SEISMIC SAFETY ASSESSMENT OF TWO CONCRETE DAMS IN A CASCADE DEVELOPMENT - INVESTIGATIONS INTO THE USE OF QUALITATIVE RISK ANALYSIS TECHNIQUES

Gilbert H SHAW[1], Benedict H FAN[2] And Desmond N HARTFORD[3]

SUMMARY

Dam safety management in mature dam safety programs requires more than the traditional standards-based approach to safety investigations. The expanded objectives include (1) consideration of all potential causes of failures or incidents, (2) the establishment of an appropriate focus for the investigations and (3) the need to prioritise additional actions including more detailed studies and/or implementation of risk reduction measures. This suggests that some form of failure modes analysis might be a useful way of achieving these objectives.

Previous BC Hydro investigations into the application of Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA) in addressing these issues in a rational and systematic manner in dam safety management have focused on dam safety reviews at individual dams. This paper describes BC Hydro's latest investigations into the potential for application of these techniques to determine the best course of action for seismic retrofitting of two concrete dams in a cascade development.

The paper indicates how, through the use of FME(C)A and supporting logic diagrams, it may be possible to make more objective and transparent the exercising of engineering judgement which is fundamental to ranking seismic performance issues in terms of risk-based importance and to the making of cases for implementing risk control initiatives. One purpose of this paper is to illustrate the concepts under investigation with the view of obtaining constructive review and criticism from the engineering profession prior to their formal adoption by BC Hydro.

INTRODUCTION

As part of its investigations into and development of risk analysis techniques for dam risk management, BC Hydro is continuing its examination of potential applications of qualitative risk analysis methods in routine dam safety investigations. In BC Hydro's dam safety program, 'routine dam safety investigations' refers to two of the cornerstones of dam risk management: (1) surveillance, which provides ongoing confirmation that the dam can remain in operation and (2) periodic dam safety reviews (every 5 to 7 years) which are aimed at confirming that the safety management system for each dam is operating effectively. BC Hydro is also interested in determining if qualitative risk-based techniques can be used to focus deficiency investigations and for developing and illustrating cases for justification of risk control measures. In this regard, there may be potential to use risk analysis techniques to assist in developing seismic emergency response plans for dams.

Efficient management of surveillance and periodic dam safety reviews as dam safety programs mature requires a much broader and better defined focus than is required when establishing 'initial surveillance activities' or during 'first round' investigations. Reasons for this improved resolution include, but are not restricted to, the following:

[1] *Gilbert H. Shaw P.Eng., Senior Engineer, B.C. Hydro, Burnaby, B.C., Canada. E-mail: gil.shaw@bchydro.bc.ca*
[2] *Benedict H. Fan P.Eng., Specialist Engineer, B.C. Hydro, Burnaby, B.C., Canada. E-mail: ben.fan@bchydro.bc.ca*
[3] *Specialist Engineer, B.C. Hydro, Burnaby, B.C., Canada, E-mail: des.hartford@bchydro.bc.ca*

- Dam systems [Dam Safety Interest Group, CEA, 1999] are invariably complex and the assessment of the safety of dams and the associated uncertainties requires a logical and systematic approach to safety investigations and information collection and assimilation.
- While many aspects of surveillance activities and emergency preparedness planning are common to all dams, there are unique features that are important to the safety management of each individual dam. These features are identified only through thorough understanding of all possible failure modes of the dam.
- Uncertainty is ever present in dam safety investigations and some means of dealing with these uncertainties is required to deal with the more obscure issues that are encountered in mature dam safety programs.
- Once a portfolio of dams have been retrofitted to meet standards that prevailed at the time the deficiencies were identified, recommendations for additional risk control initiatives to meet more recent (higher) standards, which are often set in an arbitrary manner, require careful consideration.

The final bullet is particularly important in seismic retrofitting of dams as dam owners, like owners of other engineered facilities which also do not meet "the standards of today", are faced with the dual problems of ageing structures and ever increasing current design standards. This is particularly true of seismic performance criteria for existing dams, which were designed and constructed without the current knowledge of seismicity and dynamic response of structures. Therefore, so-called 'new deficiencies' are in fact 'newly recognised deficiencies'. In addition, many older dams now suffer deterioration typical of ageing structures. As a result, surveillance and dam safety reviews, carried out in terms of "the standards of today", frequently identify numerous potential deficiencies that may contribute to the risks posed by the dams.

This paper describes the latest of BC Hydro's on-going investigations into the potential use of qualitative risk analysis in addressing some of these complex issues, in particular issues surrounding the seismic withstand of Blind Slough Dam and Ruskin Dam. The underlying question to be addressed (although not in this paper) is not "Are these dams safe?", but rather "Are they safe enough?"

The approach being investigated is Failure Modes and Effects Analysis (FMEA), a qualitative design analysis technique [British Standards Institute, 1991] which can also be used as a risk analysis technique [Canadian Standards Association, 1991]. Although application of FMEA [Beak et al., 1997] and variations of it [Stateler et al., 1995, Anderson et al., 1998] in dam safety management is relatively recent, there are strong indications that it will prove to be useful in addressing some of the challenges in assessing the safety of dams and identifying possible improvements in risk control techniques. The most common applications of failure modes analysis have been at a very general level considering broad assessments of complete systems as a cost effective first step towards establishing levels of risk and expenditure priorities [Beak et al., 1997]. In a mature dam safety program, it is necessary to determine if these concepts can be extended beyond prioritisation and be applied consistently and effectively in dam safety management. BC Hydro's investigations are also aimed at addressing many of the legitimate concerns raised by experienced dam and hydropower engineers about the difficulties of performing risk analysis for dams [Jones, 1999], several of which were encountered during the investigations described here.

DESCRIPTION OF PROJECTS

The Alouette-Stave-Ruskin Hydroelectric System

Blind Slough Dam, part of the Stave Falls Project, and Ruskin Dam are components of the Alouette-Stave-Ruskin Hydroelectric System and are located on the Stave River, 55 km east of Vancouver in British Columbia, Canada. Water from Alouette Lake, located to the west of the Stave River, is diverted through a tunnel to a 9 MW generating station on the western shores of Stave Lake. As spillway discharges or dam breach flows at Alouette Dam, which impounds Alouette Lake, would not affect Blind Slough Dam or Ruskin Dam, Alouette Dam was not included in the analysis and is not discussed further.

Natural Hazards - Hydrology and Seismicity

The watershed upstream of the Stave Falls dams has an area of 953 km^2 and is located entirely within the Coast Mountain Range of British Columbia. Annual precipitation is high, averaging about 3500 mm, and the seismicity of the area is also high. A seismic hazard analysis [BC Hydro, 1993] determined that the peak horizontal ground acceleration (PGHA) for the Design Basis Earthquake (DBE) at the Stave Falls dams is 0.23 g and the corresponding PGHA for the Maximum Design Earthquake (MDE) is 0.56 g. The seismicity at Ruskin Dam, 6.5 km downstream of Blind Slough Dam, is essentially the same.

Stave Falls Project and Blind Slough Dam

Stave Lake is the main storage reservoir of the hydroelectric system. The size of the originally natural lake was increased to 62 km^2 by the construction of the dams of the Stave Falls Project. These include the Main Dam and Intake Dam, which are adjacent and were constructed in the original river channel, and a saddle dam, called Blind Slough Dam, approximately 400 m to the east. The Main and Intake dams are currently being retrofitted to meet present day seismic safety standards and, therefore, were also excluded from the analysis. Blind Slough Dam was constructed in 1922 and is a concrete gravity structure with a length of 195 m and a maximum height of 18.3 m. It contains the discharge facilities of the Stave Falls Project which include 4 radial gate undersluices and a 10 bay sluiceway. Structural analyses of Blind Slough Dam have shown that the dam would be unlikely to survive the MDE. Seismically induced failure of Blind Slough Dam would have a direct bearing on the post-earthquake performance of Ruskin Dam downstream, assuming that Ruskin Dam survived the earthquake.

Photo No. 1 Blind Slough Dam (on left) and Stave Falls Main and Intake Dams

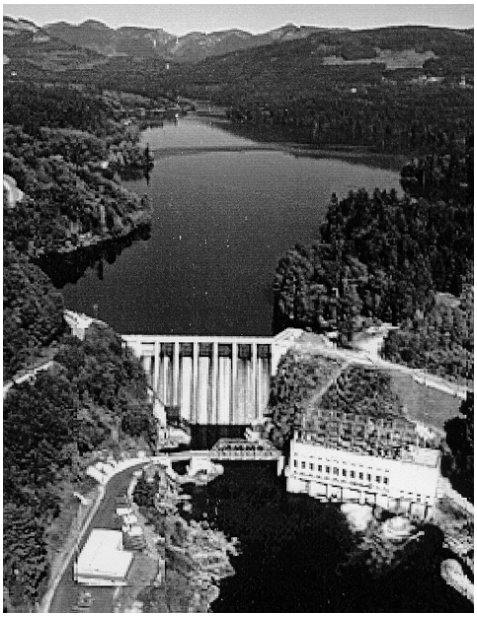

Photo No. 2 Ruskin Dam

Ruskin Dam

Discharge from Blind Slough Dam, and the Stave Falls powerhouse, flow into Hayward Lake, the reservoir impounded by Ruskin Dam. Constructed in 1930, this concrete gravity dam is 110 m long and has a maximum height of 59.4 m. Although the dam is founded on rock, the abutments are a complex soil rock formation, each with a buried channel. Power intake tunnels through the left abutment supply the 105 MW generating station. On the right abutment, the foundation rock is about 15 m below the crest of the dam and a complicated cut-off system extends upstream from the dam for approximately 130 m. Progressing upstream from the dam, this system includes a concrete gravity wall section, a vertical concrete core wall and steel sheet piling, all capped by a sloping concrete slab placed on granular backfill. Since the original construction, there has been a history of excessive seepage and some migration of fines. The discharge facilities consist of 7 radial gate outlets which extend across virtually the full length of the dam. Results of recent structural analyses indicate that the seismic withstand capability of the dam may not meet current performance goals, with the upper part of the dam, including the spillway piers, appearing to be the most vulnerable.

Current Safety Management Issues

With reference to the seismic hazard analysis [BC Hydro, 1993], the current safety management issues under investigation are:

- the seismic stability of Blind Slough Dam,
- the seismic resistance of the right abutment of Ruskin Dam,
- the seismic stability of Ruskin Dam, and
- the reliability of post-earthquake spillway gate operation at Ruskin Dam.

In addition, the seepage and the migration of fines in the right abutment of Ruskin Dam is under investigation. A 'systems analysis' approach, combining analysis of the seismic safety issues at both dams, is considered appropriate in this case because of the potential for common cause failure and the interaction between the performance goals of both dams. These issues are being investigated as part of BC Hydro's overall risk management strategy for its dams which aims to demonstrate that the risk posed by dams are effectively controlled.

RISK MANAGEMENT AND RISK ANALYSIS

Risk must be understood to be effectively managed, and this understanding is gained through risk analysis. Risk analysis generally includes (1) hazard identification and characterisation, (2) system performance and response analysis and (3) consequence analysis and their integration.

Major difficulties in performing quantitative risk analysis techniques in dam safety are the limited amount of failure data and the fact that no two dams are the same. Although there has been considerable progress in probabilistic characterisation of potential hazards, such as estimating peak ground accelerations caused by earthquakes, and notable recent progress in probabilistically modelling the seismic response of earthfill dams [Lee et al., 1998, Lin et al., 1999], similar success has not been achieved in the probabilistic modelling of the seismic performance of concrete dams. Currently, it is difficult, if not impossible, to model the 'near or at failure' behaviour of, say, concrete gravity dams with any reasonable accuracy. Therefore, detailed quantitative risk analysis for concrete dams is impractical. However, the benefits of working within the systematic framework of risk analysis (that were demonstrated through the analyses of earthfill dams) are such that it is appropriate to apply risk-based techniques in assessing the seismic safety of concrete dams to the extent that it is possible and reasonable, while avoiding the pitfalls associated with attempting to probabilistically describe the structural response of the dam. Consequently, the approach being investigated is a hybrid scenario type analysis with probabilistic description of loads and deterministically analysed responses to the loads and resulting consequences. This said, the generally good performance of concrete dams during earthquakes poses significant difficulties for qualitative description of seismic failure modes for dams as the actual failure modes can only be described in broad terms and the failure mechanisms are often beyond experience. The analysts are, therefore, required to develop working hypotheses (by hypothesis we mean *"proposition made as a basis for reasoning, without assumption of its truth"*) to explain the relationship between failure mode and failure effect. This fact, together with the fact that models of the seismic performance of dams are inevitable simplifications of reality, often goes unrecognised in the design and retrofitting decision-making process.

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS

Principles

Failure Modes and Effects Analysis (FMEA) is a design technique that was initially applied in process and manufacturing industries, such as the aerospace and hazardous process industries [Henley et al., 1992, Jones, 1996]. The primary objectives of a FMEA are (1) acquiring a structured understanding of a system, (2) identifying the function(s) of the system components and (3) determining the potential component failure modes and the effects of those failure modes on the performance of the system. FMEA can be extended to include considerations of criticality (Failure Modes, Effects and Criticality Analysis, FMECA) by characterising the likelihood of the events and severity of consequences in terms of indices [British Standards Institute, 1991].

There are two primary approaches to conducting a FMEA/FMECA: the "component" or "hardware" approach, and the "functional " approach. The "component" approach involves listing the individual components and the analysis of their possible failure modes to identify the effects on the system. The "functional" approach is based on the premise that every element of the system is designed to perform one or more functions which can be

considered as outputs. The functional FMEA/FMECA is performed by listing and analysing these outputs to determine their effects on the system. Although it may appear that the "component" approach might be best suited for analyses of dams, a hybrid approach which identifies the components, their functions, how they might fail to perform those functions and the effect of functional failure may be more appropriate. FMEA/FMECA generally uses inductive logic techniques (What happens if there is an earthquake?) which can be applied at the design stage or operational stage, and at any level of detail.

The basic steps in a FMECA are:
1. Define and understand the system.
2. Break the system down into components, defined by their function.
3. Analyse the potential failure modes of each component.
4. Assess the consequences of each identified failure mode and the effect on the performance of the system.
5. Assimilate the findings and determine the relative severity (criticality) of each failure mode.
6. Document the analysis and the results and make recommendations as appropriate.

While apparently a straightforward process, recent experience suggests that FMEA/FMECA for dams might be rather more difficult to implement than expected. One reason is that components of dams function in a 'passive manner', whereas the technique was developed for systems that operate in an 'active manner' (create outputs such as pumping action). Several other difficulties have also been identified and it may be that significant adjustments to the process will be required for application in dam safety. Nevertheless, the basic concepts of defining a 'system' and 'sub-systems' does have many benefits, including defining the system boundary which forces the analyst to reveal how the subsystems and components interact to meet the overall performance of the system.

Consistent assignment of criticality indices is particularly challenging and it is necessary to establish appropriate protocols to promote consistency throughout the analysis. In this regard, while the selection of protocols is arbitrary to a degree, the reasonableness of the arbitrary selection must be demonstrated. A further challenge is to ensure consistency between studies, if FMECA is to be applied for prioritising amongst dams in a portfolio.

System Definition and Failure Mode Identification

The "system" was defined to include Stave Lake and the mountain slopes above the lake, Blind Slough Dam, Hayward Lake, Ruskin Dam including the abutments, and the power conduits. Due to the large number of components, two levels of sub-systems were defined, the first level on the basis of the system definition just outlined, and then each second level sub-system divided into components, as shown in Fig. 1. While there are no hard and fast rules defining the extent to which the system should be broken down into subsystems and/or components, a guiding principle used in this case was that the system be broken down to a level where it could be analysed in a transparent manner and that the reasonableness of the modelling process could be judged by subject matter experts. At any level in the system, each element of the system constitutes a sub-system which may or may not require further subdivision. If an element or component is found to be highly critical, then that component may be further sub-divided. Once the components are defined, all component functions are identified. This step requires in-depth knowledge of the design intent, any departures from the design intent, the as-constructed condition and any changes to the condition. When applied to dam safety, it is generally not necessary to consider small individual components of specific items. Great care is necessary in system/sub-system definition as the number of elements to be considered can increase rapidly and the analysis can become unmanageable. Ultimately, however, the number of system subdivisions and components analysed will be controlled by the ability to realistically model the failure mechanisms and their interactions.

A preliminary assessment of the worst case consequences of failure of the components was found to be a useful aid in focusing the study. In this FMECA, the system and subsystem comprised 149 components with 307 component functions and 333 potential component failure modes. The effect on system performance of many identified potential component failure modes proved difficult to assess because of the high degree of component interaction. This problem can make the analysis very difficult and the analysis team must understand precisely how each component performs its functions and the extent to which component interaction can influence failure modes of other components. To address this difficulty, it was found necessary to supplement the FME(C)A process with qualitative event and fault trees to illustrate the conditions that must exist for a component failure mode to initiate.

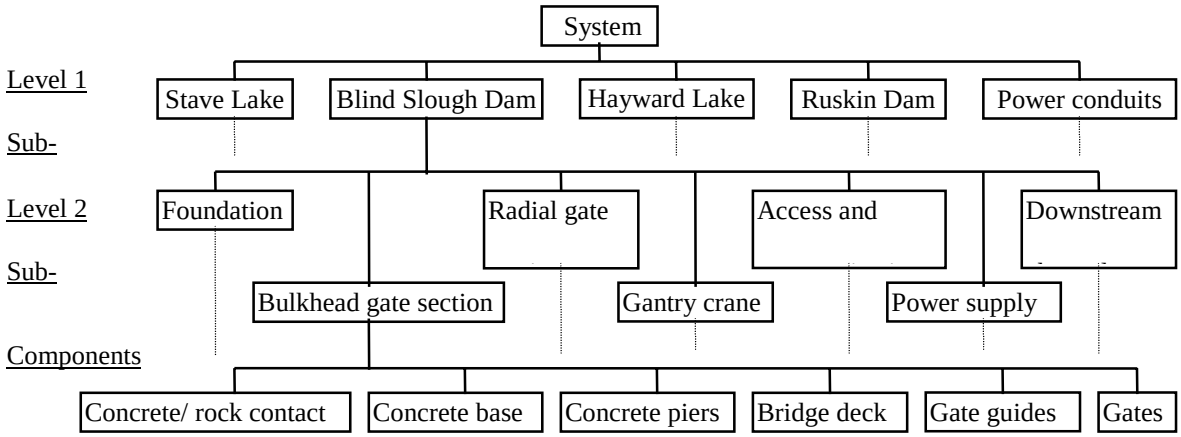

Fig. 1 Sub-systems and components

Failure Effects

Due to component interaction, it was found useful to describe failure effects in two ways, 'immediate' effects and 'ultimate' effects. This modification of the basic FMEA process appears to be necessary to accommodate the differences between failure mode analyses of 'active' and 'passive' systems. This has the added benefit of prompting the analysts to explain how failure mode initiation at any level of the system is manifested. This is potentially of great value in surveillance as the analysis can reveal how onset and development of failure modes might be detected, thereby enabling intervention before 'system failure'. Another benefit of this step is the identification of possible intervention to prevent either system failure or mitigate some of the downstream losses caused by a system failure. In this regard, BC Hydro is investigating how best to use failure modes analysis to provide additional focus for surveillance activities and emergency response planning at its dams.

Component Criticality

To obtain a comparative measure of the criticality of each identified component in relation to the system performance, indices were assigned to (1) the "likelihood" of each identified component failure mode, based on earthquake exceedance frequencies and the withstand capability given the earthquake criteria, (2) the severity of the consequences, and (3) the potential for successful detection and intervention. A criticality index for each combination was then derived from the three assigned indices. Various schemes could be adopted but it must be recognised that the objective is only to identify the relative criticality of the components. To avoid reliance on subjective estimates, deterministic analysis of the seismic response is used to estimate withstand capability and, therefore, justify the assignments of "likelihood". This requires a subtle departure from the basic approach to failure modes analysis as, rather than describing when failure mode initiation is expected, the deterministic analysis is used to bound the loading conditions under which failure mode initiation is not predicted. Strictly speaking, this approach violates a fundamental tenet of risk analysis that requires the probability of failure to be estimated. However, it does not violate principles of relative ranking, provided consistency is maintained throughout the process.

In FMECA, indices, for example in the range 1 to 5, can be assigned to the deterministically analysed onset of unfavourable performance of each component in terms of the protocols as illustrated in Table 1. The range selected for the indices should reflect the range of conditions considered in the analysis and the need to discriminate between conditions.

By anchoring the deterministic analysis to probabilistically analysed earthquake exceedance frequencies, it is possible to relate the approach to quantitative risk analysis concepts. If the analysis indicates that initiation of a failure mode might only occur for very low frequency (extremely unlikely) earthquakes, the occurrence of this failure mode can, in principle, be described as being extremely unlikely and assigned a low value such as 1. If the analysis indicates potentially unfavourable performance during more frequent earthquakes, values in the range 2 to 4 are assigned, dependent on the frequency of the loading condition of concern. A value of 5 would indicate no appreciable seismic withstand capability.

Table 1. Protocols for Assigning Likelihood Indices to Failure Mode Initiation

Deterministically Analysed Condition	Rating
Component performance capacity exceeds MDE performance goal.	1
Performance capacity considered marginal at MDE level	2
Component has DBE capacity but not MDE capacity	3
Marginal DBE withstand capacity	4
Component does not meet nominal minimum performance goals, or will not if essential maintenance is not carried out	5

Consequence indices were based on the deterministically estimated severity of ultimate failure consequences. Since the consequences of, say, failure of the radial gate section of Blind Slough Dam, failure of the right abutment of Ruskin Dam and stability failure of the whole of Ruskin Dam would be significantly different, different values were applied to each component. In some cases, it may be necessary to assign different indices to different failure modes of the same component. Similarly, if the potential for detection of a deteriorating condition and effective intervention was judged to be within normal maintenance activities, a value of 1 was assigned. Conversely, a failure mode where effective intervention to mitigate the consequences was considered to be unfeasible a value of 5 was assigned.

Using the assigned indices, a criticality index can be computed for each identified component failure mode. In this analysis, the indices were multiplied, which resulted in criticality indices in the range of 1 to 150.

Presentation of Results

The results of the analysis were presented graphically to the extent that is possible (logic diagrams, event and fault trees) and also in tabular form in which each row, corresponding to an identified component failure mode and consequence, includes:

- identification of the first and second level sub-system and component,
- a description of the identified potential failure mode,
- a description of the consequences,
- an explanation of the assessed potential successful detection and intervention, and
- numerical values corresponding to the failure mode initiation and consequence indices and the criticality index.

To facilitate cross referencing of the large number of identified potential component failure modes and consequences combinations, a unique reference number was included in each row. In addition, because of the component interaction, two columns were added to the table to list the reference numbers of other potential failure modes which would, or may, affect the likelihood of the potential failure mode in question, and list potential failure modes which would be affected by the considered potential failure mode. This cross referencing was also useful in the development of event and fault trees.

CONCLUSIONS

The concepts presented on the potential application of qualitative risk analysis techniques in the seismic safety assessment of dams have yet to be peer-reviewed prior to their adoption by BC Hydro. However, based on the experience to date, the following preliminary conclusions may be made:

- Failure Modes, Effects and Criticality Analysis, if appropriately modified, can be applied in risk-based ranking of issues concerning the seismic retrofitting of dams.
- The difficulties associated with correctly defining the system, its sub-systems and components (which reflect the complexity of the system) should not be underestimated.
- Accurate definition of component interaction is vitally important.
- The system logic diagram provides a very useful focus for the deficiency investigation as it reveals the number of components and the complexity of their interactions.
- The general inadequacy in the understanding of seismic failure modes and mechanisms of concrete dams, together with the associated modelling limitations, creates an additional constraint on the application of failure modes analysis techniques.

- Qualitative event tree and fault tree models provide an invaluable means of demonstrating the logic of the analysis process and facilitate the review of the analysis as a whole.
- The basic FMEA/FMECA process must be modified to accommodate the performance of 'passive systems' under earthquake loads in addition to the general inability to model failure mechanisms of concrete dams.

Clearly, the difficulties encountered in applying these concepts point to two distinct areas for research: (1) system-based analysis of dams and cascades of dams, and (2) analysis of the mechanics of dam failures during earthquakes. As a review of recent literature would suggest, there are extensive research initiatives into the latter, but only limited investigations into the former. The experience gained here suggests that more extensive research and development into the application of systems analysis approaches in dam safety will benefit the mechanics research initiatives by highlighting the real analysis needs of the retrofit decision-making process.

Should one adopt the definition of judgement given above, resolution of the difficulties outlined here will be a pre-requisite for sound transparent judgements concerning seismic retrofitting of dams in portfolios where needs and benefits of further improvements are not patently obvious. Otherwise, it will be necessary to continually improve the seismic withstand capability of dams, not because the improvements can be shown to be necessary and beneficial in terms of risk control, but because it is impossible to demonstrate that the risks are not intolerable and that the benefits of further risk reduction are not grossly disproportionate to the costs.

REFERENCES

Andersen, G., L.E. Chouinard, C.Y. Bouvier, and F. Abdo (1998), *Condition Assessment Methodology for Embankment Dams*. Report submitted to US Army Corps of Engineers and Hydro-Québec.

Beak, C., J.W. Findlay and D.I. Aikman (1997), "Experience of failure mode, effect and criticality analysis on UK hydropower schemes", *Proceedings of Hydropower '97*, pp 369-376, Balkema.

BC Hydro, Internal memorandum (1993), "Ruskin Dam Deficiency Investigations, Seismic Ground Motion Parameters".

British Standards Institute (December 1991), *BS 5760, Reliability of systems, equipment and components, Part 5, Guide to failure modes, effects and criticality analysis (FMEA and FMECA).*

Canadian Standards Association (1991), *CAN/CSA Q634-M91, Risk Analysis Requirements and Guidelines*.

Dam Safety Interest Group (1999), *A Guide to Dam Risk Management (Part I)*, Canadian Electricity Association.

Henley, E.J. and H. Kumamoto (1992), *Probabilistic Risk Assessment*, IEEE Press.

Jones, J.C. (1999), "An Independent Consultant's View on Risk Assessment and Evaluation of Hydroelectric Projects", *Proceedings of the International Workshop on Risk Analysis in Dam Safety Assessment*, Eds. J.T. Kuo and B.C. Yen, Water Resources Publications.

Jones, R.B. (1996), *Risk Based Management - a Reliability Centred Approach*, Gulf.

Lee, M.K., K.Y. Lum and D.N.D. Hartford (1998), "Calculation of the Seismic Risk of an Earth Dam Susceptible to Liquefaction", *Geotechnical Special Publication No. 75*, ASCE, Geo Institute, Dakoulas, Yegian and Holtz (Eds.), Vol. 2, pp. 1451-1460.

Lin, J.S. and T.K. Hung (1999), "A Procedure for Seismic Risk Analysis of Earth Dams", *Proceedings of the International Workshop on Risk Analysis in Dam Safety Assessment*, Eds. J.T. Kuo and B.C. Yen, Water Resources Publications.

Stateler, J., J.L. Von Thun, G. Scott and J. Boernge (1995), "Development of Performance Parameters for Dam Safety Monitoring", *Dam Safety '95*, pp. 523-532, ASDSO.