the many hazards, failure mechanisms and components.

Event tree
Event or failure tree analysis is the procedure to specify some initial event and then the consequent responses of the system. Event tree analysis identifies various hazardous events. For an example of an event tree, see figure 4.2.

Fault tree
Fault tree analysis is based on the opposite procedure of an event tree. Starting from some failure event, it is analysed how this may have been caused. In drawing up a fault tree, symbols such as AND gates and OR gates are used. The AND gate corresponds to a parallel arrangement and the OR gate to a serial arrangement. Example, figure 4.3. Fault tree analysis determines likelihood of event occurence.

Observations
Potential consequences, highlighted within the hazard analysis, are looked at in more detail in order to establish their individual severity levels. This can be qualitatively assessed against a previously prepared severity rating table which would result in a hazard ranking, usually with severity numbers between 1, minor and 5, [14]. A more robust check on consequences can be achieved using effect models, vulnerability models and calculation models. It is important to consider the consequences in relation to employees, the environment, the installation and company profits.

4.4 Risk analysis study

Objective
The objective of the risk analysis study is to include a probabilistic approach in the hazards, identified and quantified in the studies described above. Although an installation is designed to incorporate the latest technical means to prevent and mitigate accidents, accidents can never be excluded. However, with a probabilistic risk analysis, it can be shown that the frequencies of those unwanted events have been forced to (very) low levels. In this way, also the influence of safety provisions on the risk can be shown. It also allows to gain an insight in the risk contributing factors and their order of importance. An evaluation against risk acceptability criteria can be performed and possible risk-reducing measures may be recommended.
Probabilistic analysis for offshore structures is presented in [15].

The importance of data
The risk analysis will start from the scenarios identified and worked out in the earlier tasks. The event and/or fault trees will be worked out further by filling in the relevant (failure) frequencies and probabilities involved. Data is very important for the estimation of frequencies. Examples are: incident data, equipment failure data and human error data. Important incident-databanks for the offshore industry are, [17], [31]: WOAD, MHIDAS, FACTS, HARIS and OREDA.

Errors of much more than one order of magnitude can occur due to errors and omissions in the fault- and event tree analysis, [31]. Efficient cooperation between various experts can avoid these errors and is a prerequisite for meaningful risk assessment. An analysis to check the sensitivity to variations in the assumptions made is recommended in order to provide an indication of the criticality of the input data. A more detailed analysis on the most critical data can improve the confidence in results.

Data is the missing link between an accurate system failure model and its quantified risk of failure. Without suitable data, there is little hope that the quantified risk analysis (QRA) technique can offer any significant benefit. Data requirements for offshore risk analysis and data selection are discussed in [17].

Human factors
Human factors will be identified and the probability of human failure will be estimated. This can be done using the so called TESEO method.
It could be argued that no major safety incident is free from human contribution, [14]. This can be due to an error during the chain of events leading to the incident or an error during the recovery phase. These errors in themselves can be simple mistakes or errors of judgement and can occur during installation development, including construction and during operation, including maintenance. The people who make these errors include designers and safety assessors, operators and maintainers, installation managers and the company board.
The two main differences between errors that go unnoticed and those that result in an incident are: the opportunity to recover from errors and the consequences of non-recovery. It is these two aspects that must be considered during FSA and countered when appropriate, both during design and during ongoing operations.
In practice, 80-90 % of the process industry accidents is quoted to be attribute to human errors, [12]. Deeper understanding of the nature of human error is necessary for reducing and predicting human error to minimize its potential for causing damage, [18].

Specific studies
During the risk analysis specific studies will be carried out. For example:
- a detailed fire and explosion hazard assessment
- an assessment of the ingress of smoke/gas into the living quarters
- a review of the integrity and ability of emergency systems to withstand/survive severe accident conditions
- an evacuation, escape and rescue analysis
- a ventilation and vent system study

Risk calculation
By using the identified failure frequencies and probabilities in the event trees, frequencies for all possible outcomes of an accident development (branches of the event trees) are calculated. This information and the information about the location of the accidents and the possible presence of people, gives all the information for the calculation of:
- the individual risk as a function of the location on the platform. The individual risk is presented as risk contours on a map, and is independent of the presence of people.
- the group risk curve (F-N curve). The group risk takes into account the presence

of people and basically presents the frequency of certain numbers of people not able to survive accidents on the platform. As already mentioned in section 3.7 some companies do not use F-N curves for their workers.

The above risks are calculated and plotted in the requested form with the help of software packages, for example RISKCURVES.

Risk evaluation

Risk evaluation and acceptance is dependent upon some form of quantification of risk and its comparison with acceptable risk criteria. Criteria cover risk to persons, the installation, environment, etc. Risk is a function of the severity of consequence and the frequency of occurence. The frequency of occurences can sometimes be judged from previous experience but, more usually, must be estimated based on the calculated initiating event and the failure of a protective system to respond.

Severity of a consequence can either be in terms of a ranking, for example via a severity table as previously mentioned or a more accurate calculation of the costs of occurence, [14]. The overall consequence of risk for each hazard can be in the form of a comparative ranking, risk rating or an estimate of the potential cost of the hazard during the life of the installation, financial and loss of life. Those hazards that are judged to be intolerable plus hazards that are cheaper to prevent than to tolerate (Cost Benefit Analysis), should be classified as unacceptable (intolerable) risks. These must be dealt with before the submission of the final FSA report.

It should be noted that one never accepts that one will be killed. One lives with or tolerates something if their is no better way of doing it. Even then one attempts to reduce the risk further by procedures, safety management, etc.

4.5 Risk management

Risk management, being part of the SMS, is the process of using all the above information to control, and to improve if necessary, the levels of risk. The process of risk management builds upon the stages of risk analysis by addressing the question 'are the risks satisfactorily controlled ?', [5]. If the answer is no, then options to mitigate the consequences of the accidents can be evaluated, or options to decrease the frequencies of the accidents can be evaluated. In reality, both options are usually deployed. This process of postulating improvements and evaluating their effect on the risk levels is iterated until the risks are satisfactorily controlled and the options for risk management have been optimised.

The safety measures taken involve the hardware of the installation (structure, equipment, etc.) as well as the software of that installation (management, training personnel, etc.) and all extra life saving appliances like survival suits, life boats, smoke/gas hoods, and so on.

4.6 Final evaluation and documentation

In this final part of the QRA-study, an overall evaluation will be given of the safety of the installation. Conclusions from the different tasks will be summarized and related to eachother. Overall recommendations will be based on this.

The results from the QRA-study will be clearly documented and will form an important part of the FSA report.

5. Safety Assessment and legislation

5.1 Introduction

In general, any large system or problem is usually best handled by breaking it down into more manageable parts, in some form of hierarchy. Cullen proposes that the regulation requiring the offshore Safety Case should be completed by other regulations dealing with specific features.
With regard to the type of regulation, the Safety Case would sit well with regulations which set goals rather than prescribe solutions, [1]. These regulations would complement the Safety Case by setting intermediate goals and would give the regime a solidity which it might otherwise lack.
Construction of the installation, fire and explosion protection, and evacuation, escape and rescue are all areas where it is considered appropiate to retain regulations, though in goal-setting form. One method of demonstrating compliance would then be by FSA.

5.2 Regulations and the regulatory body

The regulatory body has the supervision task for the maintaining and fulfilling of the regulations and, in case of harm or an accident, to hold a public inquiry. Existing regulations are unduly restrictive by imposing solutions rather than objectives. [1], [19]. Lack of flexibility resulted from taking the legislation as starting-point for a safety and environment policy. The lack of flexibility is mainly caused by the slowness in adaption of the legislation to new situations, insights and technological developments. Primarily, the industry has an advising role, she may discuss and think, but decision-making and regulation are done by the regulatory body. The accent for the industry is set on fulfilling the regulations, rather than performing their own safety and environment management.
This sytem is passive and not flexibel and gives rise to a false feeling of safety caused by strict fulfilling of the existing regulations; its going according to the rules, so its safe. The system does not stimulate active involvement of the industry and acts as a brake on the application from technological developments and alternative solutions, [19].
It is advised by Cullen to have less a body of recommended regulations and a more flexible safety system that emphasizes the need for concentrated, active management of safety offshore by every individual involved. A framework for safety offshore rather than a maze of tangled regulations, [1], [19]. Primarily, the care for safety and environment is the task of the industry and is integrated in the managment system. The industry has to set its own safety objectives (goal-settings) and tests them by the ones from the regulatory body. It is the regulatory body's task to stimulate this process. The regulatory body's role is supervision and auditing of the management system and studies to safety and environmental risks.
The operator should be required to satisfy itself by means of regular (internal) audits that its SMS is being adhered to, [1]. The regulatory body should be required to regulary review the operator's audit on a selective basis, and itself to carry out such further (external) audit as it thinks fit and by regular inspection verify that the output of the SMS is satisfactory.
The role of the outside authority in examining the Safety Case should be to assess wether the operator has fulfilled his duties to identify and prevent major accidents. It is therefore essential that the outside authority is competent in assessing both the

engineering and management control aspects. Cullen recommends that there should be a single body responsible for the overall assessment, due to the integrated nature of the Safety Case.

5.3 The new regime

The transition to the new regime can't take place overnight. There should be a regulation requiring a Safety Case and that this should be complemented by a limited number of further defined regulations, [1]. Beyond this it must be for the regulatory body to develop the regime in accordance with the principles outlined. As regards existing regulations and guidance in accordance with the transition to the new regime, it is suggested that the regulatory body advises the industry of those regulations to which it is prepared to grant exemption in the Safety Case.

Situation in the United Kingdom
New developments on safety legislation in the United Kingdom are presented in [20], [21], [22], [23], [24]. These articles deal with offshore Safety Cases, the transfer of the Offshore Safety Division, new methods of inspection, importance of the SMS, subsea valves, the inadequacy of the government's registration of offshore incidents, and so on.
Responsibilty for regulating UK offshore safety moved from the Department of Energy to the Health and Safety Executive (HSE) on 1 April 1991. HSE, as part of the Health and Safety Commission (HSC), comes under the Department of Employment.
The HSE has laid down a timetable for offshore Safety Cases. According to a formal annoucement by the HSC new regulations on offshore safety management and offshore Safety Cases could be in place by autumn of 1992 and in force by late spring of 1993. After this a furhter six months will be allowed for operators to submit Safety Cases for existing installations. An absolute deadline, probably in 1995, will be set beyond which no installation will be able to operate in UK waters without its Safety Case having been accepted by HSE. If operators fail to meet the standards laid down for Safety Cases, there would be no hesitation in shutting down installations.
Safety Cases will be required for all fixed and mobile installations, currently numbering 272. Implementing the Cullen recommendations could not be considered to be moving too slowly, given the nature of the change involved.

The situation in the Netherlands is presented in the next chapter.

6. Situation in the Netherlands

6.1 General

According to the Inspector General of Mines in the Netherlands, the Cullen Report is a solid unprejudiced account of facts, backgrounds and arguments determining the way in which dangers are discerned and controlled, [2]. He has advised the Minister of Economic Affairs to adopt all the Report's recommendations as far as relevant to the Dutch situation.
The recommendations will be studied carefully and compared with the present situation on the Dutch Continental Shelf. The Dutch offshore situation differs a lot from the situation in the United Kingdom, [25], [26]. The installations on the Dutch Continental Shelf are smaller, simpler and more spaceous, which makes it easier to control risks. The total number of offshore operators and employees is smaller, which give less problems with communication and contacts between them.

6.2 Scope of FSA

The Cullen Report has given acceleration to a change in the approach of safety. This change involves a shifting from the technical inspection to the control of the safety management system of a company. The Cullen Report will serve as a mirror for all those involved in the offshore industry. [2], [6], [9], [25]. The Report emphasizes that the operator is responsible for the safety of its installations. The operator has to demonstrate that his installation is safe (Formal Safety Assessment), starting by the central role of the management system. This management involves maintenance, the responsibility of how to handle in dangerous situations, the preparation on emergeny situations and periodical auditing of this management. In the Netherlands there is considerable current activity to encourage companies to audit their safety management systems and to move to external certification based on compliance with some form of ISO 9000 series, [27]. These developments place a great emphasis on a formal, auditable management system with reliance on written procedures.
Although there will always be technical rules left, the inspection task of the government will shift from technical details to the safety management system. Important features of this shifting are the Norwegian rules for CSE, the Dutch "Arbeidsveiligheidsrapport", API-RP-750 and of course the Cullen Report, [6].
The necessity for this shift in approach resulted from the facts that the technical rules:

- worked out to be retrospective only.
- were discouraging innovation.
- had the propensity to transpose the responsibility from the operator to the regulatory body.

The operator has to make its own safety-goalsettings and the way to achieve this. Safety should not be looked at as a separate system, but as an integrated aspect of the total design and the total management system. It is recommended by Cullen to integrate Safety in Health and Environment (SHE). According to the Inspector General of Mines in the Netherlands, a unification of inspections under one umbrella, like the Health and Safety Executive in the UK, would not improve the current situation, [2].

6.3 SodM, starting points and regulations

Many Cullen recommendations were already implemented in the Dutch Mining Law and the department concerned with supervision. [2],[25]. Most operators have also integrated the recommendations in their management system. However, further talks between the State Supervision of Mines (SodM) and operators are necessary.

The recommendations make clear that we should get hold of a few concerns, [25]:
- adaption of the Mining Rules; new regulations should obligate an operator to perform a Safety Case, as described by the Cullen recommendations and to submit this to SodM.
- research to the implementation; like auditing of safety management systems, role of certifying authorities, emergency procedures for risers/pipelines, etc.
- specific studies to be made; for example to the efficiency of fire protection for risers, improvement of the sensitivity of emergency safety valves and additional reliable evacuation methods.
- pay extra attention to the execution of the supervision task; this involves testing of the paperwork safety sytem with reality, workpermits and shift handovers, isolation of mechanical and electrical systems, etc.

Their are decisions to be made which will have a significant and lasting impact on the offshore industry, [25]. An accident caused by the factors and failures as described in the Cullen Report is unacceptable and the carelessness of the operator and the shortcomings of the regulatory body are then directly to be blamed for it.
It followed from the Inquiry that one of the main events of the underlying causes of the Piper disaster was the fact that different kind of activities were going on, like drilling, production and maintenance, at the same time. [25], [26]. These, so called, concurrent or simultanious operations are carried out because of economic reasons. Cullen did not make any recommendations concerning with these concurrent operations. The Dutch Mining Law, however, obligates an operator to submit to SodM the plans for work to be carried out and the latter has the possibility to have the plans changed when the safety of persons is questionable. It is not allowed to carry out more than two concurrent activities at the same time.

The Dutch offshore Safety Case should link with the existing rules in the Netherlands. Specifically with, [6];
- the "Arbeids Veiligheidsrapport"(AVR): Ministry of Social Affairs
- the "Externe Veiligheidsrapport"(EVR): Ministry of VROM

and should link with international regulations 'Offshore Safety';
- Formal Safety Assessment (FSA): United Kingdom
- Concept Safety Evaluation (CSE): Norway

and;
- recommendations from the Cullen Report.

It is expected that, in the near future, operators will be obligated to submit to SodM a Safety Case in respect of each of its installations on the Dutch Continental Shelf, [6]. The Safety Case or FSA report should be hand in to SodM, in three-fold, 15 days before presentation of plans.
For a proposal of the contents of the FSA report, [6], see appendix C. The minimum quality of the Safety Case should be quarantied by ISO 9000-series.

6.4 'Auditing' SodM

In the beginning of 1991, the Safety Science Group from the Delft University of Technology was requested by SodM to carry out a study into the role and the inspection-method of SodM.
Primary goalsetting from this study was to contribute to the process of reorganisation and adaption of the role and working-method of SodM by looking with an external view to both SodM itself as well as her relations with the oil and gas industry, on- and offshore. The team, who carried out this study, will supply SodM with clearness and systematic handling in the process of policy-formulation and alteration.
Many companies, employees from SodM and other departments, and other organisations involved in the oil and gas industry have co-operated to interviews in the light of this study. The report of the study expected at the end of 1991, is currently in draft.

Lack of sufficient resources of suitable expertise and lack of manpower are the main problems SodM has to face. It is questioned if it is correct that SodM serves under the Ministry of Ecomic Affairs (EZ). Conflict situations occur, because of the fact that contradictionary interests have to be served, like economy on the one hand and safety on the other hand.

7. Inventory of accidents

7.1 Introduction

Safety of offshore structures is of considerable importance to employees, companies and authorities. Studies of recent accidents and application of accident statistics is mandatory in studies and practical work where the objective is to improve safety, or to identify the danger aspects.
The prime source of offshore accident statistics, among others (see section 4.4), is Veritec's World Offshore Accident Databank (WOAD), which covers the period 1970-1989, [28]. All accident information is gathered and recorded from all kinds of (public) data sources. It is believed that all 'total losses' are included, and that about 95% of all serious accidents are included, [29]. These are defined as those accidents (classified in types) leading to significant damage of structure/equipment, hydrocarbon spillage of 1000 tons or more or loss of several lives. A few areas of the world are excluded from this bi-annual survey where only limited information is available, among these are all countries with full state-owned offshore industry and insurance companies. Over 1700 offshore accidents are recorded and a further 4000 potentially hazardous incidents.

Every accident is in some way unique. Moreover, there is often a chain of consecutive events, each important but perhaps masking the all important initial event. The loss of the drilling rig Alexander L. Kielland in March 1980 is a very good example of this. Risk analists typically do not discuss the difficulties of classification and its subjective nature. Those who use such statistics without such detailed knowledge may easily be led to incorrect conclusions, [29]. WOAD recognises these difficulties and therefore presents two tables, one which counts the 'initial events', and an extended table with counts of all 'type of accidents' in a chain.

In relation to the next section, it is necessary to mention that most attention is given to fixed platforms on the North Sea.

7.2 Accidents

Worldwide
Worldwide, in the period 1980-89, the exposure of mobile platforms (5495 unit-years) was about 9 times smaller then for fixed platforms (48593 unit-years). The frequency (number of occurences per 1000 unit-years), of every event defined in table 7.1, is much higher for mobile then for fixed platforms. This latter also holds absolutely seen, except for the few events marked with a *. Especially the number of occurences for fire, explosion and spill/releases is much higher for fixed then for mobile platforms.
The frequency and number of accidents with structural damage of mobile platforms is much higher then for fixed platforms. This especially for total losses. See table 7.2 for frequencies. Most accidents with mobiles occur during drilling and tranfer operations (65% of total) and for fixed units during production operations (69%).
In the period 1980-89 the exposure of mobile units was about 1,8 times higher and 2,1 times higher for fixed units, compared with the period 1970-79. The total frequency of accidents with structural damage of mobiles decreased by a factor 1,4 and stayed about the same for fixed. However, the frequency of total losses of fixed units decreased by a factor 5,2!

Worldwide in the period 1970-89 there were 154 accidents in the offshore industry with fatalities (53% of that with mobiles and 34% with fixed) and 1150 lives were lost (mobiles 62% and fixed 31%). In the period 1980-89 there were 3,2 times more lives lost then in 1970-79.

North Sea
Exploration of oil and gas reservoirs in the North Sea started in 1957. The first drillings took place in 1961, and in 1966 the first fixed platforms were installed. The offshore industry has grown extensively since then. Most attention will be focussed on accidents in the period 1980-89.
The exposure of mobile and fixed platforms in the North Sea forms a small part of the worldwide exposure. In 1980-89, exposure in the North Sea was 823 unit-years for mobiles (15% of mobiles worldwide) and 1812 unit-years for fixed units (<4% of fixed units worldwide). The fleet of mobile platforms on the North Sea consists mainly of jack-up's (325 unit-years) and semi-submersibles (495 unit-years), together 99% of the unit-years. Compared with the period 1970-79, in 1980-89 the exposure of mobiles increased by a factor 2,1. For fixed, the exposure of 1980-84 increased by a factor 1,7 compared to 1975-79 and with a factor 1,8 in 1985-89 compared with 1980-84.
On the North Sea in the period 1980-89, the total frequency of accidents with structural damage for mobiles was a factor 2,1 higher then for fixed. For total losses a factor 9. See table 7.2. Most accidents with mobiles occured during drilling and transfer operations (62%) and for fixed during production operations (72%).
For the number of occurences of events (type of accident) vs. degree of structural damage for fixed platforms see table 7.3. The events, including initial events, in the 'chain' leading to total loss and/or severe damage are blow-out, collision, explosion, fire, spill/release and structural damage. When we take the frequency (no. of occurences per 1000 unit-years) into account and their severity of damage, most important events are fire, explosion and structural damage. Their frequencies are respectively 12,14; 7,73 and 7,73. Hydrocarbon spillage in the range of 1000 tons or more has the highest occurence, frequency 15,45. This led only once to a total loss (involving fatalities), and in most cases (71%) not to any structural damage, but to environmental pollution.

On the North Sea in the period 1970-89, 14 accidents with total losses occured, including 5 semi-submersibles, 2 jack-up's, 2 pipelines and a jacket.
In 1980-89, 15 accidents occured with fatalities, including 5 with fixed platforms and 8 with mobiles. Over 300 lives were lost. This latter was mainly due to two major accidents, namely the loss of the semi-submersible Alexander L. Kielland on 27 March 1980 (123 lives lost) and the Piper Alpha disaster on 6 July 1988 (167 lives lost).

7.3 Observations

Caution is necessary when interpreting information from databanks, [29]:
- The platform population is not homogeneous; the early Gulf of Mexico (GoM) structures, many of which are still operating, were designed to criteria considerably less severe than present ones. Also the environmental conditions in the North Sea are more severe than in the GoM. However, the total exposure in the North Sea is small (<5% of the worldwide exposure) compared with that in the GoM (68%).
- In manipulating small amounts of data extreme caution is required to avoid misleading conclusions.
- It is important when data are interpreted that exposure data associated with the

incidence of accidents and failures is given. Only then can the actuarial risks be evaluated. Since it is the annual risks which are most relevant in design and assessment, the most powerfull way to express exposure is in unit-years (or platform-years).

- Spills, for example, are recorded even if they don't cause any (structural) damage or fatalities. Some events, however, are not (always) recorded when they did not cause any damage, e.g. near collisions.
- Severe damage is much more likely to be repaired in fixed platforms then in mobile platforms, since the latter can be more easily removed from the location and replaced. Risk capital involved is usually smaller in mobile platforms. Need for continious recovery with minimum down-time implies that fixed platforms are more often repaired even when replacement might be cheaper. A good example of this latter was the very costly (jack-up) operation of Ekofisk.
- Most accidents involve a chain of events which is nearly always heavily influenced by human factors. The main reason why mobile platforms are much more prone to accidents than fixed platforms is due to human errors during operations such as ballasting, anchor and mooring system handling, and in tow.

7.4 Conclusions

Offshore accident statistics make clear that FSA studies should be carried out for both fixed and mobile structures. Some events require more attention during safety studies than others, because of their higher frequency of occurence and/or their severity of consequences. However, extreme caution is necessary when interpreting databank information to avoid misleading conclusions.

8. Retrospective view

8.1 Observations

There is an increasing (public) awarness of the hazards and safety implications in the offshore oil and gas industry associated with activities like exploration, production, and transport, handling, processing and storage of 'dangerous' hydrocarbons, [30]. Such awarness is directly related to the major accident potential of some of these activities and has resulted in the introduction of new legislation and safety requirements in many countries, over the past years. In consequence, all operations of offshore installations are faced with the numerous safety requirements and complex problems that demand skilled interpretations and safety policies. It is essential that safety levels are adequate and compliance with legislation enforced. This can be very expensive if major design changes or extra safety equipment are found to be necessary. Consequently, the effectiveness of various designs and the choice of operational, legislative and commercial options must be assessed at an early or concept design stage.
In the wake of the Piper disaster and the Inquiry that followed, the operator will be required (in the near future) to carry out an FSA and to submit to the regulatory body a Safety Case for each of its installations. FSA, involves risk and safety assessment and is advantageously applicable to the notifiable hazardous offshore installations. It can help justify the effectiveness of the safety management and enhance safety policies for the future. FSA provides a systematic approach to risk analysis. It identifies and gives a better insight in the potential hazards of the installation and the way to prevent them before they become an accident.

8.2 Benefits of FSA

Operators, developers, national administrations, civic authorities and the general public are assured that through FSA studies several possible benefits can be gained. These include, [30]:

- safety policies are developed in a logical and structured way.
- management policies and procedures are consistent with current and long-term perspectives of corporate risk and safety profiles.
- environmental and occupational risks and overall safety implications have been critically assessed.
- qualitative and quantitative safety evaluations demonstrate the adequacy of primary safety measures to prevent major accidents or limit their consequences.
- emergency plans are prepared and justified from quantitative results.
- plans for new facilities are assessed and optimised for safety and commercial implications.
- assessing the operation tolerance to human error.
- assessing the relative costs in achieving particular levels of safety; can be used in design optimisation and help to meet safety and operational requirements in a cost-effective way (i.e. Cost Benefit Analysis).
- identifying areas where more official guidance is required.
- compliance with existing and impending safety legislation is demonstrated.
- recommendations in excess of those required by regulatory authorities.
- continuing safety; design levels of reliability and operational safety must be maintained throughout the life-cycle of the project to ensure continued safety and

economic operation.

8.3 Concluding remarks

This report dealt with the various aspects of Formal Safety Assessment. Safety offshore can be improved through FSA studies. The Safety Case should 'guarantee' the safety of an offshore installation. Safety is crucially dependent on management and the Safety Case should therefore demonstrate that the company has a suitable SMS. The QRA as part of FSA provides a structured objective and quantitative approach to risks. It gives a better understanding of the hazards and the measures needed to control them. However, further studies are necessary to improve certain techniques, e.g. human factor analysis. Registration of incidents should also become more adequate.
FSA should apply to both mobile and fixed installations, both new and existing. The Safety Case should be a living process during an installation's life-cycle. So, it should be kept up-to-date. The preparation of Safety Cases is a formidable task and lack of sufficient resources of suitable expertise is widespread throughout the offshore industry, i.e. operators, regulatory bodies, certifying authorities, and so on. Implementing Cullen's recommendations, and especially the ones concerned with Safety Cases, can and should not be done hasty given the nature of the change involved.

The future will show us if the offshore industry succeeds in improved safety offshore. Formal Safety Assessment is a tool to achieve that goal.

References

[1] The Hon Lord Cullen, "The Public Inquiry into the Piper Alpha Disaster", Department of Energy, UK, November 1990

[2] IRO-Journal 13, "Cullen Report well received", The Netherlands, December 1990.

[3] Report of Committee V.2, "Inspection, Monitoring, Maintenance/Repair", Proceedings of the 11th International Ship and Offshore Structures Congress, Wuxi (China), 16-20 September 1991

[4] Broadribb, M.P., "The application of formal safety assessment to a new installation", A three Workshop on 'Risk analysis in the offshore industry II' organized by IBC Technical Services Ltd, Aberdeen, 25 March 1991

[5] Ramsay, C.G., "Techniques for fire risk management", A three day Workshop on 'Risk analysis in the offshore industry II' organized by IBC Technical services Ltd, Aberdeen, 25 March 1991

[6] Document no: 1732-RP-001, "Voorstel regelvorming veiligheidsrapport mijnbouw installaties t.b.v SodM" by FSA-group (Stork Protech/TNO), Schiedam, April 1991

[7] Cox, R.A., "Risk analysis of offshore installations - a decade of experience, and prospects for the future", A three day Workshop on 'Risk analysis in the offshore industry II' organized by IBC Technical Services Ltd, Aberdeen, 25 March 1991

[8] Carmichael, I.D., "Quality and Safety Management", Studiedag 'Milieu en veiligheid in de offshore industrie' organized by Studiecentrum voor bedrijf en veiligheid, Amsterdam, 29 May 1991

[9] Ockeloen, G.,"Het stimuleren van zelfzorg", Studiedag 'Milieu en veiligheid in de offshore industrie' organized by Studiecentrum voor bedrijf en veiligheid, Amsterdam, 29 May 1991

[10] Offshore Visie 6, "Veiligheid kan niet alleen door dikke handboeken worden opgelegd", OV 6e jaargang, The Netherlands, August 1989

[11] Top, W.N., "Veiligheidsdoorlichting als tool of management", Studiedag 'Veiligheidsmanagement' organized by Studiecentrum voor bedrijf en overheid, Amsterdam, 13 Oktober 1987

[12] Dols, H.J., "Veiligheid als integraal deel van de bedrijfsvoering", Studiedag 'Veiligheidsmanagement' organized by Studiecentrum voor bedrijf en overheid, Amsterdam, 13 Oktober 1987

[13] Fleishman, A.B., "Risk criteria and the role of Cost Benefit Analysis", A three day Workshop on 'Risk analysis in the offshore industry II' organized by IBC Technical Services Ltd, Aberdeen, 27 March 1991

[14] Whalley, S.P., "The use of human reliability in risk analysis studies", A three day Workshop 'Risk analysis in the offshore industry II' organized by IBC Technical Services Ltd, Aberdeen, 27 March 1991

[15] Vrouwenvelder A., Ligteringen, H., Moan,T., "Reliability analysis for offshore structures", ECOR Document, UK, May 1991

[16] Brascamp, M.H. and Gansevoort, J., "Storingsanalyse", PT Procestechniek number 5, The Netherlands, May 1989

[17] Morgan, J.M., "The correct choice of incident, equipment and failure & human error data and their application to offshore risk analysis", A three day Workshop on 'Risk analysis in the offshore industry II' organized by IBC Technical Services Ltd, Aberdeen, 26 March 1991

[18] Hudson, T.P.W., "Management and safe behaviour: can we prevent human error?", Studiedag 'Veiligheidsmanagement' organized by Studiecentrum voor bedrijf en overheid, Amsterdam, 13 Oktober 1987

[19] Weerheym, R., "Verantwoordelijkheid en aansprakelijkheid", Studiedag 'Milieu en veiligheid in de offshore industrie' organized by Studiecentrum voor bedrijf en veiligheid, Amsterdam, 29 May 1991

[20] Offshore Engineer, "Manpower and money issues confront safety regulator", UK, January 1991

[21] Offshore Engineer, "Cullen revisited 1 - Safety in the spotlight at post Cullen conference" and "Cullen revisited 2 - Rethinking subsea valve design and procurement", UK, March 1991

[22] Offshore Engineer, "Extra cash for a new home for UK safety", UK, April 1991

[23] Offshore Engineer, "HSE and DEn told to get moving on safety", UK, September 1991

[24] Offshore Engineer, "HSE lays down timetable for offshore safety", UK, October 1991

[25] Ockeloen, G., "Letter to the Dutch offshore industry", SodM -Ministry of Economic Affairs (EZ), The Netherlands, 30 November 1990

[26] NRC-Economie, "Offshore houdt ongevallen graag onder de oppervlakte", The Netherlands, 12 September 1991

[27] Hale, A.R., Heimplaetzer, P., Gerlings, P.O., Swuste, P., "Assessing and improving Safety Management Systems", First International Conference on Health, Safety and & Environment in oil and gas exploration and production, The Hague, 12 November 1991.

[28] WOAD, "World Offshore Accident Databank - Statistical Report 1990", Veritec, published by Veritas Offshore Technology and Services A.S., Hovik (Norway), 1990

[29] Report of Committee V.3, "Service experience offshore", Proceedings of the 11th International Ship and Offshore Structures Congress, Wuxi (China), 16-20 September 1991

[30] Lloyd's Register of Shipping, "Safety Technology", information leaflet of Lloyd's Register Safety Technology Department, UK, 1990

[31] SIPM, EPO/633, "Quantitative Risk Assessment", Report EP-55000-18, The Hague, May 1990

Appendices

A. Figures

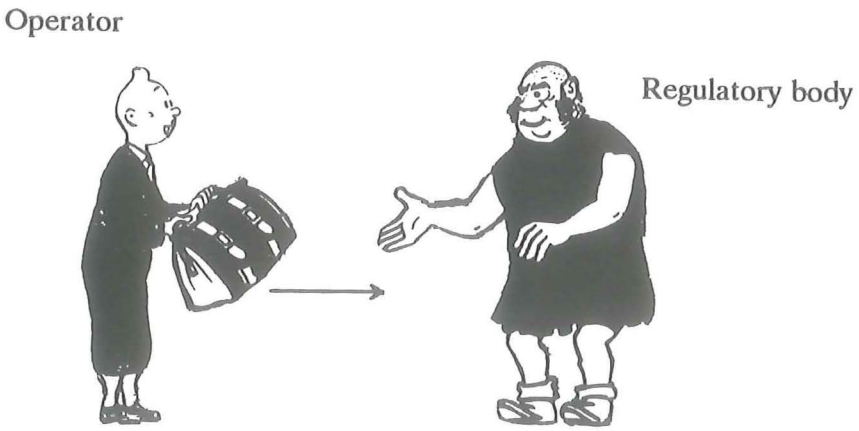

figure 2.1 Submission of a Safety Case

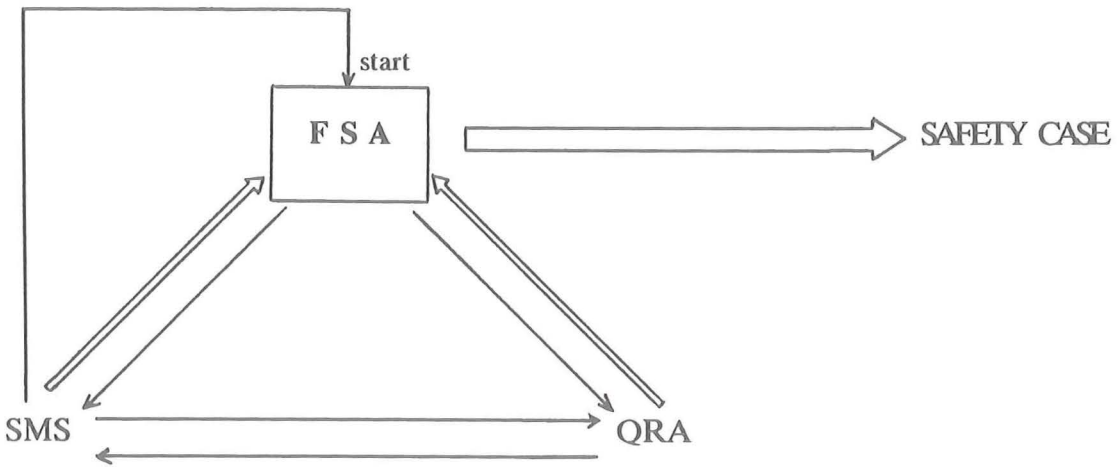

figure 2.2 Formal Safety Assessment (FSA)

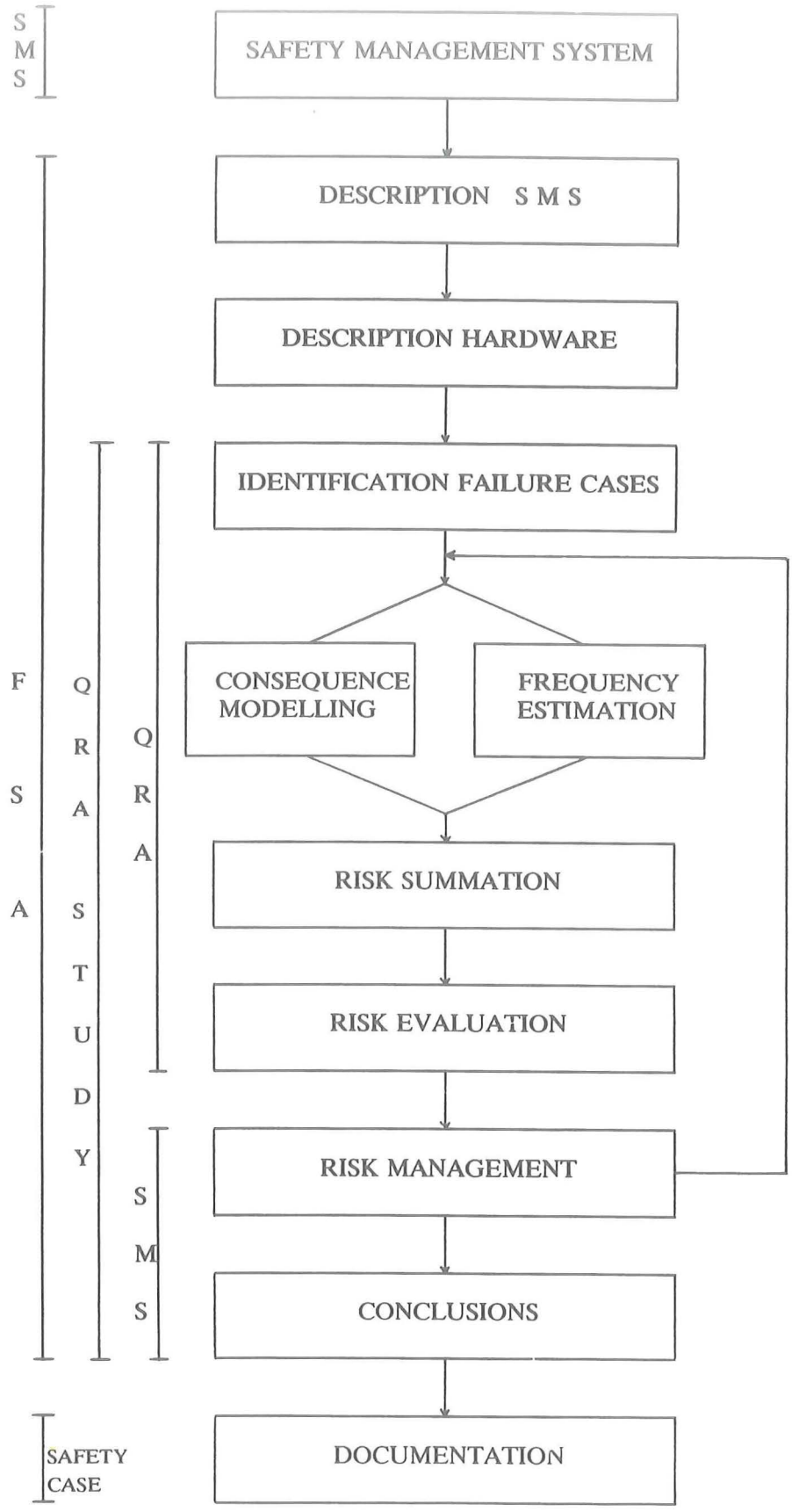

figure 2.3 FSA structure

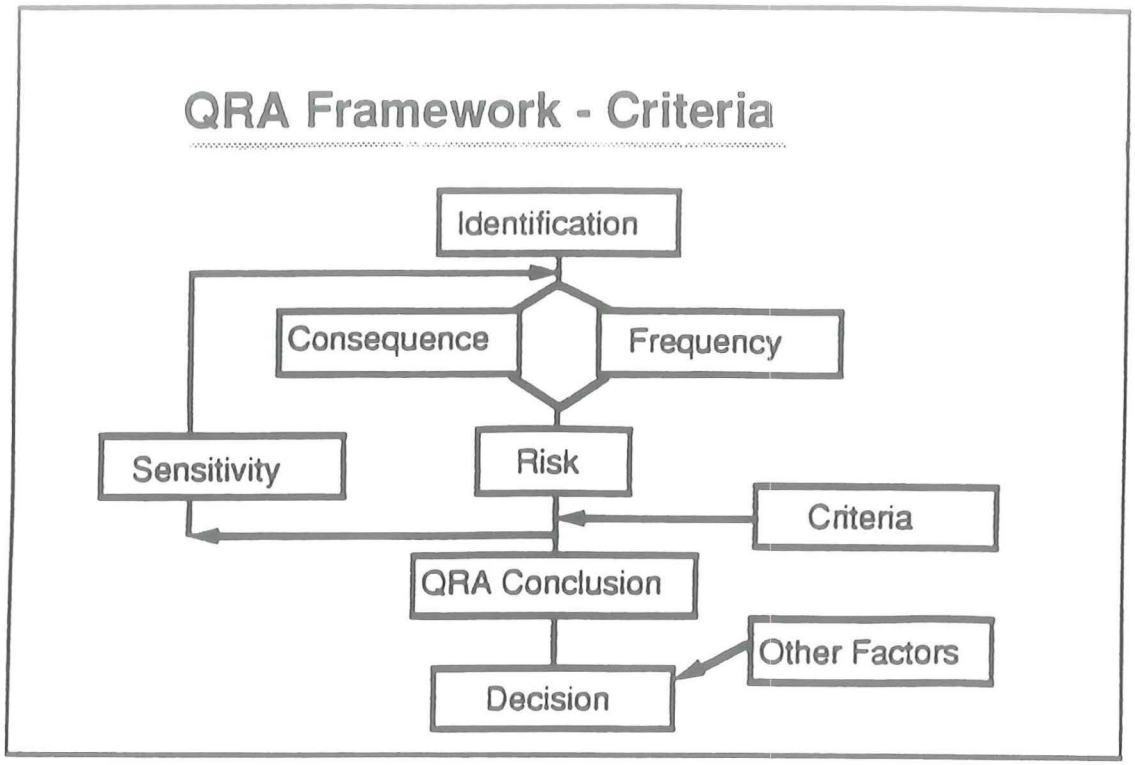

figure 3.1 QRA framework-criteria, [13]

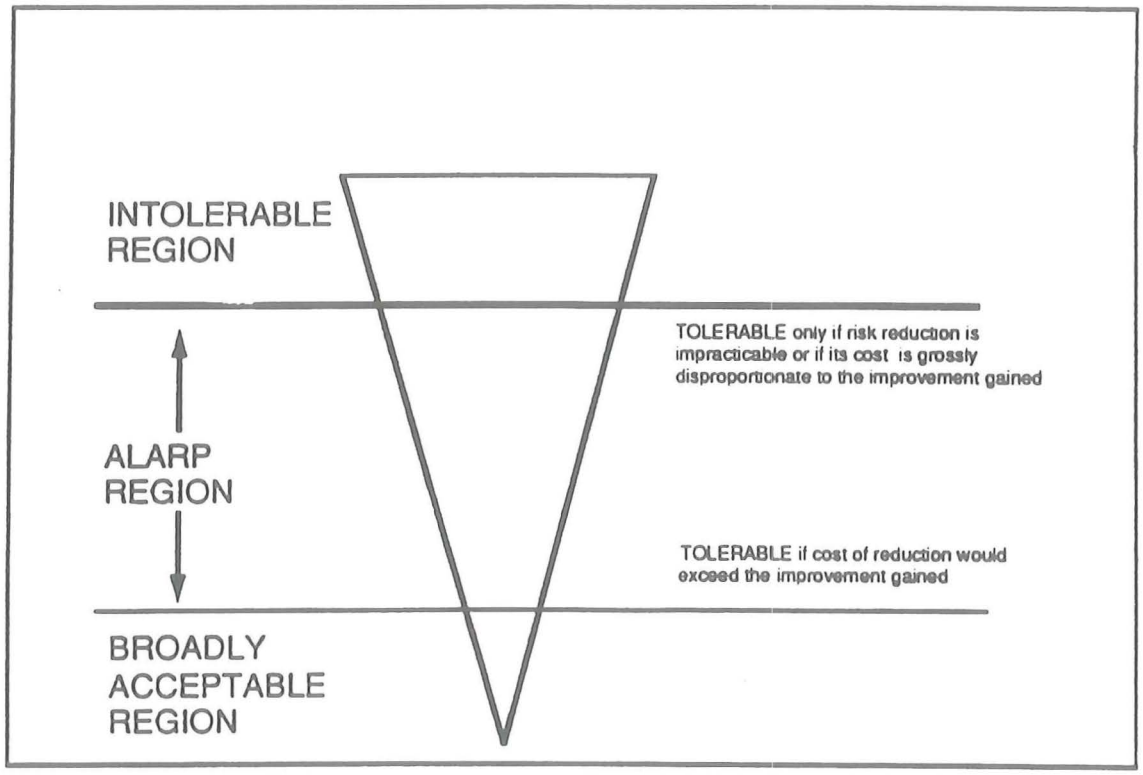

figure 3.2 Three-band framework of acceptability criteria, [1], [13]

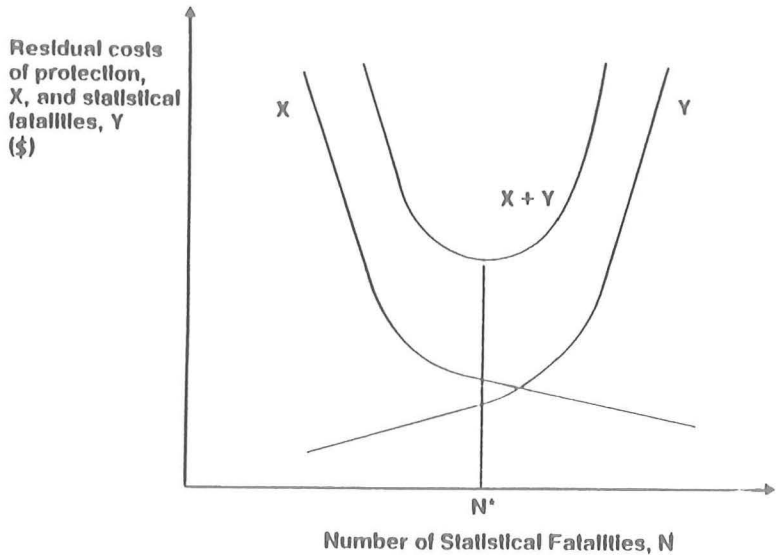

figure 3.3 Analytical framework for optimisation of protection, [13]

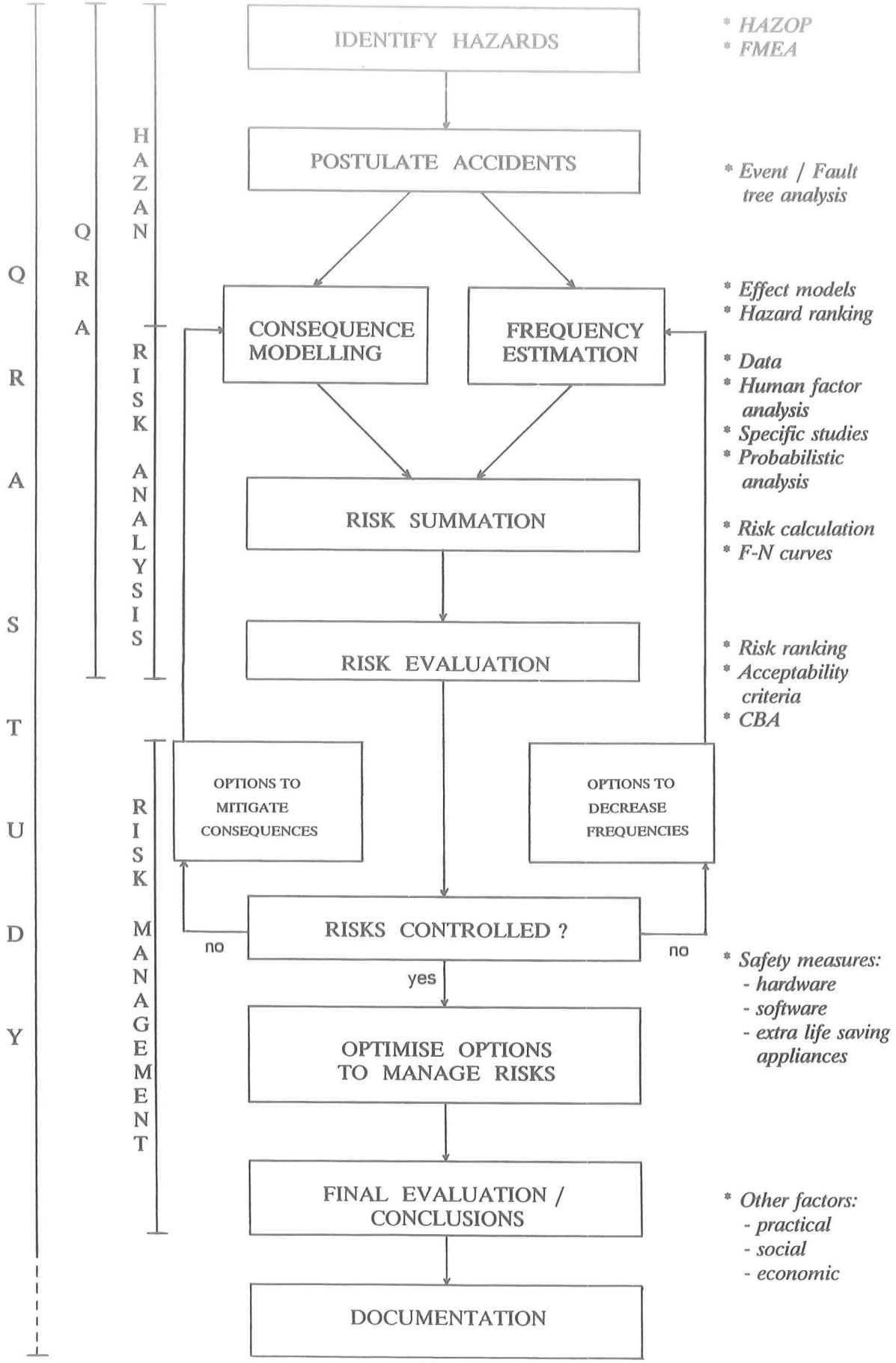

figure 4.1 QRA-study structure

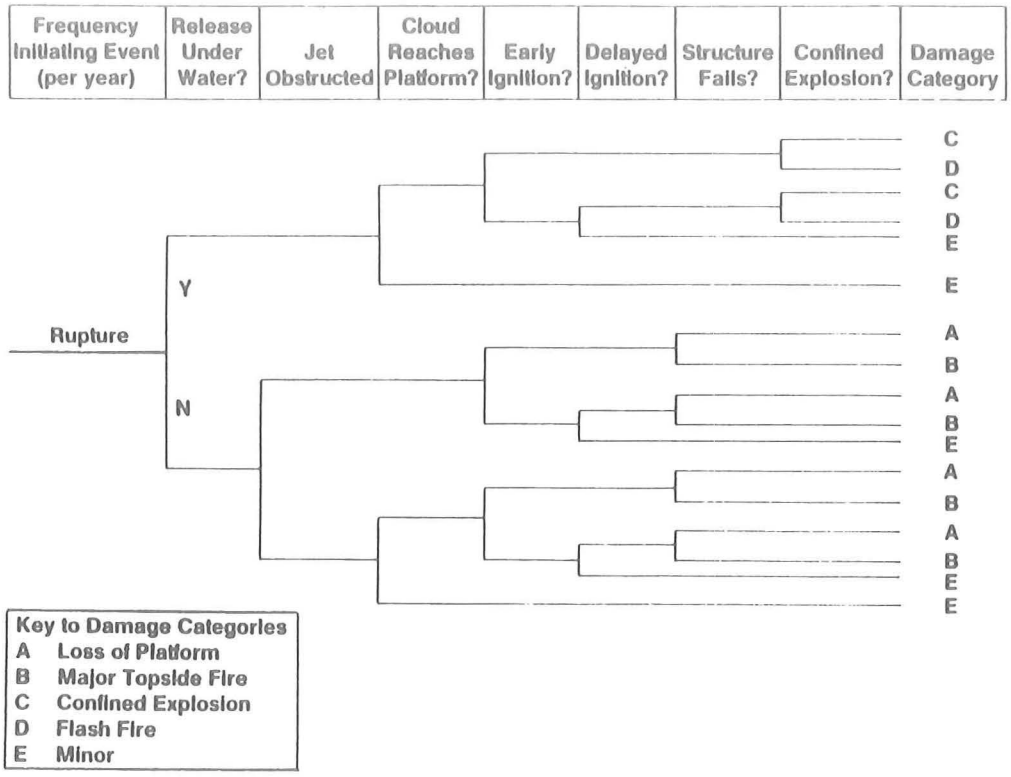

figure 4.2 Event tree, gas riser rupture

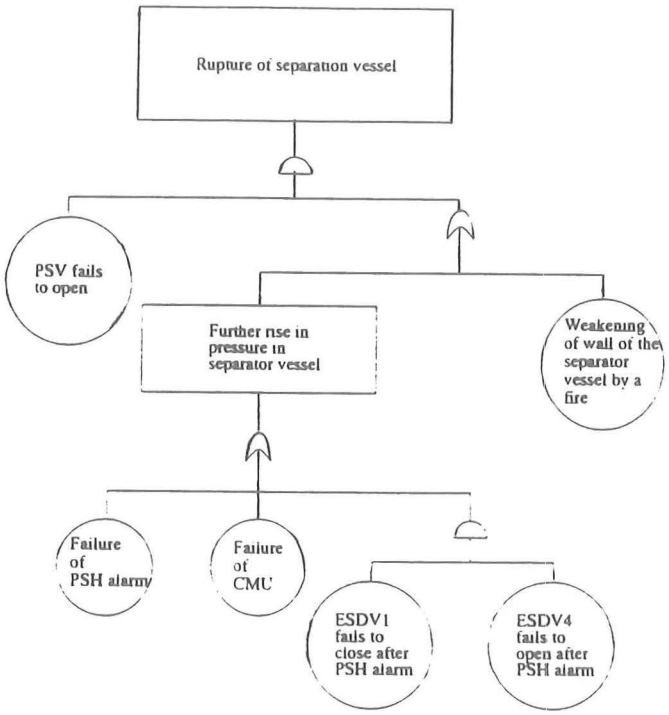

figure 4.3 Fault tree, rupture of separation vessel

B. Tables

All tables are adopted from [28].

EVENTS	TYPE	
	Mobiles	Fixed
Anchor failure	6.55	0.08
Blowout	12.38	0.93
Well problem	2.37	0.25
Capsize	9.65	0.06
Collision	5.64	0.54
Contact	8.01	0.49
Crane accident*	3.09	0.43
Explosion*	2.37	0.93
Falling load*	4.00	0.47
Fire*	10.56	2.80
Foundering	6.37	0.08
Grounding	3.82	-
Helicopter acc.	1.09	0.08
Leakage	3.09	0.06
List	7.10	0.08
Machinery fail.	2.37	0.12
Off position	12.38	0.10
Spill/release*	2.73	1.65
Struct damage	9.65	0.49
Towing accident	7.10	-
Other accident	10.37	0.45
Unit years	5495	48593

Table 7.1 Type of accident (EVENTS) vs. type of unit (TYPE) No. of occurrences per 1000 unit-years, MOBILE and FIXED units WORLDWIDE, 1980-89

DAMAGE	TYPE		Mobiles	Fixed
	Mobiles	Fixed	North Sea	North Sea
To.los	9.65	0.14	4.9	0.55
Severe	10.01	0.66	8.5	2.76
Signif	20.02	1.13	25.5	9.93
Minor	15.29	1.48	20.7	13.80
No dam	22.20	3.21	53.5	25.39
Unkn.	1.27	0.19	-	0.55
Total	78.44	6.82	113.0	52.98
Unit years	5495	48593	823	1812

Table 7.2 Degree of structural damage (DAMAGE) vs. type of unit (TYPE). No. of accidents per 1000 unit-years, MOBILE and FIXED units WORLDWIDE, 1980-89.

	DAMAGE						
EVENTS	To.los	Severe	Signif	Minor	No dam	Unkn	Total
Anchor failure	-	-	1	-	-	-	1
Blowout	1	1	-	-	2	-	4
Well problem	-	-	1	4	3	-	8
Collision	-	1	1	-	-	-	2
Contact	-	-	1	4	2	-	7
Crane accident	-	-	3	7	2	-	12
Explosion	1	2	5	4	2	-	14
Falling load	-	-	3	8	4	-	15
Fire	1	2	6	4	8	1	22
Helicopter inc	-	-	-	-	1	-	1
Leakage	-	-	-	1	2	-	3
List	-	-	2	-	-	-	2
Machinery fail	-	-	3	-	1	-	4
Spill/release	1	-	3	4	20	-	28
Struct damage	-	2	4	4	4	-	14
Other incident	-	-	-	2	5	-	7

Table 7.3 Type of accident (EVENTS) vs. degree of structural damage (DAMAGE). No. of occurrences, FIXED units in the NORTH SEA, 1980-89.

Definitions:

Type of unit

i) Mobile units:

Code	Explanation
JU	Jackup
SS	Semi-submersible
SU	Submersible
DS	Drill ship
DB	Drill barge

ii) Fixed units:

Code	Explanation
AI	Artificial island
CO	Concrete structure
JT	Jacket
TL	Tension leg platform

Degree of structural damage

Structural damage is classified according to the severity and extent of damage to structural supports and topside equipment. The classification is explained below:

Code	Shorttext	Explanation
TO	To. los	Total loss of the unit (includes constructive total losses from an insurance point of view. The platform may be repaired and put into operation again).
SE	Severe	Serious damage to several modules of the unit. Mobiles: Damage can hardly be repaired on site. Cost of damage above 2 mill. USD.
DA	Signif	Serious damage to module, local area of unit, or minor structural damage to unit. Cost of damage in range 0.9 - 2 mill. USD.
MI	Minor	Damage to major equipment. Cost of damage in range 0.1 - 0.8 mill. USD.
NO	No-dam	No or insignificant damage. Cost of damage less than 0.1 mill. USD.
	Unkn	Unknown

Type of accidental event

Shorttext	Explanation
Anchor failure	Problems with anchor or mooring device.
Blowout	An uncontrolled flow of gas, oil or other fluids from the reservoir.
Well problem	Accidental problem with the well (routine kicks not included).
Capsize	Loss of stability resulting in overturn of unit.
Collision	Accidental contact between two offshore units where at least one of the units are propelled. Except for incidents defined under "Contact" below.
Contact	a) Embarking or manoeuver operations with accidental contacts except grounding.
	b) Structure which drifts onto other unit.
Crane accident	Any event caused by or involving cranes or derrick draw-works.
Explosion	Explosion.
Falling load	Falling load/dropped objects.
Fire	Fire lasting more than 9 minutes or causing damage, or occuring together with other accident type.
Foundering	Loss of buoyancy of the unit.
Grounding	Contact of floating unit with sea bottom.
Helicopter acc.	Accident with helicopter either on or nearby a platform.
Leakage	Leakage of water into the unit causing loss of buoyancy.
Spill/Release	Release of fluid or gas to the surroundings causing potential pollution. To be recorded the spill must be minimum 1 m^3 oil equivalents or the spill is recorded together with accident type.
List	Uncontrolled inclination of unit.
Machinery malf	Propulsion - or pumping machinery failure.
Off position	Unit out of its expected position or drifting out of control.
Struct. damage	Breakage or fatigue failures (mostly failures caused by weather) of structural support.
Towing incident	Towline failure.
Other incident	Event other than specified above.

C. Proposed list of contents of FSA report

1.0 Introduction

2.0 Corporate Safety Management System
2.1 Company Safety Policy and Objectives
2.2 Organisation and Responsibilities
2.3 Standards and Codes
2.4 Monitoring and Auditing

3.0 Description of the installation
3.1 General Description
3.2 Design Basis and Data
3.3 Detailed Description
3.4 Safety Aspects
3.5 Procedures
3.6 Drawing and Document Index

4.0 Management of the installation
4.1 Installation Safety Policy and Objectives
4.2 Organisation and Responsibilities
4.3 Monitoring and Auditing

5.0 Hazard identification
5.1 Hazop
5.2 Design Accidental Events (DAE's)
5.3 Incident/Accident Record

6.0 Quantitative Risk Assessment
6.1 Fire Safety Analysis
6.2 Risk Analysis of DAE's
6.3 Incident/Accident follow-up
6.4 Recommendations

7.0 Future developments
7.1 Remedial Actions
7.2 Planned Modifications
7.3 Hazard Identification Studies
7.4 Hazard Assessment Studies
7.5 Installation Abandonment/Removal

Attachments
Drawings and Documents

The minimum quality of the report will be guaranteed by the standard codes NEN ISO 9000 till 9004.

For a more detailed list of contents and guidelines when carrying out out an FSA, see [6].