THE APPLICATION OF RISK ASSESSMENT TO EXISTING INSTALLATIONS

R.A. Cox
Chief Executive, Four Elements Ltd
25 Victoria Street, London SW1H 0EX

SUMMARY

In the past, the application of risk assessment to offshore installations has been mainly in the context of new projects. The Norwegian Petroleum Directorate's "Guidelines for Safety Evaluation of Platform Conceptual Design" are an example of this. However, in the U.K. sector there are well over 100 major platforms which may require retrospective assessment using "Formal Safety Assessment" (FSA) or "Quantitative Risk Assessment" (QRA) techniques. This paper addresses the special issues which arise when such methods are applied to existing installations.

Among these issues, the following are discussed:

- identification of remedial measures that are suitable for existing installations,
- decision-making framework for selecting upgrade measures,
- criteria for acceptability of risk for installations nearing the end of their productive life.

1.0 INTRODUCTION

There has been a pronounced trend in recent years towards the setting of safety **objectives** as the prime means of safety regulation, rather than the prescription of the **means** of achievement. This trend is in line with the philosophy of the U.K. Health and Safety at Work Act, 1974, which places a very general duty on operators to reduce risk to a level that is "as low as reasonably practicable".

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 case of large scale accidents, which by their nature are very rare, and therefore their frequency cannot be obtained from statistics alone.

The QRA technique is in widespread use in the offshore, nuclear and chemical industries, being applied to fundamental questions of conceptual design, siting, official approval and detailed design. In the full classical QRA approach, the objective is to quantify the risk of an entire industrial operation. This is usually expressed in terms of expected frequencies of fatalities. The method involves four stages: identification of failure cases, frequency estimation, consequence analysis and risk summation and evaluation.

The first step - failure case identification - is crucial to the overall quality of the analysis. For offshore platforms, the initiating events generally fall under the following headings:

- Releases of hydrocarbons from process equipment
- blowouts
- Releases from risers
- Ship collisions
- Structural failures
- Environmental loads
- Dropped objects
- Utilities failures

In real life, events may vary in size or intensity of effect. In a QRA model, only a selection of representative events can be analysed, so it is important (a) that the selected events are truly representative of the real ones and (b) that the frequency values assigned to each selected event equals the total frequency of the real events which it represents.

In practice, the above list of events is expanded into a much longer and more detailed list, specific to each platform. Typically, several hundred initiating events might be defined.

2.0 PAST USE OF QRA IN THE OFFSHORE INDUSTRY

In the offshore industry, the acceptance of QRA as an important decision-support technique has developed over a considerable length of time. In 1981, the Norwegian Petroleum Directorate published its "Guidelines for Safety Evaluation of Platform Conceptual Design" (NPD, 1981). This was based on QRA ideas, in a slightly modified form. The introduction of this methodology had a major effect on platform design concepts in the Norwegian sector of the North Sea, which may be seen by comparing platforms such as Statfjord "A" (designed before the regulations) with Gullfaks "A" (designed after the regulations). Whereas the earlier platform has a rather square plan with a somewhat cluttered layout, and conventional lifeboats, the later platform is elongated so as to separate hazardous areas from the accommodation, clear and straight escapeways running the length of the platform at several levels, free-fall lifeboats, and blast-resistant firewalls.

For the purposes of "Concept Design Safety Evaluation" (CSE), some adaptation of the basic QRA approach was required, to suit both the regulatory requirement for assessment for approval purposes and the design requirement for usable information about potential major hazards. The way in which NPD achieved this was by defining two classes of accidental event:

❶ The "Design Accidental Events" (DAE), namely those events which the platform will be designed to survive without serious loss, and

❷ "Residual Accidental Events" (RAE), which are the residue of extreme accidents which the platform will not be able to withstand.

It is relevant to note that the concept of "Design Accidental Events" has also been adopted in the nuclear industry, where it is termed the "Design Basis Accident". No such event may lead to release of radioactive materials (a consequence criterion), while the so-called "Beyond Design Basis Accidents", which are more severe, must have a demonstrably low probability (a frequency criterion).

The NPD requirements similarly place a numerical limit on the allowable annual probability of all of the RAEs summed up together (roughly 10^{-3} per platform-year). In effect, this defines the point at which accidental events are divided into the two classes. This approach therefore provides the design team with a set of clearly-defined design cases.

One of the first CSEs to be carried out in total conformity with the Guidelines was for the Heimdal platform, an 8-legged steel jacket integrated design. This study was the subject of a scientific paper published by Pyman and Gjerstad in 1983. Tables 1 and 2 of this paper are of particular interest and are reproduced here as Figures 1 and 2. The first of these lists the residual accidental events and their frequencies. It identifies process leaks, well blowouts and pipeline riser failures as dominant contributors to the total risk. Figure 2 lists the remedial measures implemented to address these accidental events.

In the UK sector, the techniques that have been applied most frequently in the past were HAZOP and Fault Tree Analysis, both of which are only applicable to specific isolated design questions. No full risk analysis was applied to a UK Sector platform prior to the Piper Alpha Disaster, although studies were carried out on specific design questions using risk analysis methods. An example of the latter was an analysis of the risks of a large gas pipeline and riser, which was directed partly at the question of whether or not a subsea valve was justifiable.

To date, it has not been necessary to carry out a QRA or CSE for the purposes of gaining field development approval or a licence to operate, nor has a risk assessment been required as part of the certification process, on any UK platform. However, it is possible that the Cullen Inquiry into the Piper Alpha Disaster will recommend the adoption of such techniques (known in this context as Formal Safety Assessments) for all existing or new platforms in the U.K. continental shelf (D.En, 1989).

In the U.K. sector there are well over 100 major platforms which may require retrospective assessment using "Formal Safety Assessment" (FSA) or "Quantitative Risk Assessment" (QRA) techniques. The remainder of this paper addresses the special issues which arise when such methods are applied to existing installations.

3.0 RISK ANALYSIS INPUT TO DESIGN

The specific ways in which risk analysis can be used to improve plant design are as follows:

❶ by decomposing the calculated total risk into its component contributors, and identifying which failure cases are the dominant contributors to the total risk.

❷ by examining whether the dominant contributors to the total risk are characterised by high probability, high consequences, or both.

❸ having identified a particular contributor to risk as being of high probability, remedial measures are suggested which are specifically directed at reducing the probability of failure (ie, improving reliability, for example by duplication of components).

❹ for those dominant contributors which are characterised by severe consequences, remedial measures are developed which specifically reduce consequences, such as lowering operating pressures, reducing inventories, installing a secondary containment system and so on.

❺ when particular improvement measures have been identified as candidates for implementation, the risk analysis may be re-run for each such option, in order to quantify the improvement in risk which would result. In conjunction with cost estimates for each option, an optimal strategy for expending resources can then be derived.

4.0 SPECIAL ISSUES IN QRA APPLICATION TO EXISTING INSTALLATIONS

4.1 General Statement of the Decision Problem

For existing installations, the question of how to ensure an appropriate level of safety is significantly different from the case of a new build. 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 package should therefore be seen in the 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 (and this principle is also firmly established in the case law arising from the Health & Safety at Work Act).

4.2 Identification of potential upgrade measures

In the QRA, a variety of models will be used to investigate the consequences of each accident scenario.

These include:

- Outflow models (liquid, gas, two phase)
- Adiabatic expansion
- Liquid spread and vaporisation (on topsides and on the sea)
- Dispersion models (dense cloud, jet)
- Fire models (pool, jet, fireball/BLEVE)
- Confined vapour cloud explosion.

Event trees are developed for each initiating event which detail the many possible scenarios and final outcomes of each event. They include consideration of mitigation effects such as valve isolation, deluge activation, and whether or not a release is ignited. By assigning probabilities to each arm of the event tree, the final frequency of each outcome can be established.

It is important to examine the opportunities for escalation, ie. whether the particular outcome of an initiating event can lead progressively to involve other hydrocarbon inventories or other parts of the platform, eg. a jet fire from a pipe failure impinging on the riser, or an explosion leading to failures of adjacent structure or pipework. This is usually achieved by examination of each postulated scenario on a simplified time-wise basis. Firstly, the **immediate effects** (i.e. within a few seconds) of the initiating event are considered seperately from the **final outcome**. This allows consideration of movement of personnel from their initial stations.

Secondly, in considering the consequences of the final outcomes, the times to certain events are assessed. Examples are: time to heat up structural steelwork to failure, times to heat up firewalls to unacceptable temperatures or to failure, and so on. These time-wise analyses are subsequently considered from the point of view of personnel survival (i.e., survival of escapeways, safe havens and evacuation facilities for the requisite length of time).

Each of the targeted events will have characteristics associated with them such as: the location of the origin of the event; whether the deluge failed; whether the ESD failed etc. Scrutiny of these characteristics may identify common features, which may become priority areas for the upgrade measures to address. For example, if the scrutiny of these chacteristics reveals that deluge failure was associated with a large proportion of the events, the deluge system would become a focus of some upgrade measures.

In many cases, more than one upgrade measure may have to be considered in combination. Individual upgrade measures may interact with each other in a number of different ways. For example, two measures may have overlapping effects, i.e. they both reduce the same risks. It may be that one measure reduces the particular risk at source, whilst another reduces the same risk at the receptor. Alternatively, two individual measures may be incompatible, e.g. the insertion of a fire wall may interfere with natural ventilation.

The activities required for systematic consideration of the options are therefore as follows:

(i) Define, by examining the physical effects of each accidental event, or by examining the causes, a candidate list of suitable upgrade measures to reduce the consequences or probabilities respectively. Add to this list any other candidates that may have been generated by other means (e.g., compliance with prescriptive requirements).

(ii) Define, on a platform-specific basis, all the accidental events which the candidate upgrade measures would protect against.

(iii) By examination of the range of coverage of the accidental events by the upgrades, develop a second candidate list, of **packages** of several individual measures, to be adopted in combination.

(iv) For each upgrade package, estimate the reduction in overall risk, relative to the base case ("do nothing").

(v) For each upgrade package, estimate weight and cost penalties.

(vi) Establish the constraints: safety acceptability criteria, cost limits, weight limits.

(vii) Discard any upgrade packages that are outside the constraints.

(viii) Discard any upgrade packages that are out-ranked by better ones (better ones being those that reduce risk more, for less cost).

(ix) Discard any upgrade packages for which the incremental improvement relative to the nearest alternative incurs a disproportionate incremental cost

(x) Assemble the remaining options in order of increasing safety (and increasing cost); present these options to the decision-maker.

(xi) In principle, there will be a presumption that the safest of the remaining options will be selected. This is in line with the principle of "as low as reasonably practicable". However, all of the remaining options are viable, and the decision-maker could chose another one if, for example, other factors are involved which have not been costed.

An example of how this can be presented in practice is the "Risk - Cost Diagram", as illustrated in Figure 3. In this diagram, various options for reducing the risk due to an oil pipeline system are compared. The options are labelled 1,2,3..... and are set out on the horizontal axis. Calculated measures of the risk associated with each option (in this case, the average rate of fatalities is used) are shown as a histogram above the horizontal axis. The corresponding capital costs are drawn in the downward direction as a second histogram. The order of the options has been rearranged such that the costs increase progressively from left to right.

From such a diagram it is easy to eliminate options which are out-ranked by others (Option 5 in this case), those that are not cost-effective (Option 2 - compared with Option 3) and those that do not meet risk targets and/or financial constraints. The remaining options are a subset from which the final choice will be made by the appropriate decision-maker.

4.0 CRITERIA FOR RISK

One approach to the setting of risk levels has been proposed by the Health and Safety Executive (HSE, 1988 and HSC, 1988) 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. The top band represents an intolerable risk level. The lower band represents a negligible risk. The middle area is where the risk should be managed so that it is "As Low As Reasonably Practicable". This middle area is therefore known as the ALARP region.

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, which is specifically recognised by HSE as a potentially relevant approach in their report on risk criteria for land-use planning near to major hazard sites (HSE, 1989, para 42 and Appendix 5).

Fleishman and Hogh (1989) have presented an example of the application of this approach to the question of cost-effectiveness of subsea isolation valves. In their paper, they review precedents for placing a monetary valuation on loss of life, concluding that this lies in the range of "between £$2x10^5$ - £$3x10^6$ per statistical fatality".

A cost-benefit approach is also an accepted principle in the application of the "ALARP" (as low as reasonably practicable) philosophy in the field of radiological protection (NRPB, 1988) and in road transport safety regulation.

Should the calculated levels of risk to personnel fall in the ALARP region, a Cost Benefit Analysis (CBA) approach should therefore be used to investigate the risk reduction per unit resource spent. The risk measure utilised in the CBA approach must obviously represent global (aggregated, or "societal") risk rather than individual risk, to be compared with the global costs.

The total risk impact of the installation is fully represented in the 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.

If it is desired to have a single-valued index of risk (and for the purpose of cost-benefit analysis, this must be the case), this value must be obtained by some form of integration of the F-N curve. The basic problem here is that the totality of the risk impact of any particular installation is a multi-faceted thing, and no matter how it is boiled down to a single indicator, there will always be some information lost on the way.

The most obvious risk index is the summation of $(f_i \times N_i)$, i.e. the average rate of fatalities. A possible drawback with this particular index is that it places equal weight on all fatalities, whereas it is often said that multiple-fatality accidents have a more serious impact, (and are certainly taken more seriously) than the same number of fatalities in single-fatality accidents. For this reason, the practice is sometimes adopted of raising the values of N_i to some power (typically 1.2), before carrying out the summation. This is equivalent to saying that an accident causing 10 fatalities has an equivalent risk impact to $10^{1.2}$ (equals 15.85) single-fatality accidents. The choice of the exponent 1.2 is, of course, a matter of policy and entirely arbitrary, although it cannot fall below 1.0.

The effect of varying the value of the exponent is to place different degrees of weight on the large-N end of the F-N curve, relative to the small-N end. No matter what value of the exponent is chosen, for any specific installation with its own characteristic F-N curve, the single valued indices may very well be dominated by events at one end or the other of the scale of N. If the exponent is 1.0, it is most likely that the index will be dominated by small accidents, while with higher values of the exponent, the index may well become dominated by large accidents.

Whichever statistic is adopted, it must be expressed in the form of actual or equivalent numbers of "statistical fatalities", and this means integrating the annual risk over the remaining life of the platform, generating a measure which is sometimes referred to as a "risk dose".

For comparing alternative upgrade strategies, the change in risk dose is what matters, and this must be calculated as follows:

improvement in risk dose =

(risk dose for remaining platform life for the "do nothing" option) - (risk dose for remaining platform life with upgrades) - (risk dose associated with the actual implementation of the upgrades).

The last of these is of considerable interest. It arises from several possible sources:

- helicopter flying risk for implementation personnel
- risks from special construction operations such as diving
- general occupational risks, specific to each trade and calculable from occupational safety statistics
- extra risks of process-related accidents due to accidental impacts or human errors during engineering work on the upgrades
- failure to reinstate systems to correct status after disabling them for upgrade work.

It is possible to estimate these incremental risks in most cases, provided that the work plan itself can be reliably estimated. It is entirely proper that they be taken into account and, in some cases, this aspect may well rule out certain upgrades that might otherwise have seemed attractive.

5.0 CONCLUSIONS

(i) Quantitative risk analysis has been used successfully for several years in the contexts of shore-based plant and new-build platforms.

(ii) The application of QRA to questions of safety upgrades to existing platforms is highly appropriate to the decision-making problem which these upgrades represent, and is in line with the current trend towards objective-based regulation

(iii) Quantitative risk analysis enables design measures which have the effect of reducing probability to be compared with design measures which influence consequences, and thereby enables an optimal choice to be made between these two disparate things. It also enables possible design improvements to be discovered which might not have been revealed by conventional methods of design development.

(iv) All options have to be seen as alternatives to the base case ("do nothing").

(v) Criteria for decision-making in this context must take account of : total aggregate risk to personnel, over remaining platform life; incremental changes in risk dose associated with upgrades; additional risks due to implementing the upgrades.

REFERENCES:

D.En. (1989) "Offshore Installations - Formal Safety Assessments", Discussion Document, Petroleum Engineering Division, Department of Energy, October 1989

Fleishman, A.B., and Hogh, M.S. (1989) "The Use of Cost Benefit Analysis in Evaluating the Acceptability of Industrial Risks - an Illustrative Case Study", 6th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries, Oslo, June 1989

HSC (1988) "Comments received on "The Tolerability of Risk from Nuclear Power Stations", Health and Safety Commission, HMSO

HSE (1988) "The Tolerability of Risk from Nuclear Power Stations", Health and Safety Executive, HMSO, I S B N 0118839829

HSE (1989) "Risk criteria for land-use planning in the vicinity of major industrial hazards", Health and Safety Executive, HMSO ISBN 0118854917

NPD (1981) "Guidelines for Safety Evaluation of Platform Conceptual Design", Norwegian Petroleum Directorate

NRPB (1988) "Revised Estimates of the Monetary Value of Collective Dose", NRPB-M157

Pyman, M.A.F., and Gjerstad, T. (1983) "Experience in applying hazard assessment techniques offshore in the Norwegian Sector" 4th International Loss Prevention Symposium, Harrogate, 1983.

FIGURE 1 (Source: Pyman and Gjerstad, 1983)

TABLE 1 : SUMMARY OF EXPECTED FREQUENCY OF ACCIDENTAL EFFECTS ON THE SHELTER AREA

ACCIDENT EFFECT	TOTAL EXPECTED FREQUENCY (/10^6/years)	CONFIDENCE LIMITS 95% Upper	5 % Lower
1. Hydrocarbon fire extending into shelter area following fire on LQ firewall of greater than 30 mins duration (approx.) at 150 k2/m^2.			
a) Following explosion in the process system* breaching compressor module firewall (28 events).	255	526	121
b) Following prolonged duration fire in the process system* due to riser rupture in the process module (8 events).	305	505	117
c) Following prolonged duration fire in the process system* due to BLEVE (10 events).	4	7	1
d) Following wellhead blowout and diffuse flame (not jet flame) leading to extensive topsides fire (production phase) (5 events).	247	816	43
2. Non hydrocarbon explosion originating in utilities module breaching firewalls on each side, with subsequent fire intruding into shelter area.	18	54	6
3. Extensive hydrocarbon fire originating at or near sea level from riser leak and engulfing the shelter area (single riser) (4 events).	385	1020	90
4. Extensive hydrocarbon fire that results in local collapse of the module support frame due to heat loading (150 kW/m^2) with no direct deluge system, leading to structural damage that renders the shelter area unusuable (8 events).	67	147	25
5. Extreme earthquake of 10^5 year return period.	5	15	2
6. Passing vessel collision.	13	50	4
7. Helicopter crash onto utilities module and fire.	8	24	2
TOTAL	1307	3164	411

FIGURE 2

(Source: Pyman and Gjerstad, 1983)

TABLE 2

Principal safety measures proposed and implemented for Heimdal main platform following the CONCEPTUAL SAFETY EVALUATION.

HAZARD	REMEDIAL MEASURES
Process system explosions	1. Update major firewalls between process and LQ.
	2. Introduce additional hydrocarbon fire walls on cellar deck to prevent fire ingress under LQ.
Riser rupture in the process area	1. Relocation of riser ESD valve to cellar deck.
	2. Deluge on riser pipe in topsides.
Wellhead fire	1. Location of drilling derrick at far end of platform in preference to alternative proposed location.
	2. Protection of flare boom base against enveloping heat radiation.
Riser fire at sea level	1. Package of measures to reduce likelihood of leakage from riser at sea level.
Evacuation	1. Use of free fall lifeboats.

FIGURE 3 RISK-COST DIAGRAM

EXAMPLE RISK COST DIAGRAM

Comparison of Risk and Cost for a number of risk reducing measures for an oil pipeline.