Determination of ALARP in conditions of uncertainty

J.D. Rimington CB
London, UK

V.M. Trbojevic
EQE International Ltd., UK

ABSTRACT: This paper offers the philosophical basis for tolerability of risk with levels of uncertainty of often unknown magnitude. The uncertainty of a risk estimate is treated in an explicit manner. It is recognised that the reduction of uncertainty does not of itself bring about risk reduction, but simply leads to better directed approach to precautions. It is these that reduce the risk. The process leading to tolerable level of risk starts with a reduction of uncertainty based on relevance and quality of evidence, and linking these to specific precautions; this is followed by further evaluating risk reducing measures against the remaining precautions. An example of application of this process is presented.

1 INTRODUCTION

Tolerability criteria are based on the following: above a certain level, a risk is regarded as intolerable and cannot be justified in any ordinary circumstances; below such levels an activity is allowed to take place provided that the associated risks have been made as low as reasonably practicable, HSE (1988).

The aim of this paper is to develop the philosophical basis for tolerability of risk with levels of uncertainty of often unknown magnitude. However, as any form of a numerical rule set has been ruled out at this stage, the problem had to be viewed from a slightly different perspective in which the uncertainty of a risk estimate is treated in an explicit manner.

Discussions about the treatment of uncertainty in risk analysis have been going on since the first application of Probabilistic Safety Analysis (PSA) in the nuclear industry. Since probability is the best known and most widely used formalism for expressing uncertainty, two views of probability have arisen: the frequentist or classical, and the subjectivist or Bayesian. The classical view defines the probability of an event occurring in a particular trial as the frequency with which it occurs in a long sequence of similar trials. Such interpretation depends on the existence of statistically significant data and in turn requires a demonstration that the results of such an analysis are also statistically significant in order to be used in a meaningful way, Schofield (1998).

In a subjective or Bayesian view, a probability of an event is the degree of belief that an analyst has that it will occur, given all the relevant information currently known. The probability is, therefore, a function of the event and the available information or a body of evidence. Implicitly in developing their results, the analyst must already have weighed the uncertainty against the evidence or available information. Any approaches in which uncertainties are explicitly treated from the start are nowadays labelled as Bayesian, Schofield, (1998).

The existing Tolerability of Risk (ToR) doctrine, HSE (1988), requires that the cost-benefit calculations are to be biased by applying "gross disproportion" to risks nearer the tolerability limit. Besides that it makes common sense, this application of the principle of gross disproportion can be interpreted as a precaution against the uncertainties in the best estimate of risk near the tolerable limit. Hence, there is a built-in recognition of uncertainties in the existing ToR doctrine.

HSE's recently published discussion document, HSE (1999), also stresses the fact that "uncertainty permeates the whole process of risk assessment, and that the HSE's approach to risk assessment and management has a number of safeguards to ensure the approach is in line with the Precautionary principle".

This discussion illustrates the real need for some form of guidelines for the treatment of uncertainties of risk estimates in such applications. This paper may be considered as an attempt towards this goal.

2 OUTLINE OF THE APPROACH

Risk and uncertainty are allied concepts in the sense that complete uncertainty related to some hazard could often imply a very high risk from encountering it. However, the reduction of uncertainty does not of itself bring about risk reduction, but simply leads to better directed approach to precautions. It is these that reduce the risk. Generally, the greater the remaining uncertainty, the greater the necessary precaution. The phases of assembling a risk model are shown in Figure 1.

The process of risk reduction proposed in this paper comprises two main stages:

1 Reduction of uncertainty
- Identification of uncertainties associated with an emerging the risk model.
- Assessing uncertainties by increasing the relevance and quality of evidence, in relation to the outline of the "risk object". This is a matter of increasing focus.
- Reducing uncertainty by inserting specific precautions. The precautionary margin could be decreased at this stage in line with the reduction of uncertainty.

2 Evaluating further risk reducing measures against the remaining precautions.

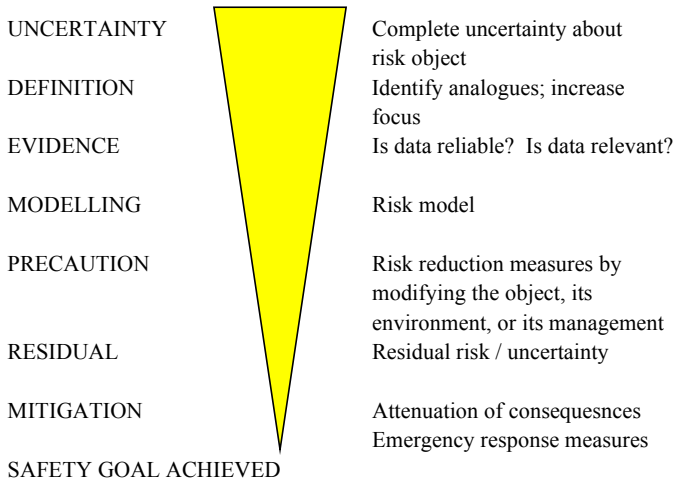

Figure 1 Process of Risk Reduction

3 REDUCTION OF UNCERTAINTY

3.1 *Identification of Uncertainties*

The uncertainties associated with risk estimation in QRA, in general, fall into three categories, Schofield (1998):

- Data - Deficiencies can arise from (a) the effect of small sample sizes, (b) the questionable relevance of generic data to specific items of equipment, and (c) the effect of limited reporting in relation to failure modes;
- Systematic - Deficiencies in the definition of the system under analysis in its environment, including particularly (a) identification of hazards and associated accident scenarios, (b) the physical conditions prevailing, especially environmentally, and (c) the accuracy with which the mode of operation is predicted.
- Consequence methodologies - Deficiencies are associated with prediction of accident escalation, such as heat fluxes, smoke concentration, structural damage and human behaviour. These phenomena are typically interactive, with complexity associated both with the compact and congested nature of offshore installations and their large hydrocarbon inventories, and with the sometimes intrinsically chaotic behaviour of the phenomena, e.g. turbulence in gas explosions, being modelled.

Overall uncertainty in a QRA arises from the combined effect of deficiencies and uncertainties of all these sources. Each case needs to be treated on its merits, with different elements isolated so far as feasible both in the estimation and the design, but treated with precautionary emphasis placed on mutually reinforcing safeguards. The worst case arises where a search for overprecision in quantification is allowed to bring about the use of pseudo-science to obtain numbers, arising sometimes from a false belief that the lack of a complete numerical structure might invalidate the whole assessment process.

For a risk assessment to be "suitable and sufficient" which is one of the requirements if it is to be used for ALARP demonstration, it should represent a consensus of subjective and objective inputs, Schofield (2000).

3.2 *Quality of Evidence*

No set of precautions is likely to be much better than the idea of the risks on which it is based, and since precaution is usually far more expensive than gathering and properly considering evidence, the latter process is clearly critical. The limitations of much of the evidence actually presented in connection with risk modelling need to be fully recognised at the outset, and allowance made. These limitations generally concern the relevance of the analogues adduced to the actual risk situation; and they can also be methodological. Naturally, the data itself must also pass the test of provenance; its source and innate strength will be the first questions to be addressed in any review.

Deficiencies in evidence often result from an effort to provide a quantitative view which the available data cannot sustain, and sometimes also from the overoptimistic application of computer modelling techniques. Quantification is obviously very desirable, because risk itself is a concept involving probability or degree, and because there is a need to prioritise risk elements so as to produce a balanced precautionary response. It is moreover a regulatory requirement that a safety case be supported by a "suitable and sufficient" QRA. Adequate numbers depend however on a solid experiential basis with a supportable link to the actual risk situation. The question arises, and will be pursued in this paper, what approaches should be adopted where this is not, or not entirely, the case.

3.3 *Reduction of Uncertainty by Increasing Focus on Evidence*

Where risks are judged to be at the higher end of the tolerability spectrum, the prior effort, before risk reducing measures are considered, should be to reduce the uncertainties through processes involving a close scrutiny of the evidence and validation where possible of the available data. A question arises if the risk is represented not as a single point best estimate, but as probability distribution representing uncertainty, i.e. as the probability distribution representing uncertainty about an inherently variable quantity. With ever increasing computational power, the use of input parameters described by distributions can easily be envisaged in future risk analyses. It is obvious in such cases, that some part (or a tail end) of the risk distribution will cross the tolerability limit, however minimally. This could be interpreted as a breach of the limit, and it would seem then to follow that an operator must undertake action regardless of cost, to shift the whole of the curve beyond the limit. In practice this would not be achievable. The situation can be represented graphically in Figure 2.

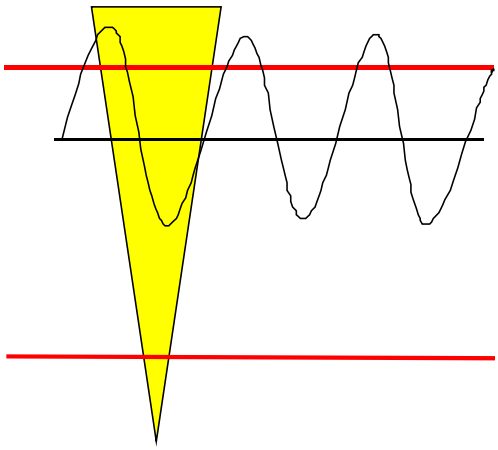

Figure 2 Risk Estimate and Related Evidence

In the above diagram, the point estimate of risk (the centre of the risk distribution "bell") is represented by a straight line and the quality of the evidence by a wavy line denoting excursions from reliable evidence. The aim of the first step referred to above is to flatten these excursions by demonstrating the acceptability of evidence (or reduction in uncertainty) and to follow this by the second step in which risk reduction is carried out in line with the accepted evidence, with due allowance for the remaining uncertainty.

In general, reduction of uncertainty can be achieved in two ways:

- By integrating more and more relevant information into the analysis; for example, as the number of trials is increased, the numerical value of probability will asymptotically tend to settle down to some value, Watson (1994).
- By exploring different solutions in order to solve the basic problem; this is based on a quest for a simpler and more elegant solution in which the influence of uncertain or un-measurable parameters is decreased to an acceptable level.

4 DEMONSTRATION OF ALARP

In relation to a new design, and once there is satisfaction that the overall risk is well within the tolerability limit, the demonstration of ALARP may often consist of a common sense judgement that best practice is being employed in relation to all safety critical elements of the design, following a testing of the assumptions made about the hazard and operational environment, and a scrutiny of the relevance of the proposed precautions and their fit with the proposed management system. However, an inspector is fully entitled to question the design proposal to ensure that cost-effective opportunities for better safety have not been overlooked. The greatest opportunities at the cheapest cost always exist at the design stage, and if lost can rarely be recovered, subsequent add-ons often being disproportionately expensive.

For safety add-ons , or when the basic design elements of a new design have been fixed, ALARP operates incrementally, so that the cost of an add-on is compared to the safety benefit conferred without reference to more fundamental redesign - unless opportunities for this are or could fairly readily be available cost-effectively.

An inspector is entitled to ask for consideration of any such opportunities.

It will be borne in mind that the onus to demonstrate that ALARP has been reached lies on the op-

erator, by virtue ultimately of the HSWA 1974. An inspector's
satisfaction that this is the case must not be unreasonably withheld or delayed, and matters can be taken to appeal if necessary, but the inspector's initial task is to challenge the operator's arguments, to seek to identify areas of significant uncertainty and inquire how they are being addressed, and generally to press the case for safety.

This is essentially an iterative process based on the rule that the Inspector does not himself propose design solutions, but taking into account the degree of uncertainty present in solutions which may be offered, may challenge an operator to meet standards reflecting "worst case" situations however unlikely these may appear to be and to demonstrate to him that on a balance of cost and feasibility the thing should not be attempted. It should be emphasised that this is not an evasion of the ALARP principle, but a way of meeting it where the uncertainties remain considerable.

Where high consequence risks combined with considerable uncertainties exist, the demonstration of ALARP is an onerous matter.

5 EXAMPLES OF APPLICATION

The application of the proposed approach is shown in the example of a Floating Production, Storage and Off-loading Vessel (FPSO)

5.1 *Description*

Monohull FPSO; forward passive turret, accommodation/TR, heli-deck and lifeboats aft; oil and gas reservoir; vessel has 14 cargo oil tanks; production equipment located on production deck, 4 m above the vessel upper deck level.

5.2 *Issue No. 1*

A critical event which is accepted in the safety case as possible is a large gas cloud accumulation and ignition, with accompanying large explosion over-pressure, in the area between the process deck and the vessel deck (storage tank covers). An escape tunnel has been provided to enable escape from process to accommodation/TR; this tunnel is being designed to withstand an explosion over-pressure of 0.5 bar.

5.3 *Design Basis*

The tunnel design is based on predicted over-pressure values of the order of 0.1 bar. This prediction, using theoretical over-pressure modelling is claimed to be pessimistic on the basis of assuming complete filling of the space between the two decks with a stochiometric mixture of gas, and ignition in the worst assessed position. On this basis, it was assumed that 0.5 bar rating for the tunnel is acceptable.

5.4 *Uncertainty and Lack of Evidence*

There is no evidence in the safety case that the installation design specifically caters for such an event on a defensible risk basis. It has not been demonstrated that such an event is not reasonably foreseeable, and consideration of risk reduction measures to protect personnel against it are such that an ALARP demonstration has not been made.

Furthermore, the over-pressure prediction is not validated for the scale and complexity of the gas-filled area. As such, there is no evidence that the prediction is pessimistic, even assuming complete filling with a stochiometric mixture. The current design is not robust in relation to uncertainty in over-pressures and the possibility of much larger over-pressures that may not be unexpected. Any possible precautions or pessimism in the design were not discussed.

5.5 *Treatment of Uncertainty*

The verdict in this case was that the duty holder has not properly applied the principle "as far as reasonably practicable" either in the design or mitigation measures. The first choice could have been to incorporate uncertainty in the over-pressure prediction by taking a precautionary approach and designing the tunnel to the maximum over-pressure that the supporting structure could retain. If the maximum over-pressure of the supporting structure was small, as could be the case with large floor areas, a possibility of having a "lifeline" tunnel design could have been investigated.

The second choice could have been to investigate the reserve capacity of the supporting structure and the tunnel in order to assess the robustness not only to over-pressure in the space between two decks, but also its vulnerability to fire and/or smoke ingress through cracks or damage areas.

In both cases the recognition of the lack of evidence either in a common sense design approach of having a "lifeline", or in more robust over-pressure prediction, has not been matched with precaution. Consequently, any ALARP demonstration would not have been robust.

6 CONCLUSIONS

To summarise the argument at this point; where the consequences of an accident could be large and there is significant uncertainty in risk estimates for important elements of design, ALARP cannot be judged solely in relation to cost and risk estimates (useful as these will often be to orient discussion between the operator and the regulator), in view of potential uncertainties of unknown magnitudes in such estimates. What ALARP consists of in such circumstances is made to emerge from a process of thorough critical scrutiny by a regulatory body able to demand "another go at the problem". This is emphasised particularly in situations when the QRA is used to argue that a particular safety measure is not reasonably practicable.

In the course of examining such situations an inspector may be justified in taking as his starting point what it is technically feasible to do rather than what may have been proposed as reasonably practicable; and challenging the operator to show that, perhaps by an innovative approach, what is feasible is not in fact reasonably practicable.

It should be emphasised such an approach does not mean in any sense that a higher level of safety than ALARP is demanded, e.g. by insisting on a standard based on feasibility alone. An argument involving cost versus risk reduction remains important, subject to robustness of risk analysis against uncertainty and tolerability of risk, and the discussion takes place against a background of goals, not of deterministic requirements.

It can indeed emerge on examination that at a certain point, the cost of further design improvement would increase exponentially (the "cliff-edge" effect) while up to that point improvement can be gained at relatively low expense if imagination is applied to redesign, and cases exist where this has proved to be so. The demonstrated

existence of a cliff edge effect can be a powerful indicator that the regulatory demand has been satisfied; so that (conversely) action up to a cliff edge may well reflect reasonable practicability.

ACKNOWLEDGEMENT

The support from the HSE-OSD and conversations with Dr. S.L. Schofield are greatly appreciated.

REFERENCES

HSE 1988. The Tolerability of Risk from Nuclear Power Stations, Revised 1992. ISBN 0 11 886368 1.

Schofield, S.L. 1998. Offshore QRA and the ALARP Principle, Reliability Engineering and System Safety, 61, 31-37.

HSE 1999. Reducing Risk, Protecting People - Discussion Document.

Schofield, S.L. 2000. The ALARP Principle and QRA, Proceedings of OMAE 2000 Conference, Paper No. S&R-6098, New Orleans, USA.

Watson, S.R. 1994. The meaning of probability in probabilistic safety analysis, Reliability Engineering and System safety, 45, 261-269.