CONCLUSIONS

The basic objectives, principles and approach to safety case formulation are the same whether an installation is onshore or offshore, and this is likely to be reflected in forthcoming legislation.

However, the complexity, compactness, relative isolation and an historically different safety culture of offshore installations may mean that a more thorough analysis of potential hazards and escalation paths is needed, and this will require both better data in terms of release frequencies, source terms and near-field consequence analysis and improved methods or understanding to allow the hazards to be analysed in an efficient manner. The benefits of this analysis will be a better understanding of safety and how to achieve practicable safety improvements.

The Cullen Report and subsequent offshore safety legislation is likely to set a new and higher standard than any before it. The Cullen Report embodies the widely publicised principles of managing safety but extracts the key factors in such a lucid manner that it provides a reference that should be read by all with a safety responsibility.

The implementation of the Cullen Report recommendations should take the UK offshore industry to an improved safety regime and provide a basis for reviewing and improving safety in offshore activities in the UK and elsewhere in the world.

REFERENCES

(1) HSE, 1990 A Guide to the Control of Industrial Major Accident Hazards Regulations 1984, HMSO, ISBN 9-11-885579-4.

(2) Lord Cullen, 1990 The Public Inquiry into the Piper Alpha Disaster (Two Volumes) HMSO, ISBN 010-113-102

(3) HSC, 1992 Consultative Document 'Draft Offshore Installations (Safety Case) Regulations 199-'

ONE COMPANY'S EXPERIENCE OF FORMAL SAFETY ASSESSMENT & PREPARATION OF OFFSHORE SAFETY CASES

M.J. Wendes

Cullen Team, BP Exploration, UK Operations, Aberdeen

The retrospective and simultaneous assessment of 28 installations in a short timeframe and with an industry wide shortage of expert resources is an immense challenge. The momentum was established by a pilot study then a centralised team followed by transfer to the individual installation groups. In the "forthwith" studies the analytical emphasis was placed on engineering judgement supported by proven and readily available consequence modelling. This was followed, where appropriate, by more sophisticated modelling and risk assessment. The information becoming available is enormous but the true value of the work done to date is now being realised as it provides input to assessing the need for remedial measures and making difficult and complex decisions.

Keywords: Formal Safety Assessment (FSA) Offshore Safety Case, Quantified Risk Assessment (QRA)

INTRODUCTION

BP Exploration currently operates a total of 24 hydrocarbon producing installations, a water reinjection platform and a semi-submersible emergency support vessel in the United Kingdom Continental Shelf. They range from large oil platforms, with 200 personnel onboard, to small not normally manned gas platforms.

Two further installations are under construction with several other developments at various stages of design.

For a number of years it has been appreciated within BP that reliance purely on good engineering practice, the application of approved standards and the certification and inspection regimes could not of themselves comprehensively identify and control the hazards and sequences of events that could lead to a major accident.

The benefits of techniques and tools to help systematically identify hazards, analyse consequences and assess risks have been readily appreciated and a significant investment has been made in recent years to increase our capability in this area.

An important application of this new technology has been in new developments, forming part of a more general initiative to ensure safety engineering input is fed into new developments from the very earliest stages. To achieve this effectively, it was recognised that the implementation of a fairly formal and systematic plan was appropriate.

Hence for those installations under construction or development, safety engineering, using the best analytical tools available, has been an inherent part of the design. Safety Case preparation has therefore consisted of pulling together studies that were an integral part of the design process. In organisational terms the Safety Case simply became part of the project deliverables.

BP has been strongly supportive of the concept of pulling together all the relevant engineering and management information in a formalised manner to demonstrate the safety of the design and operation of both onshore and offshore facilities.

The preparation of a Safety Case, therefore, is a natural development of a process which in any event was becoming company practice. The main challenge has been to retrospectively and simultaneously prepare Safety Cases for all the existing installations, in a relatively short timeframe and with an industry wide shortage of experienced expert resources. Some of the experiences gained and lessons learned as we have endeavoured to rise to this challenge are presented in this paper.

There are two main thrusts in the Safety Case; the "Safety Management System" and a demonstration that the potential major hazards of the installation have been identified and appropriate controls provided which includes the provision of an adequate Temporary Safe Refuge and Evacuation, Escape and Rescue facilities.

This paper concentrates on the latter due to the background and involvement of the author.

A large number of other experiences and lessons have been learned in the review and presentation of the Management of Safety. These are worthy of discussion in their own right. The exclusion of this topic in this paper must in no way be taken as a reflection of the importance of this issue or the effort BP has put in to address it.

Another very important facet of the process of Formal Safety Assessment is the involvement of the whole workforce. A separate paper addressing this issue has recently been given by an Assistant General Manager of BP Exploration (1).

One final point to note is that a fairer title for this paper would be "One Person's View of One Operating Company's.....". The person in this case is someone who has for the last eighteen months been working at the coal face; involved in the nitty gritty of applying the process of Formal Safety Assessment to a number of existing installations.

This is hopefully a valid viewpoint, and one that is of interest, though it must be emphasised that it cannot represent in totality the Company position. Indeed as we are presently right in the middle of the whole process it is not possible to present a consensus opinion.

FACTORS INFLUENCING THE FSA PROCESS

Regulatory Requirement

The preparation of the Safety Case is mainly, but not purely, for internal use but also to fulfil a forthcoming regulatory requirement. Paragraph 17.35 of the Cullen Report (2) states "Primarily the Safety Case is a matter of ensuring that every company produces an FSA to assure itself that its operations are safe and gains the benefits of the FSA already described. Only secondarily is it a matter of demonstrating this to the regulatory body. That said, such a demonstration both meets a legitimate expectation of the workforce and the public and provides a sound basis for regulatory control."

This prioritisaton has been difficult to keep. It quickly became apparent that the regulatory position would influence the approach and methodology that should be adopted. During ongoing dialogue, both directly and via UKOOA, a picture of their developing position was pieced together. This picture was clarified in the Consultative Document (3). Hence there has throughout the process been a sense of not only needing to tackle the task in what was internally considered to be the best way possible but also of having to comply with predicted future regulatory requirements which whilst being fairly high level and goal setting, would tend by their nature to influence the details of what is required.

Time Frame

In addition to influencing the content and approach taken in the Safety Case, the other important influence from the regulator is over the time frame within which the work has to be completed. A brief list of past and future milestones is as follows:

- Piper Alpha Disaster, July 1988
- SI 1029 Emergency Pipe-line Valve, December 1990
  (review of benefits of Subsea Isolation Valves)
- Cullen Report, November 1990
- Completion of Forthwith EER Study, December 1991
- Consultative Document, February 1992
- Regulations, Autumn 1992
- Safety Case Final Submission, November 1993
- Safety Case accepted, November 1995

Given the scale of the task this is a relatively tight timescale and does dictate along with the other factors mentioned here the approach that has to be taken.

One point to note is that one of the most difficult dates to meet will be that established as a target for completing remedial measures. Working back from that date it is clear that a programme of proposed remedial works will need to be available by the time the Safety Case is submitted which requires an even earlier commitment to invest funds in the proposed measures.

Resource Limitations

Resource limitations have been a very real influencing factor in the approach taken. Both inhouse and externally the capability and capacity of expert resources in this area is limited. Making maximum use of available resources has been a key objective.

Internal Structure

Within BP the individual assets (an asset consists of either a single platform or a small group of interlinked platforms) have a large degree of autonomy to run their business. Establishing a central team to manage the execution of the work and then effectively hand over a completed Safety Case runs contrary to this management philosophy.

This approach would also run contrary to the underlying philosophy of Formal Safety Assessment where the objective is for the operators of an installation to "own" the Safety Case and to use the whole process to help manage safety more effectively.

ORGANISATION OF FSA WORK

A number of recommendations in the Cullen Report led to the need for operators to make an immediate response, not least of which were the recommendations requiring the four "forthwith" safety studies.

Whilst acknowledging the principle of asset autonomy, it was readily apparent that to expedite an efficient and consistent response to these recommendations a central, Cullen, team would have to be established to develop some initial momentum. This team addressed all the Cullen recommendations and prepared methodologies for the "forthwith" studies.

Meanwhile the assets appointed FSA coordinators. These coordinators then employed a variety of inhouse and external engineers to carry out the "Emergency Systems Review" (ESR) and "Smoke and Gas Ingress" (SGI) studies. The "Fire Risk Analysis" (FRA) and "Evacuation, Escape and Rescue" (EER) studies were controlled by the Cullen Team on behalf of the assets due to the expert skills required of which there was an acute shortage.

It was identified that there would be benefits in fast tracking one existing installation (Forties Charlie) to produce a pilot case. This was done and has proved to be a useful exercise.

The Cullen Team became the natural focal point for internal discussions and consultation with the HSE both directly and via BP's membership of UKOOA.

As the "forthwith" studies progressed it became apparent that there would be the need for some further safety studies. The Consultative Document (3) also pointed towards a requirement to do significantly more quantified risk assessment (QRA) than had been envisaged. These factors coupled with the need to commence preparation of the Safety Case document itself led to the assets strengthening their internal teams and a transfer of responsibility for the ongoing work. The Cullen Team is now taking on a support and advisory role, and is helping the assets as far as possible to achieve a consistent approach.

One very positive aspect of the FSA process has been the diversity of involvement throughout the company, and the increased general awareness of major hazard issues. To ensure harmony of approach has required considerable communications effort.

During 1991 the numbers involved full time in the Cullen Team peaked at around 30 with around 10 additional people working fulltime in the assets on Safety Case work. The Cullen Team now has 4 full time members with upward of 20 people working full time in the assets, with large numbers of other people working part time, supported by numerous external consultants. In 1990/1991 the cost of the FSA work was several million pounds and this will no doubt be exceeded this year and in the forthcoming years.

CULLEN REPORT

"Forthwith Studies"

Responding to the Cullen Report (2) was relatively straight forward. The debate had all taken place at the public inquiry and hence the task was to absorb the contents and recommendations and to develop an appropriate response.

Amongst the many recommendations the four "forthwith" studies required priority attention. Methodologies were pieced together using the relevant paragraphs in the report keeping in mind the limited resources available and the short time frame established for the EER. In general the statements in the Cullen Report were pitched at a sufficiently high level that whilst they provided an overall framework there was still a fair amount of flexibility in interpreting the requirements and developing the details of the methodologies.

A brief outline of the approach adopted in each "forthwith" study is given in Figure 1.

Overall the approach adopted can be best described as a series of systematic qualitative analyses with the primary objective of identifying any critical weaknesses. The analytical emphasis was placed on engineering judgement supported by consequence analysis.

Logically the FRA should have preceded the other three studies with the EER being last. This approach could not be followed due to the requirement to complete the EER studies within approximately one year. Allowing for the time to establish the organisation and prepare a methodology this in affect meant completing EER studies for 25 installations in around eight months. This is not far off producing one a week. It would have been impossible to meet this deadline if the other studies, particularly the FRA, had had to be substantially complete to input into the EER study.

For the ESR it was concluded that it would be practical to conduct the study in two phases, he second phase incorporating results form the FRA. As the FRA did not model smoke or gas movements to any great extent it was concluded that the SGI was best conducted as a stand-alone exercise.

Resolution of Safety Case Findings

Recognising that the "forthwith" studies would form part of the foundation of the Safety Case, a framework for building on this foundation was established. This is illustrated in Figure 2.

Identified safety concerns may require further analysis to confirm the nature of the problem, though this need only be carried out to the extent that is required to resolve the concern satisfactorily. This requires iteration.

The key principles of this approach were:

- selective detailed analysis to verify/understand hazards
- analytical emphasis on engineering judgement, consequence analysis and risk analysis in descending order
- knowledge of all hazards before considering remedial measures
- consideration of procedural measures before engineering modification
- preference for hazard prevention before control or mitigation
- use of cost benefit analysis to resolve competing remedial options

The intention was that QRA would be used where it was appropriate to help resolve issues that could not be satisfactorily addressed using engineering judgement or consequence analysis. In the first instance it would be used in a relative manner to compare competing options for risk reduction and then in hopefully rare situations have to be used to help judge the tolerability of particular situations.

Detailed Consequence Analysis

In practice one of the main areas for further detailed analysis has been topside fire and explosion scenarios. A key feature of this further analysis has been on understanding in detail the effects of the predicted heat and blast loads on the primary and secondary structure, and decks and walls. To ensure a balanced approach this has also meant that state of the art consequence models have also been used to assess the fire and blast loads. This level of analysis is an order of magnitude more complex than used in the "forthwith" studies and an order of magnitude more costly.

There are other areas where at present we have not felt confident enough in the available technology to tackle them in a rigourous quantitative manner:

- smoke and gas movement and ingress into the TSR
- other ways of losing life support in the TSR, for example excessive temperature rise
- loss of command support
- human factors

These are clearly important areas and it is accepted that part of the "living" FSA concept is that as proven technology becomes available that it should be applied.

In general there is a very real danger of information overload. All of the more detailed analyses tend to produce vast amounts of information and not give totally black and white answers. There is nearly always a large number of factors that can affect the final results, and it is not always practicable to run comprehensive sensitivity analyses in every case.

Assessing all the information produced to determine the need for an appropriate programme of remedial measures and to summarise it in a suitably short Safety Case document are both proving to be very complex and difficult tasks.

It is vital that a broad overview is maintained and that imbalances do not start to occur in the amount of effort put into looking at particular hazardous scenario on an installation to the detriment perhaps of other scenarios.

CONSULTATIVE DOCUMENT

In places the guidance in the Consultative Document (3) is of a fairly detailed and specific nature leaving fairly limited room for interpretation. On the other hand it is not detailed enough that it can be followed in a systematic way.

Trying to conform to the guidance for such a wide variety of different types of installation is proving problematic.

Two areas in particular are giving rise to concern: the requirement for extensive use of QRA and the emphasis on the TSR.

Quantified Risk Assessment

Part of the guidance addresses in a general way the use of risk assessment. This section gives good, clear, well balanced guidance on the use of QRA within the Safety Case to help achieve as low as reasonably practicable safety levels. Good engineering and understanding the limitations of QRA are both emphasised.

This guidance fitted in well with the internal approach being developed for resolution of Safety Case findings.

The guidance then takes on a much more detailed nature, culminating in the requirement to meet specific standards and criteria. To achieve this there is very little option other than to carry out a full QRA.

The approach required to carry out a full QRA has to be a lot more rigourous and systematic than adopted for the "forthwith" studies. To carry out the vast number of calculations, requires a more mechanistic approach. The emphasis moves to computing as fast and as accurately as possible the numbers and then assessing the risk results produced. A number of consultants are presently responding to the challenge of developing software to cope satisfactorily with this large computational task. Improving clarity and auditability is vital as is the need to be able to rerun QRAs with different input data, modifications etc quickly and efficiently.

A strategy review concluded that to meet the deadlines we would need four consultants working in parallel assisting various groups of assets.

Technically this poses new challenges as on the one hand we want to achieve as much consistency as possible whilst on the other hand we do not want to be so prescriptive that we demotivate and put a stumbling block in the way of the consultants who are working very hard assisting us.

We have therefore tried to concentrate on developing a good working relationship with the consultants, evolving with them a methodology and approach. The only key requirement we have felt obliged to stipulate is that appropriate focus is give to

i) TSR Impairment
ii) Evacuation
iii) Access to TSR

and that these key components do not get lost in a sea of individual risk estimates.

We have firmly resisted the use of some "black box" type software, emphasising the importance we place on understanding the hazardous scenarios and their interaction with the installation.

We are trying to ensure that our Safety Cases do not degenerate into large quantities of frequency and probability values from which it is difficult to gain a good understanding of the salient points.

This can be an uphill struggle. Risk numbers can look very imposing, comprehensive and authoritative. The fact that there are large numbers of assumptions and uncertainties can rapidly become overlooked and QRA is used more and more to judge tolerability where accuracy is crucial rather than to aid management decisions where confidence levels can be more adequately handled.

Temporary Safe Refuge

The failure of the accommodation area on Piper Alpha to provide adequate protection against fire and smoke was highlighted during the Public Inquiry. Lord Cullen interpreted the evidence as pointing to the need for a "Temporary Safe Refuge" which would provide shelter for personnel onboard against gas releases, fires and associated smoke.

The definition of a TSR and its associated performance standards is a key part of the Consultative Document (3), with a minimum endurance time stipulated together with a risk criteria for loss of integrity. These issues have been one of the important areas of feed back and debate on the Consultative Document (3).

There is concern that a definition and standards that may be appropriate for a large platform may not be appropriate for a small platform, though of course the principle of ensuring a safe means of escape and evacuation remains the same.

There is a danger that focussing too intently on the TSR could lead to an imbalance in the Safety Case for particular installations and could lead to inappropriate allocation of effort and resources. From everybody's point of view this would be undesirable.

REMEDIAL MEASURES

It has been important in all of the analyses that have been carried out to remember that the ultimate goal is not to produce a set of studies and reports but to understand the hazards and establish if there are any reasonably practicable measures that can be taken to prevent, control or mitigate them.

Identifying all the possible hazards and measures that could be taken to reduce them requires both those involved in the analytical studies and those who operate the installations to work together.

As a company it is recognised that to assist in identifying reasonably practicable measures there is a need to balance costs against risk reduction. Whilst the emphasis is rightly that in each case it is the quality and professionalism of the assessment that is paramount, it is also important that this assessment is approached in a reasonably consistent way across the assets.

During the Cullen Inquiry, BP Exploration presented a paper on how this balance was assessed when considering retrospective installation of subsea isolation valves. This approach is being refined into a general guideline for use across the assets.

This is where the true value of all the work to date is going to be tried and tested. How valuable will it be to the offshore workforce in helping them to understand the nature of the hazards they are exposed too and the measures that are in place to protect them? How valuable will it be to those involved in making what in some cases may be difficult and complex decisions?

References

(1) "The Operator's View of the Workforce Involvement in Offshore Safety", Mr D G A McKenzie, 16th June 1992, Institute of Petroleum - Aberdeen.

(2) "The Public Inquiry into the Piper Alpha Disaster", The Hon Lord Cullen, November 1990.

(3) "Draft Offshore Installations (Safety Case) Regulations 199-", CONSULTATIVE DOCUMENT, Health and Safety Commission, February 1992.

FIGURE 1

OVERVIEW OF APPROACH TO "FORTHWITH" STUDIES

Fire Risk Analysis

1. Preparation of plant area/isolatable system matrix
2. Model worst credible fire and explosion scenarios within each area
3. Assess damage levels and identify critical weaknesses

Evacuation, Escape and Rescue

1. Definition and description of existing evacuation system
2. Audit and comparison against existing and proposed standards
3. Base case assessment of system (without effects of accidents)
4. Assessment of system in response to accident scenarios

Emergency Systems Review

1. Identify and agree systems for review
2. Assess failure modes and effects and determine vulnerability
3. Assess impact of accident scenarios (from FRA) on "vulnerable" elements
4. Assess overall consequences for the systems

Smoke and Gas Ingress Review

1. Survey HVAC, doors and penetrations
2. Assess adequacy

COMPARISON OF EVENT TREE, FAULT TREE AND MARKOV METHODS FOR PROBABILISTIC SAFETY ASSESSMENT AND APPLICATION TO ACCIDENT MITIGATION

H James, (ICI FCMO, Blackley, Manchester), MJ Harris (University of Manchester) and SF Hall (SRD, AEA Technology, Warrington)

1. SYNOPSIS

Probabilistic safety assessment (PSA) is used extensively in the nuclear industry. The main stages of PSA and the traditional event tree method are described. Focussing on hydrogen explosions, an event tree model is compared to a novel Markov model and a fault tree, and an unexpected implication for accident mitigation is revealed.

KEYWORDS: Probabilistic safety assessment, event tree, fault tree, Markov, PWR, hydrogen

2. ACRONYMS

CET	Containment Event Tree
LOCA	Loss of Coolant Accident
MCS	Minimal Cut Set
PCSR	Pre-Construction Safety Report
PDS	Plant Damage State
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
RPV	Reactor Pressure Vessel
SRD	Safety and Reliability Directorate (part of AEA Technology, UK)
STPM	Stochastic Transition Probability Matrix
WCAP	WCAP-9991 (pre-construction PSA for Sizewell B)

3. INTRODUCTION TO PSA

PSA tries to assess the whole spectrum of risk presented by a hazardous plant or operation. It does this by systematically modelling a great number of different accident sequences. The main cause of possible public or environmental harm from an accident in a nuclear plant is the radioactive release that may result, so PSA attempts to assess the frequency of occurrence of the whole range of such releases.

The analysis is generally divided into three parts (see Figure 1). Firstly, it models the propagation of an accident through the plant. For each sequence which leads to a state in which the core of the reactor cannot definitely be cooled, the analysis then traces subsequent possible sequences of events in the containment (the building surrounding the reactor and associated equipment) and finally assesses the effects of any radioactive release. The analysis is normally limited to examining only the first twenty-four hours of the accident.