A step change in reservoir safety management: Quantitative Risk Assessment and its strategic implications

A. J. BROWN, Jacobs. UK
J.R. CLAYDON, Independent Consultant, Yorkshire, UK
J. D. GOSDEN , Jacobs, UK

SYNOPSIS. Quantitative risk assessment (QRA) techniques now provide the ability to make meaningful estimates of the probability of failure, its consequences and thus the risk (probability x consequences) of dam failure. This has the potential to provide a major, step, improvement in reservoir safety management in UK. This paper describes the areas where QRA may be applied, the issues on which a strategy for use of QRA on dams needs to be developed and agreed within the UK reservoir engineering community, together with the requirements of the tools for the QRA.

INTRODUCTION

There are now several published alternative tools to assist in carrying out Quantitative Risk Assessment (QRA) of dam safety, including ICOLD Bulletin 130 (2005), ANCOLD Guidelines (2005), Canadian work (Hartford et al, 2004) and the UK Interim Guide (Brown and Gosden, 2004). Related approaches to asset management for flood and coastal risk management are also being developed in the UK using the concept of fragility curves, the variation of probability of failure with loading conditions (Defra Project FD2318, 2007).

Adoption of QRA as a tool for dam safety management provides significant benefits, but also significant challenges in that it may be in conflict with traditional "deterministic" standards and challenge preconceptions as to traditional priorities for reservoir safety.

This paper explores areas where QRA offers opportunities to improve management of reservoir safety, discussing the benefits and disbenefits of each, and the consequential strategic issues and associated requirements for QRA tools.

Ensuring reservoir safety into the future. Thomas Telford, London, 2008

ENSURING RESERVOIR SAFETY

WHAT IS THE PURPOSE OF QUANTITATIVE RISK ASSESSMENT?

Quantitative Risk Assessment for reservoirs has different objectives, depending on the perspective of the stakeholder. Communication between stakeholders requires a common understanding of processes and terminology. The current situation is that there is no universally agreed methodology or suite of tools for QRA, which can lead to misunderstanding and lack of acceptance of results. In order to come to agreement on the method to be used it is first useful to consider the needs of the different stakeholders.

The Regulator

The Regulator needs to understand the level of risk across the range of dams and reservoir which are present in the UK, and how these compare to other risk to the public, so that appropriate risk control measures are put in place. The Reservoirs (Safety Provisions) Act 1930 and the Reservoirs Act 1975 are both based on the volume of water stored. Although this is, in principle, simple to measure it does not measure the risk to the public, i.e. the product of the probability of failure and the consequences if a dam did fail.

The UK government prefers a risk based approach to management of residual risk, where risk is defined as the product of probability of an event, and its consequences. Evidence of this includes the paper on flood risk assessment (Defra, 2004) accompanying the consultation on the new government strategy "Making space for water" and the Health and Safety Executive (HSE) approach to regulating health and safety, as set out in "Reducing risk, protecting people" (2001). Similarly in the last few years Defra have renamed their "Flood and Coastal Defence" function as "Flood Risk Management".

The Interim Pitt report into the summer 2007 flooding includes a number of important recommendations which are likely to affect reservoir safety, including

> *IC33 – flooding legislation should be updated and streamlined under a single unifying Act that addresses all sources of flooding and facilitate flood risk management*
>
> *IC62 – the Government should implement the legislative changes proposed in the recently published Environment Agency biennial report on dam and reservoir safety*

It is clear from the report that a risk based approach is preferred by Government, and this highlights the need for the dam engineering industry to provide the appropriate technical tools.

The Owner

The owner has a wide range of needs with which QRA can assist. These include

a) To understand the magnitude of the consequences of dam failure. This may be obvious in a qualitative way to most owners – the consequences would be so severe they could go out of business. However there will be some owners who are unaware of the potential hazards and many who will have no idea of the scale of the economic damage that could be caused.
b) To have information on the likely extent of flooding and the number of people that would need to be evacuated, in the event of a dam failure
c) For a single reservoir to:
    - Understand the potential failure modes of the reservoir.
    - Consider the effect of changes in inspection and monitoring.
    - Assess options and alternatives to reduce the risk
    - Optimize the level of risk during any remediation process
    - Define the post remediation residual risk and identify appropriate residual risk control strategies
d) For a portfolio of reservoirs to:
    - Compare reservoirs for prioritized attention.
    - Provide reassurance to others especially those at risk of flooding.
    - Provide information for corporate risk management and insurance.
    - Demonstrate due diligence in the management of the asset

The Panel Engineer

The Inspecting Engineer is responsible for reviewing the adequacy of the safety of a dam. As such Engineering Guides have been developed to assist in this process, the earliest on Floods and Reservoirs being issued in 1976. QRA provides improved tools for use in this assessment, by providing

- A systematic means of reviewing and quantifying modes of failure.
- An analysis which can be updated.
- A means of showing the effect of improvements.

Summary

The various stakeholders in dam safety have a range of different objectives, which would benefit from a commonly agreed approach and toolbox of methods for quantitative risk assessment.

WHAT IS A TOLERABLE LEVEL OF RESIDUAL RISK?

Adoption of a risk based approach is significant in that it recognises that residual risk can never be zero, but is reduced to a tolerable level. The quantification of risk provided by QRA allows comparison of the flood risk

from dams with the risk from other forms of flooding and thus a rational basis for deciding what level of risk is tolerable.

The loss of life in some historic dam failures, and fluvial and coastal flood events, in the UK is shown in Table 1. The data from the historic fluvial and coastal events are plotted on a FN chart in Figure 1, together with the estimated fatalities in the event of failure of major UK dams from a number of QRA studies for major dam owners.

It can be seen that the risk from fluvial floods is similar to the risk of failure from the highest risk dams, in that although a failure of a higher risk dam has the potential to kill say 100 more people than a major fluvial flood, the annual probability is estimated to be 100 times less, such that the risk is similar.

In relation to coastal flooding, it is noted that coastal defences in the UK are generally designed only to retain a 1 in 200 chance per year (0.5% annual probability) flood event and historically have not been specifically designed for overtopping and are therefore likely to fail in say a 1 in 1000 chance (0.1% annual probability) flood. Major flood defences protecting London are designed to retain a 1 in 1000 chance per year flood, so the annual probability of failure would be correspondingly lower. In contrast dam embankments are designed to pass the Probable Maximum Flood (a probability of the order of a 1 in a million annual chance per year) safely. When other threats are considered the overall annual probability of failure of dams is as shown on Figure 1, but still generally less than the probability of failure of coastal defences.

This comparison of the consequences and probability of loss of life from different types of flooding shows how QRA can be a powerful tool to compare different risks to life.

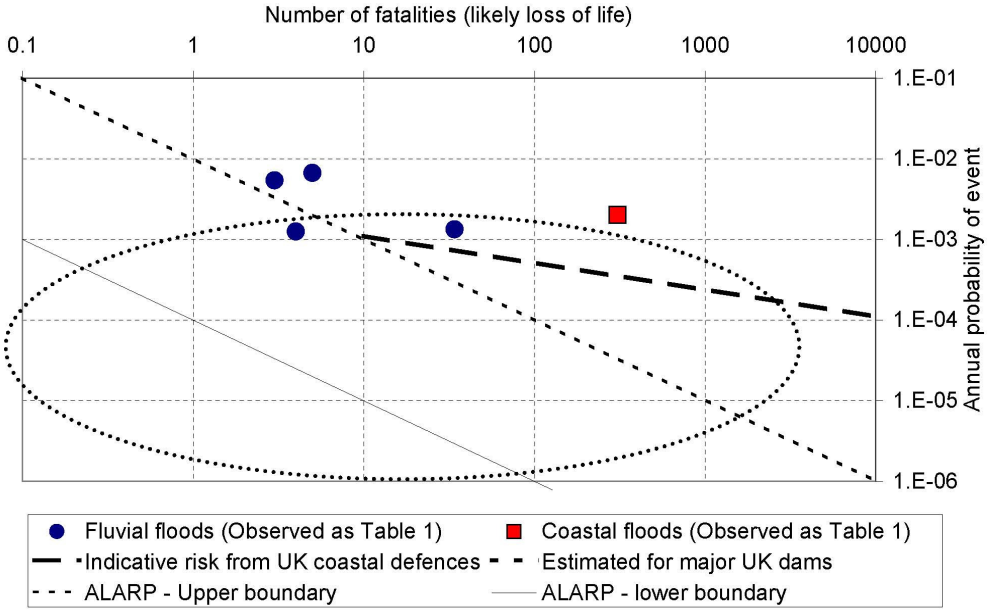
The strategic issue that then arises is what level of residual risk to flooding is tolerable, and where national resources are limited which type of flood risk should be prioritised for risk reduction. A similar approach can be adopted to compare the risk from dam failure with other high hazard industries.

The requirement for tools for QRA of dam safety is therefore to provide quantitative output which is on the same basis as, and thus comparable with, quantification of other risks to society.

Table 1 : Loss of life in some major floods in the United Kingdom

Year	Source of flooding	Location	Annual chance	Number of properties flooded	Loss of life
2007	Fluvial	Widespread	Commonly 4 times average monthly rainfall	48,000	13
2005	Fluvial	Carlisle	1 in 185	1,800	3
2000	Fluvial	Widespread	Commonly 1 in 15	9,000	0
1998	Fluvial	Widespread at Easter	1 in 150 to 1 in 50	Not avail.	5
1953	Coastal	East coast	1 in 500	24,000	307
1952	Fluvial	Lynmouth	1 in 750	165	34
1925	Dam failure	Skelmorlie	Not avail.	Not avail.	5
1925	Dam failure	Eigau/ Coedty	Not avail.	Not avail.	16
1912	Fluvial	Norwich	1 in 800	1200	4
1864	Dam failure	Dale Dyke	Not avail.	Not avail.	250
1852	Dam failure	Bilberry	Not avail.	Not avail.	81

Figure 1 : Comparison of risk from various forms of flooding (UK data)



HOW SHOULD ENGINEERS DECIDE WHEN A DAM IS SAFE ENOUGH?

QRA provides a means to quantify how a dam may fail, including explicit consideration of modes of failure, and quantification of each of the steps in that process. An example of this is the methodology used by US Bureau of Reclamation to assess the safety of their dams against internal erosion, where the dam safety review team answers each of the questions shown in Table 3 (Cryganiewicz et al, 2007). Although panel engineers may consider modes of failure in a generalized way when assessing the adequacy of a dam, it is often not carried out systemically and it is rare for it to be written down.

It is suggested that more systematic use, and documentation, of event trains to capture likely modes of failure is desirable as a means for owners to demonstrate their safety case and panel engineers to provide an audit trail of their safety review. Such event trains should be part of the QRA toolbox of techniques. The process of thinking through the most likely failure modes of a dam has also proved invaluable to Supervising and Inspecting Engineers in identifying likely indicators of adverse performance, and thus elements of the dam where surveillance should be focused.

Table 3 US BOR Event Train for failure from internal erosion

Q	Adverse step in event tree	Example for failure along bottom outlet pipe
1	What is the event that initiates internal erosion?	Pipe fractures
2	Will high flows occur sufficient to begin erosion?	Flows may be limited by pipe diameter
3	Is there an unfiltered exit?	Rock toe may limit
4	Will a roof form completely through the core?	Depends on type of core material (unknown)
5	Are flows limited by an upstream element?	Magnitude of flows determined by size of pipe, size of fracture and head on the pipe
6	Will early intervention be unsuccessful?	Use of existing drawoff
7	Will breach process initiate?	
8	Will heroic intervention be unsuccessful?	Full emergency drawdown, with additional imported pumps

The second part of a QRA analysis, of quantifying the probabilities of each of the steps which could lead to failure, requires a clear definition of failure. Traditional techniques such as Floods and Reservoir Safety (ICE, 1996) provide a recommended design standard, in terms of a specified flood with wave freeboard. This has the weakness that the calculation provides no measure of how close to failure the dam may be. QRA would normally

define failure as the loss of the ability of the dam to retain the reservoir, and by defining a probability this provides a measure of the proximity to failure. This change would be similar to the change in structural design of reinforced concrete from elastic design in CP114 to plastic design in CP110 in 1975.

It is suggested that Floods and Reservoir Safety should be rewritten to be a risk based approach, where the Critical Flood (the flood that would just cause failure in the duration of a single storm) is related to a tolerable probability of failure. The techniques and tools for this analysis already exist; the main uncertainty relates to the magnitude of overtopping flow to cause failure which is the subject of ongoing research.

HOW IS THE ADEQUACY OF SAFETY EVALUATED IN OTHER INDUSTRIES?

The Control of Major Accident Hazards Regulations 1999 (COMAH), which implemented European Directive 96/82/ EC, requires that operators of top tier sites produce a "Safety Report", with the purpose and content of the report set out in Schedule 4 of the Regulations. Such a report can be in several parts, with contents including

a) Demonstrating a safety management system is in place
b) Accident hazards (failure modes) have been identified and necessary measures taken to prevent such accidents
c) Safety has been incorporated in the design, construction, operation and management
d) On-site emergency plans have been drawn up
e) Information to allow planners to make a decision relating to the siting of new development around establishments

Further detail on interpretation of the COMAH regulations, including when risk has been reduced "As low as reasonably practicable" (ALARP) and how QRA assists in this process is given in HSE publications, including Appendix 3 of Reducing Risks Protecting People (HSE, 2001a) and Guidance Notes to Inspectors (HSE, 2001b). There are similar requirements for the safety case in other high hazard industries.

The principles and administration of review of the safety case in different industries was reviewed in the HSE Discussion Document "Regulating Higher Hazard Industries" published in 2000, and the Cullen Report into the Ladbroke Grove Rail incident published in September 2001. The latter endorsed the use of safety cases, but raised important questions about what makes them effective. These led to the HSC Policy Statement (2003) on "Our approach to permissioning regimes", which sets out their approach to management of the risk from high hazard industries. This includes ten

principles. The key items relevant to application to reservoir safety are contained in principle 3 and include:

- Permissioning regimes build on the fact that the legal duty to manage risks lies with the organizations that create them
- The key to receiving "permission" will normally be a description and demonstration of how duty holders manage their risks
- The process of describing and demonstrating requires duty holders to think through their actual operations, from beginning to end, identify their hazards and consider the risk and control measures or systems needed to comply with the requirements of the regime

DISCUSSION – NEED FOR A UK STRATEGY FOR RESERVOIRS

Should we move towards a safety case for reservoirs?

The question "Is the dam safe enough?" (Hatford et al, 2004) is a tricky one to answer. As Low As Reasonably Practical (Appendix 3 of HSE, 2001) may satisfy Health and Safety Executive (HSE) but not consultees in the flood plain of a proposed new reservoir. Comparison between different risks in society is difficult in terms of agreed methodologies, communication and acceptability. A way forward might be for each reservoir to have a Safety Case prepared at construction or the next inspection and periodically reviewed and updated subsequently. This would have the advantages of transparency, and ensuring that owners of reservoirs thought through and documented how they manage the safety of their reservoirs.

The Safety Case would be a documented statement of the risk to third parties posed by the dam, and how those risks were being managed to ensure they were tolerable. Such a safety case would be similar to the "safety report" defined in COMAH regulations, and could include

a) Description and drawings of dam and reservoir
b) Impact assessment of likely consequences if the dam failed
c) Data on performance of dam, including Reservoir Record, Instrumentation and Monitoring
d) Statement as to design criteria for dam, and supporting calculations such as floods, slope stability, internal erosion and failure modes (where available; if not available prepared only when considered necessary to support the safety case).
e) Evaluation of most likely failure modes and for higher hazard dams quantification of probability of failure
f) On-site emergency plan
g) For high consequence dams inundation maps for use for evacuation in the event of imminent dam failure
h) Statement as to Surveillance and dam safety management regimes

This would be building on the current provision of information to Inspecting Engineers under Section 21(5) of the Reservoirs Act 1975, but would differ in that the owner would add "h", a formal statement of how he manages the safety of his dam, and that he endorses this as reasonable. The big advantage of the safety case system is that it focuses liability where it lies. It would also have the advantage that the owner can include how the subject dam relates to the whole of his portfolio, and thus provide a basis for an owner to prioritise work across his portfolio.

It is recognised that non-technical owners will require assistance from dam engineers in preparing the safety case, but the final document must be signed off by the Undertaker as being their responsibility

A range of options for the preparation and review of a safety case regime for reservoirs are given in Table 4. The safety case would apply to all new reservoirs, alterations and existing reservoirs. The role of the "qualified civil engineer" would remain, similar to the Registered Professional Engineer in some countries, but could be as advisor to the owner, or in an independent role. The closest to the current regime would be Option C, but would mean that the safety case was prepared independent of accredited engineers. It would be more logical for the safety case to be prepared by accredited engineers, which would mean adoption of Options B or E, the difference relating to the system for review.

Related issues include that

a) The Safety Case would have to be kept as a live document by the owner, being submitted to the Regulator for consent at prescribed intervals, which could be ten years for Consequence Class A2 and B dams, and five years for Consequence Class A1
b) To maintain the independence of a review this is not just independent of the undertaker but also independent of the preparer of the safety case
c) If the cost was considered disproportionate for small, low consequence dams, then a two tier approach could be adopted, with a safety case only required for Category A dams, or dams which come under the ICOLD definition of "large dam" (which applies to only the largest 20% of UK dams)

<u>Should we move to risk based engineering assessment?</u>

Application of deterministic standards have several disadvantages, including that it can lead to overdesign, lack of thinking about the problem, lack of recognition of adverse circumstances in which the standards are inappropriate and lack of recognition of uncertainty. A risk based approach requires explicit consideration of failure modes which has the advantage that

this develops a greater understanding of the problem, requires explicit consideration of uncertainty and enables meaningful/measurable use of ALARP principles to decide when additional costs are proportionate to the reduction in risk achieved. It is considered that a risk based approach ultimately leads to better decision making in terms of management of residual risk to both the public and the owner of the asset.

Table 4: Options for Safety case regime for reservoirs

Option	Preparation of safety case	Regulator	Involvement by Panel Engineers
A	Owner prepares	Technical review (Note 1)	None
B	Owner prepares, but employs Panel Engineer to oversee preparation, and sign off	Technical review (Note 1)	Employed by Owner to oversee and sign-off safety case.
C	Owner prepares	Check that independent review completed and actions being taken	Independent review employed by Owner
D	Owner prepares	As C	Independent review employed by Regulator
E	Owner prepares, but employs Panel Engineer to oversee preparation, and sign off	As C	a) As B, and b) Independent review employed by Regulator

Note 1. Where the Regulator carries out a technical review this would be by staff in the sole employ of the Regulator, to avoid commercial conflict of interests. For the 2000 dams in England and Wales this could be the equivalent of 3 or 4 full time staff.

What level of residual risk is tolerable, and how does it relate to other residual risks faced by society?

One measure of an acceptable probability of flooding from dam failure is to compare it with standards for the probability of fluvial floods, with Table 5 showing the definitions given by both Planning Policy Statement (PPS) controlling new development in UK, and the European Floods Directive. However, a fluvial flood is a natural event whereas a reservoir is a man-made structure/threat. Arguably the probability of flooding due to dam failure should be say 10 times less. A more comprehensive measure of tolerable risk is As Low as Reasonably Practicable (ALARP) analysis of risk (probability x consequences). This provides a tool to evaluate when the

cost of further risk reduction measures is proportional in relation to the reduction in residual risk.

Table 5 Terminology for probability of floods

Probability of flooding	European Union Floods Directive (2007/60/EC)	Table D.1 of PPS 25 (2006)	
		Zone	Annual probability
Low	Not defined	1	Less than 1 in 1000 (<0.1%)
Medium	Likely return period ≥100 years	2	1 in 100 to 1 in 1000 (1% -0.1%)
High	Not defined	3a – High probability	1 in 100 or greater (>1%)
		3b – Functional flood plain	1in 20 (5%) or greater

CONCLUSIONS

Quantitative risk assessment (QRA) techniques now provide the ability to make meaningful estimates of the probability of failure, its consequences and thus the risk (probability x consequences) of dam failure. This provides the ability to use QRA to make more informed dam safety decisions, but also challenges the status quo. This paper has described some of the opportunities and the practical consequences.

The following issues are identified where it is recommended that current practice is modified

a) the dam owner should be made responsible for preparing a "safety case" which sets the risk to the public from that dam, and how he is managing that risk ALARP, this safety case being sent to the Enforcement Authority. This safety case would be subject to independent review under the existing periodic Section 10 Inspection process. The level of detail would depend on the level of risk or consequences, and could vary from simple qualitative assessment, through event trees to full quantitative risk assessment
b) the existing "Floods and Reservoir Safety" prepared to assist Panel Engineers and dam owners, is based on "deterministic" standards" and should be rewritten to be risk based. Similarly other existing and future engineering guides should be rewritten to be risk based.
c) the UK should have a toolbox of different techniques for QRA, suitable for a range of uses by the stakeholders involved in dams.

The differences between particular dam engineers is noted and suggests that a panel of users should be set up to develop the toolbox of QRA tools, rather than leaving development to a single contractor or user group. It is

anticipated that the specification for the techniques in this toolbox would include:

- quantitative output which is on the same basis as, and thus comparable with, quantification of other risks to society
- suitable for a range of level of detail of application, from preliminary screening analysis of low risk dams, to detailed analysis of extremely high consequence dams
- be practical and useable by a knowledgeable practitioner not just theoretical and not a 'black box' written by the developers
- methods for dam owners to use in support of their safety case, including justification where the cost of further risk reduction works is disproportionate to the reduction in risk that would be achieved
- output in the format that could be annexed to both the safety case and a Section 10 Inspection Report under the Reservoirs Act 1975, as an audit trail

REFERENCES

ANCOLD, 2005, *Guidelines on risk assessment.* 156pp excl appendices

Brown, A.J. and Gosden, J.D., 2004a, *Interim Guide to quantitative risk assessment for UK reservoirs.* Thomas Telford.

Cyganiewicz J M, Engemoen WO, Redlinger CG, 2007, *Bureau of Reclamation experience with evaluating internal erosion of embankment dams. In Internal Erosion of dams and their foundations*. Pubs Taylor & Francis.

DCLG (2006) *Planning Policy Statement 25 (PPS25): Development and Flood Risk*

Defra (2004) *Flood and coastal erosion risk assessment and prioritisation.* Background paper accompanying consultation on "Making Space for water". Flood Management Division. July

Defra, 2007, *Performance and reliability of flood and coastal defences.* R&D Technical Report FD2318.

Hartford DND, Baecher GB, 2004, *Risk and uncertainty in dam safety.* CEA technologies Dam safety Interest group. Thomas Telford. 391pp

HSC (2003) Policy statement *Our approach to permissiong regimes.*

HSE (2000) *Regulating higher hazard industries: exploring the issues.* Draft for discussion. London, HSE

HSE (2001a) *Reducing risks, protecting people*

HSE (2001b) *Principles and guidelines to assist HSE in its judgments that duty holders have reduced risk as low as reasonably practicable.* On HSE website.

ICE, 1996, *Floods and reservoir safety*, 3rd Edition. Thomas Telford

ICOLD, 2005, *Risk assessment in dam safety management.* Bulletin 130