Introduction

In the foreword to the Malaysian Guidelines for Operation, Maintenance and Surveillance of Dams (Malaysian Inter-Departmental Committee on Dam Safety 1989), it is stated “The expanding inventory of dams has brought into focus the subject of dam safety”. At the time of the guideline publication, there had been a considerable increase in the inventory of dams with those constructed during the previous 10 years accounting for 90% of the total storage. The Bakun Dam alone, which is due for completion in 2010, will more than double the current storage capacity. This, together with a number of other dams under design or construction within Sarawak, is a significant structure within the world context of large dams, which again stresses the need for dam safety. The safety of a dam covers all stages in the life cycle commencing with the inception stage through the planning and design stages followed by the construction and commissioning, ongoing operation and maintenance and surveillance and in certain cases decommissioning.

1. Background

Throughout history, dams built to store water have occasionally failed with the resulting loss of life, social, economic financial and environmental losses. Failures have involved dams built without application of engineering principles, but have also involved dams built to accepted engineering standards of design and construction at the time. The technology of dams has improved with the increased knowledge of design principles and of the characteristics of foundation and dam materials, and it is generally agreed that safe dams can be built and existing dams can be safely maintained with proper application of current technology.

According to FEMA (1979), the goal of making dams “as safe as practical” implies a limit to maximum reasonable effort. It must be recognized that no dam can ever be completely “fail-safe” because of incomplete understanding of or uncertainties associated with natural (earthquakes and floods) and manmade (sabotage) destructive forces; with materials behavior and response to these forces; and in control of the construction process or in human error associated with the operation and maintenance of a dam. Dam safety management must, therefore, ensure that uncertainties are properly balanced with competent technical judgment. The overall purpose of Dam Safety Guidelines and any associated Legislation is, therefore, to enhance national dam safety. The immediate objective is to encourage high safety standards in the practices and procedures used by regulating agencies or designers and owners for dam site investigation, design, construction, operation and maintenance, and emergency preparedness.

As safe as practical may be related to As Low as Reasonably Practicable (ALARP) in the emerging risk assessment approach being used for evaluation of upgrade works where risk is defined as “The measure of the probability and severity of an adverse effect to life, health, property, or the environment” (ANCOLD 2003). In consideration of ALARP, the following statements apply:

- “Risk is tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained” and
- “Residual risk is tolerable only if further risk reduction is impracticable or requires action that is grossly disproportionate in time, trouble and effort to the reduction in risk achieved”.

The level of risk is reduced within the ALARP region by consideration of the effect of the remedial options on the various failure modes with respect to their likelihood of occurrence and the consequence of failure from which the risk is calculated as the product of likelihood and consequences for all failure modes and hazards affecting the structure being evaluated. At the present stage of development, the use of risk assessment in reaching a conclusion on the safety of a dam is seen as an enhancement to the traditional Standards based approach (ANCOLD 2003) and is not an alternative or the sole basis for decision making.

A dam safety management program is, therefore, a system that incorporates dam safety values as part of the culture of the organisation and the day-to-day operation of a dam and comprises policies, procedures and investigations which minimise the risk of dam failure. The benefits of a functional dam safety management program (NRM 2002) are as follows:
The owner is aware that the dam complies with current engineering standards for safety
- The owner is assured that the dam is operated in a safe manner
- The owner has the condition of the dam assessed on a regular basis
- The owner is prepared for an emergency situation at the dam
- The risk of dam failure is minimised.

The objective of dam safety can be achieved as management and technical decisions during all project stages give proper recognition to safety considerations, whether by use of traditional standards approaches, or using the risk assessment approaches to enhance the decision making processes.

2 Understanding Dams and Failure Modes

Dam safety is governed by an understanding of the potential failure modes and methods of dealing with these during all phases of the design, construction and operation of the dam in order to minimise the likelihood of occurrence. There are practical limitations on the amount of physical data that can be obtained during planning and design. Furthermore, judgment and extrapolation are necessary to assess foundation conditions and to design an appropriate structure and experience is essential in applying these judgments and understanding how failure modes can occur.

According to Foster et al (1998), there have been 63 embankment dam failures since 1950, for which the percentage of the failure modes were as follows.

- Overtopping 40.5%
- Inadequate spillway capacity 32.0%
- Spillway gate failure 8.5%
- Piping 54.5%
- Piping through the embankment 35.5%
- Piping through or into the foundation 19.0%
- Other causes including earthquake 4.5%

A Failure Modes Effects Analysis (FMEA) is commonly undertaken as part of a dam safety review or may be used in certain instances of design when dealing with novel or unusual designs. The FMEA provides a structured approach for identifying the potential failure modes of the various components of the system being evaluated and the effects of the component failures on the performance of the system, eg the dam. The FMEA is always qualitative and can include a comparison with the available standards and prevailing practices at the time to determine whether the dam conforms to current practice with respect to a particular load condition and failure mode using the following matrix.

<table>
<thead>
<tr>
<th>Compliance categories for Standards Based Assessment of Dam Safety</th>
<th>Sufficient Information is available to make a definitive assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>The dam is assessed to conform with current practice with respect to the particular loading condition</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The benefits of carrying out a FMEA are:
- The analysis increases the understanding of the entire system by identification of all of the components and their respective failure modes;
- Provides a sound basis for identifying deficiencies as well as for concluding that failure modes have been “designed out” of the system and cannot lead to a failure sequence;
- The analysis focuses on the functions of the components and the relation of the component functions to the entire system;
- The analysis includes extreme hazards and hazards associated with normal operation;
- Readily provides information on the significant contributors to system failure and on deficiencies in information, as indicated in the above table.
- The results can be used to prioritise rehabilitation and upgrade works;
- Can be used to provide an understanding of the overall failure mechanism as the basis for development of fault trees and event trees;
- The analysis provides documentation that due care has been taken in the evaluation of the system with respect to safety and operation.
The fundamental steps in completing a FMEA are as follows (Adapted from ANCOLD 2003):
- Define the system (eg HEP) and any sub-systems, which do not overlap in function; such as, RCC dam, power intake, powerhouse, outlet works, reservoir etc;
- Define the components of each sub-system, to ensure that all components are clearly identified and numbered;
- Provide the design function (s) for each component. Where applicable, operating details would be provided;
- Identify causes of the failure modes and operating conditions under which the failure can occur; that is, hazards of flood, earthquake, normal operation, etc;
- Identify failure modes;
- Identify the effects of the component failure on the system considering local and global effects;
- Identify failure detection methods; that is, alarms, warning systems, etc;
- Identify compensating or mitigating provisions including isolation and redundancy;
- Assign the severity classification (if criticality is not being performed) which is a qualitative statement of failure significance with levels from minor to catastrophic or may be the compliance with the standards bases described above.

At completion of the FMEA, the results should be reviewed and the analysis results documented in such a way as to provide the relevant information for which the analysis was carried out. A typical tabular form for the FMEA is as follows.

<table>
<thead>
<tr>
<th>Component</th>
<th>ID Number</th>
<th>Primary Function</th>
<th>Auxiliary Functions</th>
<th>Failure Modes</th>
<th>FM No</th>
<th>Causes</th>
<th>Failure Effect</th>
<th>Failure Detection</th>
<th>Mitigating Action</th>
<th>Severity/Compliance</th>
</tr>
</thead>
</table>

If sufficient information is available, the analysis can also be extended to determine the likelihood and consequences of component failure from which the criticality is obtained and is called a Failure Modes Effects and Criticality Analysis (FMECA).

3 Uncertainty in Dam Safety

There are a considerable number of uncertainties associated with dams, with some of the reasons being as follows (Kreuzer 2005):
- Each dam is unique and finding useful reference from other dams of its kind is difficult for a reliable diagnosis of symptoms of unusual behaviour;
- Dams are complex structures with the two major elements being (1) the foundation and (2) the man-made. The intricate interaction between these two parts adds to the level of uncertainty and it is usually the foundation, which generally turns out to be a weaker link for predicting performance;
- Compared with other civil structures, dams are, to a larger extent, more exposed to the variability in nature (geology, floods, earthquakes, climatic changes).

Three different types of uncertainty pervade dam safety decision-making, as follows (Hartford 2001).
- Aleatory uncertainty - inherent randomness, natural variation, or chance outcomes in the physical world;
- Epistemic uncertainty - lack of data, lack of knowledge about events and processes that limits our ability to model the real world; and
- Decision-model uncertainty - the inability to understand decision objectives, or at least, how alternative projects or designs should be evaluated. This uncertainty includes, for example, uncertainty in policy-related issues such as, corporate values and government objectives, economic climate etc.

Each of these uncertainties has an impact on dam safety and any risk related issues for either new or existing dams. Hartford et al (Hartford 2001), state that the approach chosen to address risk issues must be related to the nature of the decision, the context in which the decision is to be made, and the level of societal concern engendered by the risk issue. Figure 1 shows the proposed “decision context” for risk issues that can be broadly divided into three categories A, B and C, which are defined below. The “decision-context” classification system is dynamic and decision issues can move from one category to another as a result of technological changes, scientific advances, or changes in public perception.
Category A is applicable to “routine” risk management situations for dams where the application of codes and standards is appropriate. An example of the Category A decision context could relate to the operation, maintenance, and testing of spillway gates;

Category B relates to those situations that are less “cut and dried” but where there is general guidance concerning how to implement risk controls, with certain aspects of the risk that are unique to the situation at hand: some uncertainty surrounding existing practices; costs of implementing best practice can be extremely high; risk raises some societal concerns. Decisions in this category include retrofitting old dams to new standards which constitute current authoritative good practice.

Category C can be related to the more complex safety decisions, where the public interest and/or the environment are of paramount importance but where it is necessary to make significant trade-offs between benefits and risks. The risk control measures can be expected to be novel and potentially extremely costly for the risk reduction benefits gained. Societal interest and involvement are potentially high requiring a participatory role for the public. An example is retrofitting dams to meet new safety requirements that have not achieved the status of authoritative good practice.

The “decision context” provides a clear indication of the areas requiring the application of codes and standards, good practice, engineering judgement and those which may involve risk assessment techniques and societal involvement in the application of Dam Safety.

4 The Use of Guidelines
Guidelines are used to describe definite management practices to reinforce decision-maker awareness of safety needs. Those charged with administering the guidelines must recognize that the achievement of dam safety is through a continuous, dynamic process in which guidelines, practices, and procedures are examined periodically and updated. Technical procedures need to change with technological advancement, and management should ensure that observed deficient practices are corrected and that successful practices are duplicated (FEMA 1979).

Guidelines should be treated as guides and any unusual dam safety requirements should be approached using the application of the “decision context” described above. The following statement is made in the preface to the Malaysian Guidelines on Operation, Maintenance and Surveillance of dams “as these guidelines are of a general nature, they are intended to be used as a general guide for drawing up specific procedures and practice to suit site and management conditions of individual dams”. Where Legislation is in place relating to the use of the Guidelines, which may be treated more as a standard, then it is imperative that dam owners and designers consult with the regulatory body when design, operation or maintenance decisions fall outside of the guidelines in the Category B or C decision context described above.

5 Safety in Design
5.1 What is Safety in Design
Safe design is a process defined as:

“The integration of hazard identification and risk assessment methods early in the design process to eliminate or minimise the risks of injury throughout the life of the product being designed.” (GHD 2009)
A safety in design approach begins in the conceptual and planning phases within a design’s lifecycle, with an emphasis on making choices about design, materials and methods of manufacture or construction, to enhance safety. The designer needs to consider how safety can best be achieved in each of the lifecycle phases i.e. designing a building with a lift for occupants, where the design also includes sufficient space and safe access to the lift well or machine room for maintenance work.

Safety in design is part of a broader range of design objectives, including practicality, aesthetics, cost and the functionality of the plant, building or structure. A safety in design approach involves successfully achieving a balance of these sometimes competing objectives, without compromising the health and safety of those potentially affected by the plant, building or structure over its lifecycle.

A range of parties influence the design function at varying phases of the design process including:
- Design professionals such as architects, engineers, industrial designers;
- Other groups who make design decisions, such as clients, developers, builders, owners, job managers, health and safety professionals and ergonomics practitioners;
- Personnel who should work or be affected by the plant, building or structure;
- Suppliers (including manufacturers, importers, plant-hire), constructors, installers and trades/maintenance personnel;
- Government regulators and inspectorates.

Where safety in design principles are included within legislation, this means that it is no longer sufficient to assume that compliance with a code or standard is enough. Designers need to demonstrate that they have identified the risks in their design and where a particular code/standard is not appropriate to eliminate these risks; a systematic risk based approach should be used to determine the right solution.

5.2 What does this all mean to designers?
In complying with the requirements of safety in design legislation (where applicable), designers are to consider:
- Which risks are within their scope and control;
- Client Interaction – the risks being addressed generally relate to the client’s site and staff, and therefore the client needs to be involved in the process, i.e. direct input into risk identification (including workshops) and risk reduction/management;
- A systematic and formalised approach should be adopted to managing risks dependant on the type of risks;
- Where it is not reasonably practicable to eliminate a risk associated with a design’s lifecycle, then the risk should be reduced so far as reasonably practicable.

5.3 Safety in Design Approach
The approach used for safety in design is as follows (GHD 2009):
- Establish the context for the design - Confirming how all job stakeholders should work together is an integral part in establishing the risk management process;
- Forseeable uses of the design – the designer should identify the client’s main objectives and outcomes of the design. This information is important to establish the intended and foreseeable uses of the design;
- Safety in Design Risk Assessment – This should be developed and updated regularly during the design. All safety related decisions, including justifications for why Potential Control Measures are not selected, should also be included within the Safety in Design Risk Assessment;
- Communicate and Consult - Consult with the client/end user at all stages of the design for effective management of risks and decisions on the implementation of control measures.

The Safety in Design Risk Assessment is a means by which residual risks that have been treated so far as reasonably practicable can be communicated to all parties at the end of the design. Appropriate procedures or processes should be implemented in the workplace to deal with the ongoing management of the residual risks.

6 Dam Safety during Construction
Compliance with the design intent during the implementation of a scheme is essential for dam safety and ongoing involvement of the designer in the construction, either as an adviser, reviewer or resident staff is highly desirable and has not always occurred in the past leading to dam safety incidents, failures or potential deficiencies where the designers intent has not been fulfilled in the construction of the structure. There is always the danger in believing that the design report, specifications and drawings can fully impart the understanding and design intent of the designers, whose role is often curtailed at the completion of these documents.
Construction is a critical phase in achieving a safe dam. Any project must be continuously evaluated, and "re-engineered" as required, during construction to assure that the final design is compatible with conditions encountered during construction. Quality of construction is also critical to safety. Deficiencies in materials or construction practices can occur during all stages of the construction, and constant vigilance is necessary to prevent them. Sampling and testing at a completed project cannot be relied on as an effective substitute for inspection and quality control during construction.

Furthermore, the various methods of procurement (FIDIC Red and Yellow Book, EPC, EPCM, etc) allow for varying levels designer and owner involvement in the decision making during the design and construction for which appropriate conditions of contract and review are essential to mitigate the likelihood of critical failure modes being overlooked or dismissed in the construction process. To this end, Review Boards or Panels of Experts provide valuable input to the design and construction phases where they are able to provide advice independently from the designer and contractor with respect to shortcomings and ways of dealing with these.

During construction, apart from the on site contractor's Health and Safety (HSA) requirements, the most significant risks are presented by slope stability issues, flooding and diversion requirements for which appropriate standards and construction requirements are required to ensure that the downstream population at risk and the contractor are working within an acceptable risk. This has been clearly demonstrated in the development of the diversion works design example discussed as follows.

6.1 Diversion Flood Risk
The diversion works for the Baleh Dam, which has a height above foundation of about 220 m, comprise two 12 m diameter horseshoe tunnels with an upstream and downstream coffer dam for protection of the works area. There are two approaches to the selection of the flood recurrence required for the design of the river diversion final crest level.
- Precedent based on experience on similar sized projects; or
- Risk based using the evaluation of the likelihood of failure during the works and the economic and life loss potential in the event that the failure of either the coffer dam or the man dam occurs. The application of this method requires breach analyses to be carried out and economic evaluation as well as life loss estimates to be made.

In the case of the Baleh dam, the selection of the diversion flood recurrence interval was based on precedent where a 1 in 50 AEP event was used for a RCC main dam and 1 in 100 AEP flood for a CFRD or ECRD main dam option. The design of the coffer dam was, however, based on an evaluation of the risk posed by the overtopping failure mode for a RCC coffer dam or a central core rockfill coffer dam by calculating the probability of the coffer dam being overtopped during the construction period, as shown on Table 1. This table shows that the potential for overtopping the coffer dam is about 1 in 50 during the construction period. There are a number of longhouses in close proximity to the dam for which the dam break from the sizes of coffer dams that are being considered, up to 50 m high, would result in a peak discharge in the order to 80,000 m$^3$/s at the dam reducing to about 63,000 m$^3$/s at the first longhouse located at 12 km downstream from the dam, as shown on Figure 1. The hydrograph shown on Figure 1 indicates that the flood level will rise approximately 25 m within 2 hours at this location.

<table>
<thead>
<tr>
<th>Elevation (m asl)</th>
<th>Flood Event AEP</th>
<th>Construction Period to reach Elevation (months)</th>
<th>Total Construction Time (Including 6 months river bed excavation) (Months)</th>
<th>Likelihood of Exceeding Elevation (%)</th>
<th>Equivalent AEP (1/Likelihood%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFRD Dam (Coffer Dam Crest Level 87.7 m)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87.7</td>
<td>100</td>
<td>18</td>
<td>24</td>
<td>2.00</td>
<td>1.99%</td>
</tr>
<tr>
<td>90.0</td>
<td>135</td>
<td>19</td>
<td>25</td>
<td>2.08</td>
<td>1.54%</td>
</tr>
<tr>
<td>98.0</td>
<td>380</td>
<td>21</td>
<td>27</td>
<td>2.25</td>
<td>0.59%</td>
</tr>
<tr>
<td>134.0</td>
<td>8500</td>
<td>30.5</td>
<td>36.5</td>
<td>3.04</td>
<td>0.036%</td>
</tr>
</tbody>
</table>

The incremental downstream flooding will continue at about 20 m depth for a distance of 50 km downstream from the dam and thereafter there is a linear reduction to the downstream port of Sibu where the increase in depth is less than 300 mm. The flood level rise of 300 mm is considered to have no impact in terms of
identifying people at risk. As shown on Figure 1, the flood level rise will take about 85 hours before overtopping the embankment starts, which will allow a significant amount of time to issue flood warnings to the downstream population at risk as the flood level rises to critical levels for warning of an impending dam failure using an Emergency Response Plan. This will reduce the potential consequences of failure with respect to life loss, however, in order to reduce the likelihood of the overtopping failure occurring, it was recommended that the coffer dam be constructed using RCC as this will allow overtopping with a significantly lower probability of failure.

Figure 1 Baleh Dam Embankment Coffer Dam Overtopping Breach Hydrograph

7 Dam Safety Management during operation

The owner of each dam is responsible for its safety and the objective of dam safety management is to protect life, property (eg community infrastructure, dam) and the environment from the failure of any dam. This objective can be achieved by implementing, and maintaining, an appropriate dam safety program. The principal activities of a dam safety programme as shown on Figure 2 are design, construction, operation and maintenance, surveillance, safety review, remedial action, education and training and emergency preparedness (ANCOLD 2003).

7.1 Operation and maintenance

The life of a dam may extend beyond a hundred years. Dams are subject to the ageing process and changing natural forces and there is a need to keep a constant vigilance on these structures to ensure that their safety is not compromised. The notion that once a dam is built and operational only minor maintenance work is necessary is a fallacy, which can lead to a dangerous consequence. On the contrary, operation and maintenance of a dam should be a properly organised activity based on sound engineering procedures and practice (Malaysian Inter-Departmental Committee on Dam Safety -1989). Operation and maintenance manuals and procedures are, therefore, required for ensuring the health of the structures is maintained on an ongoing basis.

Figure 2 Elements of a Dam Safety Program (ANCOLD 2003)
7.2 Surveillance

Following commissioning and during operation, the dam structure and associated works will respond to the loads including normal loads and more extreme loads resulting from floods, seismic, temperature and winds. The Prime objective of the Surveillance system is to analyse and present data on the response of a dam and its environs in order to ensure adequate warning of any unsafe trends in the behaviour of the dam. As shown on Figure 3, this entails monitoring, together with visual inspections, checking and testing of instrumentation followed by reporting and analysis of the data to understand the structural response to these loads for an overall assessment of the safety of the structure.

The inspections may include:
- Routine visual inspections by operating personnel as part of their duties at the dam. These inspections may be daily to weekly, depending on the hazard or significance of the structure. The routine inspections are one of the most important activities in a dam surveillance program and are used to identify and report on deficiencies by visual observation of the dam;
- Routine or Periodic Dam Safety Inspection by an inspector, other than the operator in which deficiencies are identified and reported on for corrective actions by structured observation of the dam and surrounds;
- Comprehensive inspection carried out by dams engineer and specialists (where relevant) to identify deficiencies in the dam safety management programme and the structure by a thorough onsite inspection; equipment testing, evaluation of dam safety management documentation, surveillance data; and by applying current criteria and prevailing knowledge;
- Special Emergency Inspections carried out by Dams Engineer and Specialists to examine a particular feature of a dam for some special reason (e.g. after earthquakes, heavy floods, rapid drawdown, emergency situation) to determine the need for pre-emptive or corrective actions.

The frequency of inspections should be established by taking into account the consequences of dam failure, the level of risk at the dam, the type and size of the dam and the value of the dam to the dam owner and the community. More frequent inspections may be necessary where a dam is known to have some form of deficiency.

As shown on Figure 3, the Institutional Memory of dam owners varies throughout the lifetime of a dam, which can adversely affect the quality of surveillance activities and indeed all aspects of Dam Safety Management. While many of the “older dams” have little or no documentation on the original site exploration, design, construction, and past operation, newer dams generally have a significant build up of knowledge during the design and construction stage and initial documentation, which ideally should continue to grow with the dam. This is often not the case and people leave, data is lost or training and passing on of knowledge is inadequate and knowledge only increases, a shown on Figure 3, at times where significant events occur or remedial works are carried out or major dam safety reviews are completed. Hence, it is important for the Dam Safety Program to include the aspects of Education and Training and information management to ensure as far as possible that the various aspects of the program are maintained. In particular, training of personnel responsible for the inspections is important to ensure that deficiencies are identified.

7.3 Monitoring

Dam monitoring requires checking and recording of the performance and behavioral trends of a dam and appurtenant structures by direct measurement, observation and measuring with devices or instruments that provide data from which performance and behavioural trends are established. The frequency of monitoring
should be determined by taking into account the consequences of dam failure, the level of risk at the dam, the type and size of the dam, and the value of the dam to the dam owner and the community. The higher the hazard and risk, the more frequent the monitoring (ANCOLD 2003). The instrumentation may be read manually or electronic equipment with data logging or telemetry can be provided for enhancing the realtime performance monitoring and setting of alarm limits for abnormal behaviour. Technology does not, however, replace visual surveillance and electronic data should be compared regularly, where possible, with manual readings to check data quality.

There are two approaches that may be used by the design engineer or dam safety review engineer for assessing instrumentation requirements for a structure:
- a prescriptive approach based on precedent, Guidelines or a knowledge of the dam performance based on the design analyses; and
- an alternative risk-based approach.

ANCOLD (1983, 2003) provide guidance on a prescriptive approach for identifying the recommended instrumentation and frequency of reading. An alternative risk-based approach can be used Smart (2006) based on a decision tree and involves a five-step process, as follows:
- Brainstorming of potential failure modes;
- Review of the visual monitoring program;
- Evaluation of each instrument or array of instruments using a decision tree;
- Review of the potential failure modes following evaluation of the instrumentation to ensure adequate coverage; and
- Review and adjustment of the monitoring program, including monitoring frequency and need for additional instrumentation, based on the outcomes of the first four steps.

A summary of the decisions based on the USBR guidelines given in Smart (2006) and their background are summarised below.
- **FM of concern** – Is the potential failure mode considered to be of practical concern for this dam? Is the failure mode considered to have a likelihood of occurrence high enough to warrant monitoring?
- **Direct measure of FM** – Is the measurement a direct (or significant indirect) measure of a potential failure mode? The most effective way to monitor potential failure modes is by direct measurement of the effects of their development. For example, monitoring of turbidity of seepage flows provides a direct measure of piping.
- **Unnecessarily redundant** – Is the measurement unnecessarily redundant to other measurements or visual observations? Can visual observations or other instruments provide better monitoring of the potential failure mode? For high risk failure modes, redundant monitoring of failure modes may be beneficial.
- **Useful** – Are the measurements useful in monitoring a potential failure mode? Instruments which do not provide a direct measure of a failure mode may still be useful in providing information for research purposes, but not specifically on the performance of the dam. This may include instrumentation which was installed for a specific purpose such as monitoring during first filling.
- **Adequate to monitor FM** – Are the measurements adequate to monitor the potential failure mode in conjunction with visual monitoring? The coverage provided by and/or precision of the instrument under consideration must be reviewed to ensure that adequate information is available to monitor development of failure mechanisms. It may be necessary to identify additional instruments/observations to augment the monitoring program.
- **Reliable** – Is the instrument providing the reliable measurements for use in monitoring a potential failure mode?

For failure modes where there is inadequate instrumentation coverage, additional measurements or observations must be identified. Where additional instrumentation is required, a second decision is used to assist in the process, as presented on Figure 4. The decisions for evaluating additional instrumentation and the basis of the decision are summarised as follows:
- **FM area can be precisely located** – Can the location for development of the failure mode be precisely located? It is critical that new instrumentation is installed in a location where it will provide information on the development of a failure mode.
- **Installation likely to induce failure** – Is installation of the proposed instrumentation likely to lead to failure of the structure? This decision is central to the “Do No Harm Philosophy” discussed in Smart (2006). The potential for damaging the structure through the installation and the benefits provided by the instrumentation must be considered.
7.4 Safety Reviews
A Safety Review is a procedure for assessing the safety of a dam, and generally comprises a detailed study of structural, hydraulic, hydrologic and geotechnical design aspects and of the records and reports from surveillance activities as well as a review of the dam safety management documentation. The integrity of a dam is assessed for known failure modes and mechanisms in terms of safe acceptance criteria (engineering standards, dam safety guidelines) or risk management criteria where these are being used.

In general, periodic Safety Reviews at 20-year intervals are considered appropriate, however, this may be changed to account for:
- A deficiency or weakness identified during the surveillance program or by other means
- The age of the dam;
- Changes in standards, acceptance criteria or technology;
- Changes in arrangements at the dam;
- A requirement by a higher authority or regulator.

8 Dam Safety Preparedness
The standards used for design, construction, operation, maintenance and surveillance of dams are intended to minimise the risk of dam failure. However, as unusual circumstances or observed deficiencies at the dam could result in dam failure, dam owners need to identify conditions which could lead to failure situations and which may require dam safety emergency planning.

A failure of the dam or associated structure will result in downstream impacts, which may vary between little impact to an extreme impact. The failure impact defines the requirements for monitoring and surveillance while an Emergency Response Plan (ERP) covering potential dam safety incidents or failure scenarios is essential to minimise the risk and appropriate plans should be developed and tested. An Emergency Response Plan (ERP) is a formal plan (ANCOLD 2003) that:
- identifies emergency conditions which could endanger the integrity of the dam and which require immediate action;
- prescribes procedures which should be followed by the dam owner and operating personnel in the event of an emergency;
- provides timely warning to appropriate emergency management agencies for their implementation of protection measures for downstream communities.

Embarkment dams can be expected to fail more slowly than concrete structures and failure times for fill dams have varied from a few hours to several days, while concrete dams have been known to fail almost instantaneously. Assuming that no previous adverse trends have been noted in the dam surveillance, the guarding of a dam would require round the clock inspection to ensure the maximum time for evacuation of people in time of emergency. Instrumentation and telemetry may go a long way to providing this information, however, in times of extreme flood or earthquake, the likelihood of telemetry equipment functioning properly
and the message being delivered to the appropriate personnel for taking action is expected to be low and due cognisance of this must be taken when developing the ERP.

Flood emergency planning for communities below dams is the responsibility of Emergency Management Authorities, not dam owners. Dam owners have a responsibility to assist emergency management authorities with the development of warning systems and plans for the protection of those communities, however, the existence of warning systems and flood emergency plans does not absolve a dam owner from the responsibility to protect the structure ie warning systems and plans are no substitute for structural upgrading (Haines 1995)

9 Conclusions
The safety of a dam covers all stages in the life cycle and the owner of each dam is responsible for its safety for which the following statements are pertinent:
- We are living in a litigious world for which safety requires more than just following codes or standards;
- The “best” sites for dams have all but gone in a number of countries and safe designs are required for larger and larger structures on second choice sites;
- Populations are increasing and urban areas are expanding into flood prone areas of new dams or older dams previously on the outskirts of major cities or communities.

These issues emphasise the importance of dam safety at all stages of a dam’s life and the need for managing the safety of new and existing dams using a structured Dam Safety Management Programme.

References
1 ANCOLD (1983) Australian National Committee on Large Dams. Guidelines for Dam Instrumentation and Monitoring Systems
2 ANCOLD (2003) Australian National Committee on Large Dams, Guidelines on Dam Safety Management
4 GHD (2009), Health and Safety Procedure, Safety in Design, January 2009
6 Hartford et al, Handling Uncertainty in Dam Safety Decision Making, 21st USDS Annual Meeting, 2001, D.N.D. Hartford, R.A. Stewart
8 Kreuzer H (2005), Assessing Uncertainty in Dam Engineering, ICOLD, 73rd Annual Meeting May 2005
9 Malaysian Inter-Departmental Committee on Dam Safety (1989), Guidelines for Operation, Maintenance and Surveillance of Dams, October 1989

Malcolm Barker graduated with a BSc Civil Engineering from the University of Natal Durban South Africa. Malcolm has over 33 years of civil engineering experience in the design, construction and safety of dams, hydropower projects and canals. He has participated in many dam projects in Australia, Canada, Zimbabwe, South Africa, Malaysia, Papua New Guinea and China. He has been involved in the design of Embankment, Rockfill, RCC and concrete dams and power stations and has successfully played the role of Technical Team Leader in the prefeasibility and feasibility design of the Baleh HEP and the prefeasibility study of the Putai HEP, Serani HEP and Run of River HEP scheme in Sarawak, Malaysia. Malcolm has also served in different capacities in the Australian National Committee on Large Dams (ANCOLD).