JUSTIFICATION OF RISK-TAKING THROUGH REASONING, REASONABLENESS AND PRACTICABILITY

D.N.D. Hartford,
Scientific Advisor: - Safety and Risk Assessment
BC Hydro

The demand to specify what is "safe" by means of a simple determinant is virtually universal across society. However, such simplicity of determination with respect to the vast array of situations where safety is a consideration is rare, and is arguably a chimera, because safety is fundamentally a relative concept regardless how it might be defined in a dictionary.

This paper presents the view that the form and nature of "criteria for risk acceptability" are primarily political constructs determined by the legal and political frameworks of the jurisdiction where the risk is to be taken and the consequences of failure are absorbed. Accordingly, the paper presents the view that the matter of risk acceptance criteria is a complex matter of socio-economics and politics, informed by the engineering and natural sciences and then "made to work in practice" by the professions (doctors, engineers, lawyers, etc.).

The paper begins by explaining the historical and legal background to risk acceptance criteria in general, pointing out the distinct difference between risk acceptance in terms of common law and that of the Roman/Napoleonic legal code system. The difference between the quantitative risk acceptance criteria of the Roman/Napoleonic code legal system and the role if quantified risk in the determination of the Tolerability of Risk in the common law system will be discussed.

The paper then outlines the principles of risk regulation in the common law system which provides the Safety Case framework, whereby the tolerability and even the acceptability of risk can be established. The paper will then attempt to integrate all of the topics of the workshop within an overall analytical event tree/fault tree framework that is applicable to both the common law and Roman/Napoleonic legal systems. The paper will explain why in terms of the Roman/Napoleonic system, once the risk acceptance criteria are set in law, the most important thing for the analysts to do is "get the numbers right" whereas in terms of the common law system, the numbers are only the starting point of an reasoned argument pertaining to the tolerability of the risk.

The paper concludes by outlining why in terms of the common law system, risk acceptance is largely a reasoned argument that should always err on the side of safety through demonstration that risks have been reduced As Low As Reasonably Practicable. The matter of "practicability" being a matter of engineering whereas the matter of "reasonableness" is ultimately a societal matter, the validity of which can only be known after the Courts have ruled following an accident.

Political nature of safety

Maintaining the safety of the public involves complicated trade-offs and decision-making, which is highly political. Dams for example often have multiple purposes, which necessarily become important factors in decision-making. In other instances, many structures provide the same function to different users which results in the costs, the benefits and the risks being distributed in an uneven way

Although structural failures are rare, they are not impossible, nor inconceivable. It must be recognised that the probability of a structure to fail is not zero. And this recognition raises the questions: What would be the probability and what would be the consequences of the failure of a structure? How should these be weighted in a decision-making process?

Risk acceptability is a complex and in principle a political issue. Politics is the only activity where comparing apples and oranges is legitimate. Even in jurisdictions where the Roman/Napoleonic legal system prevails, political considerations can overrule the results of the risk assessment, as is the case of Schipol airport, which significantly exceeds the Netherlands VROM safety criteria (Figure 1 from Vrijling et al., 2004). This situation with Schipol is not unique and it exists in countries where the British legal systems applies for example, Sydney Airport, Australia (FAC, 1990).

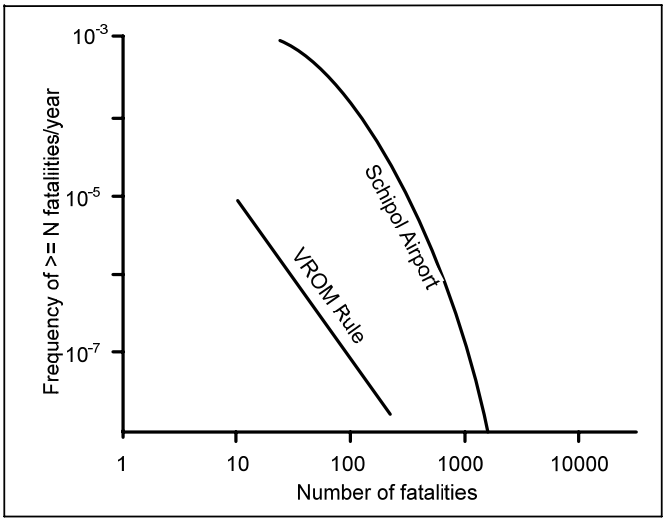

Figure 1. Political reality of societal risk criteria

Historical perspectives

The type of risk assessment criteria that might be appropriate for structural safety decision-making, as in any public safety policies and criteria, must be structured in terms of the prevailing legal system. Thus, any determination of risk acceptability will be determined in part by the underlying principles

that determine national and sometimes international laws. How these underlying legal principles affect the way risk assessment is carried out can be illustrated by comparing the differences that arise in the two most common legal systems. The "common law" system prevails in countries where the legal system developed under the British influence and the "Roman/Napoleonic" system that prevails in much of continental Europe and countries that developed under the European influence.

The fundamental principle underpinning the Roman/Napoleonic code is that costs and benefits must be balanced. That is the (marginal) costs of safety improvements should balance the benefits in terms of lives and property saved. On the other hand, in terms of the common law system where the ALARP principle (As Low as Reasonably Practicable) applies, the (marginal) costs of safety improvements should grossly outweigh the benefits in terms of lives and property saved. The most important point that arises at this stage is that; the two systems are incompatible and the differences cannot be reconciled. In terms of the Roman/Napoleonic system, the decision process is a straightforward balancing of costs and benefits requiring accurate analysis, and in terms of the common law system, the accuracy of the analysis is not as critical as the effort that goes into the demonstration of gross disproportion.

One of the most striking differences between the two systems is that in terms of the common law system, *what is not explicitly allowed is forbidden, unless it can be justified, where necessary in court*; whereas in terms of the Roman/Napoleonic system, *everything that is not explicitly forbidden is allowed*. This important distinction leads to completely different interpretations of the meaning of "As Low As Reasonably Practicable" under the different legal systems. These differences of legal definition mean that "seemingly different" or "seemingly similar" measures or metrics can lead to completely different conclusions (Ale, 2005).

Against this background, it is clear that the methods of determining the adequacy of the level of safety are not directly transposable from one jurisdiction to another. How safety decisions are made in Switzerland necessarily will not be directly applicable or even permissible in the United States.

Tolerability and Acceptability of Risk

Once it is accepted that zero risk is usually unattainable, that risk can be estimated, and that improvements in existing risk situations are always desirable then consideration can be given to the notions of broadly acceptable risk and tolerable risk (Figure 2).

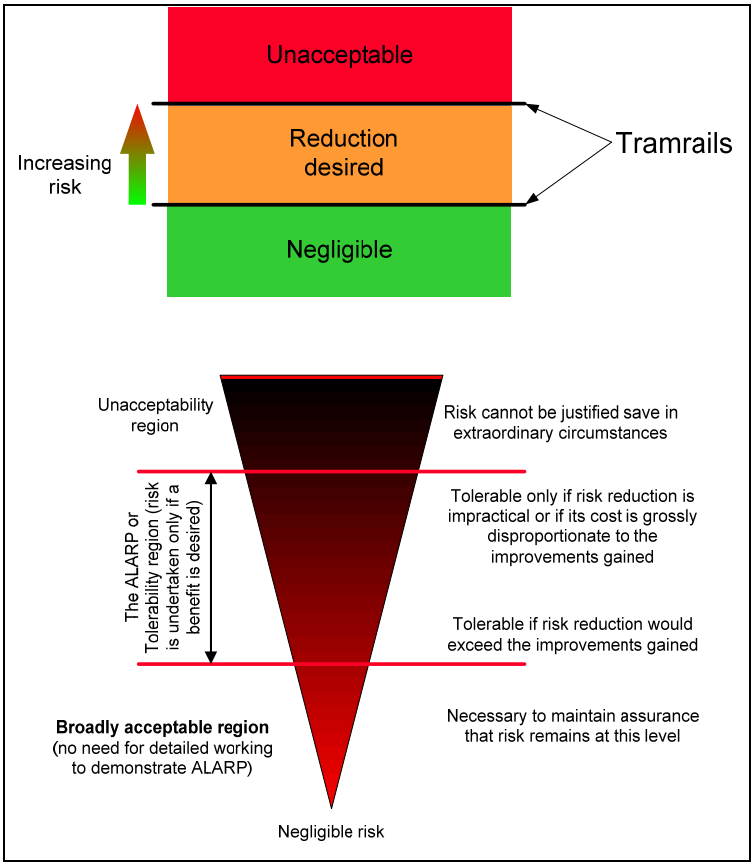

Figure 2 Acceptable and tolerable risk (Ale, ibid, UK HSE, ibid)

However, there is a subtle difference between the common law situation and that of the Roman/Napoleonic code in that under common law, improvements in risk situations must be achieved if reasonable opportunities exist. Thus, the manner in which the acceptability and the tolerability of risk are determined differs between the legal systems. In the Roman/Napoleonic system, the notion of tolerability of risk does not really apply because the legally enshrined "decision rule" constitutes the political acceptability of the risk. The situation under the common law system is such that risks are only tolerable if there are no reasonable opportunities to implement further risk reduction measures.

Presently, four classes of risk criteria are recognised (Vrijling et al., 2004):

1. criteria based on risk-cost-benefit measures,
2. criteria based on past performance or revealed preferences,
3. criteria based on societal or laymen's preferences, expressed preferences, and,
4. criteria based on natural standards, e.g. as in some environmental risk criteria.

In the Netherlands, the maximum individual risk in any new potentially hazardous situation is 10^{-6}/yr and 10^{-5}/yr for existing installations. The interpretation of societal risk is treated somewhat differently between the UK legal system and that of the Netherlands, particularly with respect to how risk aversion is accounted for (refer to Ale, 2005, ibid.). The situations

are broadly illustrated in Figure 3 (data from Ale, 2002, HSE, 1992, HSE, 2001, Govt. of Hong Kong, 2003).

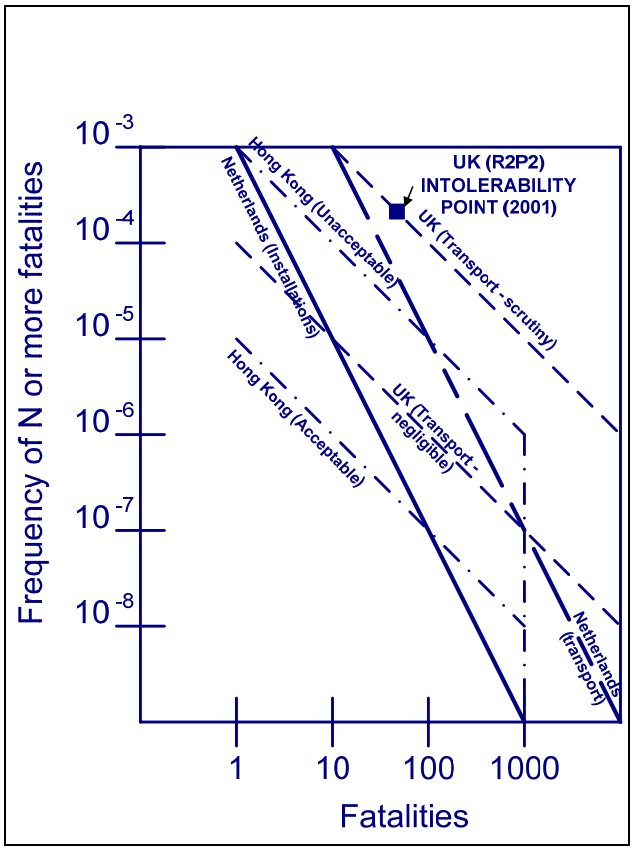

Figure 3. Societal risk criteria

Subject to the determining considerations that that zero risk is usually unattainable, that risk can be estimated, that improvements in existing risk situations are always desirable, and that improvements in risk situations must be achieved if reasonable opportunities exist, risk tolerability in the United Kingdom as summarised from Rimington et al. (2003) recognises the following risk levels:

1. An annual risk of death that is significantly lower than 1 in a million ($1{:}10^6$ or 10^{-6}/year) arising from any particular source is generally taken as a negligible level of risk. The risk of death from lightning is an example where very general precautions are taken without significantly affecting the course of everyday life.
2. An annual risk of death to members of the public from a hazardous facility (industrial or major public project such as infrastructure) in excess of $1{:}10^4$ (1 in 10,000 per year) has been explicitly deemed to be intolerable under normal circumstances. However, this does not preclude individuals from regular participation in sporting activities involving much higher risks, often in the range of $1{:}10^2$ – $1{:}10^3$.
3. The region of risk tolerability lies between these values of $1{:}10^6$/year and $1{:}10^4$/year. The Tolerability of Risk philosophy introduces

> requirements for; (a) the implementation of risk mitigation measures for situations that arise should things go wrong, (b) ongoing demonstration that the risk is being at least maintained at the estimated level, and, (c) a continuous search for effective ways to further reduce risk. All of these conditions apply for the risk to be considered tolerable, although the latter provision is qualified in that the costs of these measures be reasonable, in so far as not being grossly disproportionate to the risk reduction benefits gained.

According to Ale (Ale, 2005) in terms of the situation in the Netherlands, *"the limits are the end of the discussion and the role of ALARA or ALARP is more of a token statement. Courts invariably state that, should the government want more safety, it should put stricter levels in the law"*. In the United Kingdom, the requirements to demonstrate ALARP in terms of a logical argument that favours safety in terms of practicability and gross disproportion as a measure of reasonableness means that any numerical criteria are the starting point for the discussion between the regulator and the duty holder. Thus, in the Netherlands, the endeavour of risk assessment is analytical, set in a predefined legal framework, whereas in the UK risk assessment is more a matter of qualitative judgement.

The emphasis on quantification in the Netherlands places the onus on the duty holder to get the risk modelling and numerical elements of analysis right with the result that the emphasis is on rigorous scientific analysis to establish the facts, the political judgements being already built into the risk acceptability criteria. In the United Kingdom once the validity of the numbers have been established as a starting point, the main emphasis is on the robustness of the qualitative arguments around reasonable practicability and gross disproportion. In the United Kingdom risk assessment is a matter of fact and judgement with the added complication that ultimately it is up to the courts to determine if the duty holders have complied with their obligations after the fact, and thus far, court precedents are largely lacking. Thus, in the United Kingdom there is no way of being sure in advance if the duty holder's ALARP demonstration is sustainable in court, whereas in the Netherlands, the surety is provide by getting the numbers right.

While the numerical criteria adopted in the Netherlands and the United Kingdom look quite similar and while both regulatory philosophies recognise the same characteristics of risks (unacceptable, negligible and intermediate requiring careful consideration and continual vigilance) the interpretation is vastly different. However, as Ale points out (Ale, 2005, ibid.) the end result in terms of safety is quite similar.

The risk assessment criteria for hazardous industries in general that are either established, or are being established particularly in Europe,

essentially reflect the philosophies presented above. The criteria for Hong Kong extend these hazardous industry concepts to natural hazards in the form of landslide risk assessment criteria. The situation in Hong Kong regarding landslides is such that some losses are unavoidable, but the Government clearly wants to eliminate the possibility of loss of life in excess of 1,000 per event by restricting land usage to the extent that such losses cannot occur.

Risk-informed decision-making

While, the risk informed decision-making applies primarily to the common law system, the concepts can be seen to apply under the Roman/Napoleonic when political considerations override the decision rules.

Risk assessment provides a basis for clarifying the costs, benefits and risks and a framework to permit the decision-makers to arrive at informed decisions in the interests of society. Against this background, the position adopted by ICOLD in Bulletin 130 with respect to risk assessment for dams applies broadly to all built infrastructure. "*The traditional standards-based approach, by itself, is becoming increasingly inadequate to handle a single dam or a portfolio of dams in allocating limited resources for their operation, repair or improvement, in a climate of growing public scrutiny. Risk assessment is one technique, which could assist with this type of complex problem"* (ICOLD 2005).

In terms of the common law system, the role of risk assessment in safety management of built infrastructure is to inform decisions. The engineering calculations and the engineering criteria for acceptance are not the sole basis for the decisions as is the case with the traditional approach to structural safety decision-making. This also applies to probabilistic reliability calculations that generate a reliability index if they are used in safety analysis. The choice of an appropriate reliability index is a political choice, not a matter or engineering judgment.

Setting the decision context

The decision context defines the nature of the decision to be made. Traditionally, the decision context for structures has been to avoid structural collapse. In terms of the risk-informed approach, it is necessary to determine the spectrum of interests affected by the decision to set the decision context. The United Kingdom Offshore Operator's Association (UKOOA) when faced with a problem of commercial decisions with societal dimensions created the framework illustrated in Figure 4. This framework can be readily adapted for developing the decision context for structural safety decisions.

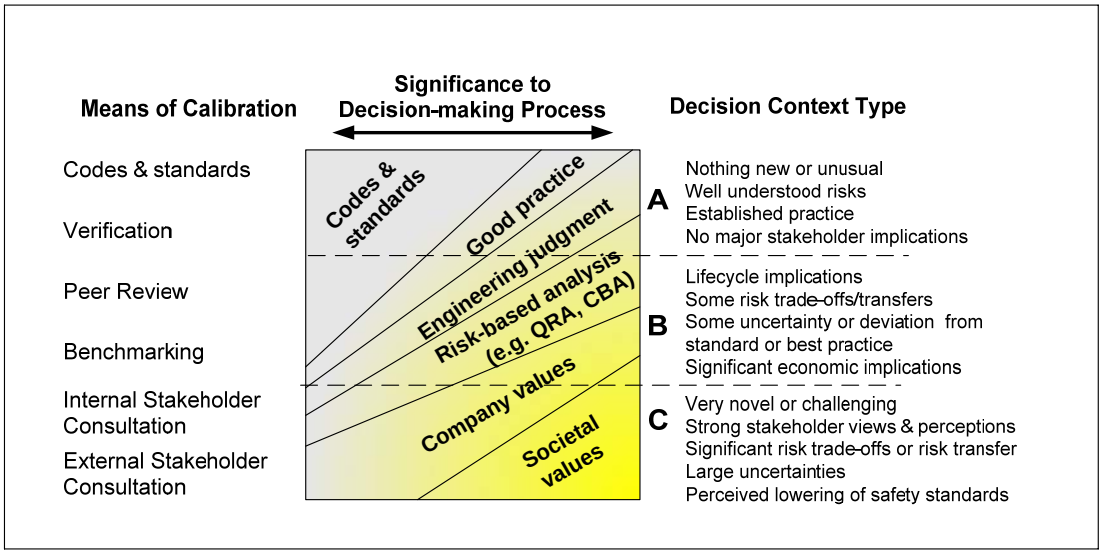

Figure 4. UKOOA Risk decision framework

Typically, structural safety decisions that pertain to the questions "avoid by how much?", "what constitutes "adequate?", and, "how limited?", and the questions "how safe is the structure?", and "how safe should the structure be?" can be considered to be in the lower part of Type B decision context and frequently entirely in Type C decision context. This is in stark contrast the traditional rules-based approach which has all of the attributes of the Type A decision context.

Principles of Risk Informed Decision-making

The basic principles of risk informed decision making are that the process is:

- Comprehensive
- Fair and equitable
- Transparent
- Consultative
- Defensible

The extent to which each of these basic principles applies depends on the nature of the risk and the objective of the risk assessment. Risk regulators and risk creators must be able to explain the hazard, the characteristics of the risk involved, the degree of uncertainty in that quantification, the methods used to make those assessments, and the confidence limits that can be placed on them. Clear and unambiguous characterisation of the problem is essential. It is also necessary to demonstrate the independence of the people raising the questions; to show that an interdisciplinary approach has been adopted; that established good practice has been applied; that conclusions have been fully tested and evaluated. It is necessary to demonstrate that these conclusions have been peer reviewed - but also that the data and evidence used, and the methodology applied, have been peer reviewed by appropriate people.

The “bow-tie” risk model (Figure 5.) provides a framework for conducting the risk analysis and illustrating how the risk controls have been established and how different risk control systems differ.

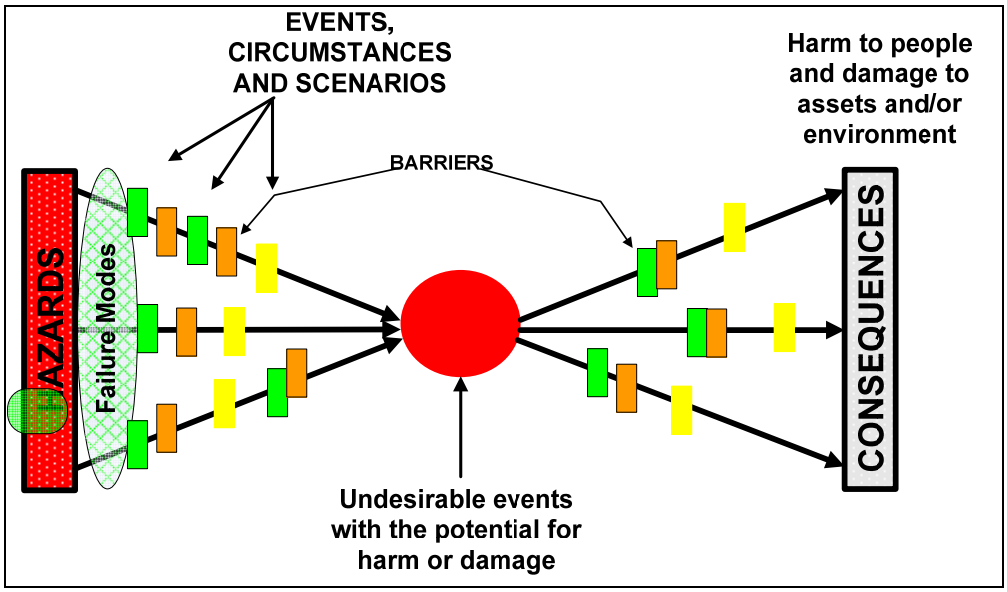

Figure 5. Bow-tie risk analysis & risk management model

Conclusions

Determination of “How safe is safe enough” is fundamentally a political matter, it is not a matter of engineering. This is even the case to a degree at a personal level because the state is deeply involved in prescribing what is “safe” to eat; what are safe behaviours; minimum levels of safety for engineered systems etc. This involvement by the state can be considered to be risk regulation even if the regulation is prescriptive and based on deterministic rules.

The philosophy of the UK Health and Safety Executive is that *“Risk-regulation is not first and foremost about protecting people at all costs. It is about making trade-offs. Trade-offs between different risks; between risks to some individuals or groups, and risks to others; between costs and benefits. It is the nature of risk that, frequently, those who create the risk do not bear its consequences nor its wider costs. So the market does not function properly as a distributive mechanism. The State must intervene to regulate risk.*

In doing so, the state's regulator has to confront some basic issues: most notably, the need for economic, social and technological progress compared with "zero risk" or `guaranteed safety". The regulator has to assert the propositions that risk is an necessary part of the human condition; that progress often depends both on incurring risk and on learning from failures (that is, accidents); that risks must be controlled but cannot in most circumstances be eliminated; that control of risks must - in the interests of technological development and societal progress - move public opinion from focussing on what is acceptable to what is tolerable; and that 'safe enough'

is the goal to be striven for in design, engineering and risk management" (Bacon, 1999).

Communication with the wider public, with policy advisers and with political decision takers - about purposes, processes and reasoning - is now essential. Transparency and communication will inevitably expose the extent to which scientific, engineering and regulatory decisions about risk depend upon the exercise of *informed judgement* rather than objective data. Transparency will also reveal the political, societal and personal values that underpin these judgements. Transparency is essential to retain the trust that will enable risk creators and regulators to continue to sanction processes that create risks. No amount of sound science, engineering, probabilistic risk analysis or risk quantification will get away from that need.

Hence, the answer to the question *How Safe should the structure be?* is found in the domain of social politics and economics, not in engineering, engineering and risk assessment informs the decision process.

References

Ale, B.J.M. (2005) *Tolerable or Acceptable: A comparison of risk regulation in the United Kingdom and in the Netherlands*. Risk Analysis, Vol. 25, No. 2.

Ale, B.J.M. (2002) *Risk Assessment Practices in the Netherlands*. Safety Science 40, pp. 105 – 126.

Bacon, J. H. (1997). "Engineering for Hazard Reduction: A Regulator's Perspective", Michael Leonard Lecture, London.

Federal Airports Corporation (FAC) (1990). "Hazard Analysis and Risk Assessment Working Paper", Draft Environmental Impact Statement, Sydney (Kingsford Smith) Airport, Australian Centre of Advanced Risk and Reliability Engineering Ltd., 1990.

Government of Hong Kong (2003) *Societal Risk Guidelines for Acceptable Risk Level*
http://www.info.gov.hk/planning/tech_doc/hkpsg/english/ch12/ch12_fig3.htm

Hartford, D.N.D. and Baecher, G.B. (2004) Risk and uncertainty in dam safety. Thomas Telford.

International Commission on Large Dams (ICOLD) (2005) Bulletin 130: Risk Assessment in Dam Safety Management.

Rimington, J., McQuaid, J., Trbojevic, V. (2003) Application of Risk-Based Strategies to Workers' Health and Safety Protection: UK Experience Reed Business Information ISBN 905901275 5.

United Kingdom Offshore Operators Association (UKOOA) (1999). A Framework for Risk Related Decision Support.

Vrijling, J.K., Van Gelder, P.H.A.J.M., Goossens, LHJ, and Voortman, H.G., (2004*). A framework for risk criteria for critical infrastructures: fundamentals and case studies in the Netherlands*. Journal of Risk Research 7 (6), 569–579.