Dams Safety Committee

NEW SOUTH WALES

DSC2D June 2010

DEMONSTRATION OF SAFETY FOR DAMS

Table of Contents

Item **Page**

1. INTRODUCTION

The *normal requirements* of the NSW Dams Safety Committee (DSC) are set out in its guidance sheets with its principal guidance sheet, *DSC Background, Functions and Operations - DSC1A,* outlining the DSC's general operations and authority.

This sheet (DSC2D) covers the means by which prescribed dam owners are to demonstrate that the failure risks posed by their dams meet DSC requirements. Dam owners, and their professional advisers, have full responsibility to determine, and put in place appropriate actions and programs to ensure the ongoing safety of their dams. The purpose of this guidance sheet is to provide the owners of prescribed, or proposed, dams with general advice on good dam safety practice, along with specific advice on their responsibilities and the requirements of the DSC in this area.

The DSC Safety Goals and Key Requirements (Section 2) at the start of the sheet are a summary - the whole sheet is to be read for a proper understanding of DSC considerations on demonstrating the safety of dams. Sections 1 to 4 inclusive are directed to dam owners, managers and other non-technical stakeholders. The remainder of this sheet is directed to professional people experienced in dam engineering, safety management or related specialized fields.

2. DSC SAFETY GOALS & KEY REQUIREMENTS

2.1 DSC Safety Goals

The primary goal of the DSC for prescribed dams is that they meet the DSC safety requirements set out in this and other sheets. Secondary goals are:

- risks to community interests are identified and assessed, are properly managed, are reduced when necessary and are kept under review throughout the life of a dam;
- risks to public safety meet the DSC *public safety risk guidelines* (*Background to DSC Risk Policy Context* - DSC1B - Section 2, under Principle D.3);
- other risks with a potential for an adverse effect on community interests meet criteria set by the owner and agreed with the DSC;
- needed safety improvements are undertaken *as soon as reasonably practicable*, in a way that best serves community interests;
- the DSC approach will facilitate a whole of Government approach to public safety.

The goals of a dam owner are however wider than those of the DSC and extend to such aspects as business interests, owner's continued viability and discharge of the owner's common law duty of care. Nevertheless, it is for the dam owner to determine how the DSC's goals will be achieved and to demonstrate to the DSC that they are achieved or will be achieved following appropriate action(s). The following sections of this sheet aim to provide guidance and direction to assist owners in achieving the DSC's goals.

2.2 DSC Key Requirements

This section summarises the DSC requirements outlined in this sheet.

The process for demonstration of safety

1. Safety of a dam is normally to be demonstrated by a *safety review* which follows the process set out in Figures 3 to 5. Owners need to make a case to the DSC to vary the process (Sub-section 4.6).

What is the role of the *Surveillance Report* in demonstration of dam safety?

1. A s*urveillance report* is to conclude, on the basis of present knowledge, that the dam fits one of these descriptions:
   - the dam clearly meets DSC requirements (documentation in support of this conclusion must exist); or
   - the dam clearly does not meet DSC requirements; or
   - the safety status of the dam is uncertain (Sub-section 5.1);
2. The sheet *Surveillance Reports for Dams (DSC2C)* requires that the *Surveillance Report* say whether a *safety review* is essential to determine the dam's safety status (Sub-section 5.1).

How is the safety of a dam to be established?

1. For a dam older than fifteen years in its existing configuration, an owner is normally required to undertake or update a *safety review* to establish its safety status. For dams less than fifteen years old in the present configuration, a *design report, construction certificate* and *construction report* would normally be accepted in lieu of a *safety review* provided these documents meet DSC requirements (Sub-section 6.1).

What is the scope of a *safety review*?

1. The scope of a *safety review* is to be determined by the dam owner but should address any issues of interest to the DSC (Sub-section 6.3).

When is a *safety review* required?

1. A *safety review* is required whenever the safety of a prescribed dam is in question. Safety reviews are not required for Low consequence category dams. (Sub-section 6.4).

Who can do a *safety review*?

1. Persons who prepare *safety reviews* need to possess the qualifications, skills and experience to arrive at a sound conclusion on the safety of dams (Sub-section 6.5).

Is a peer review required?

1. For any *safety review* that is prepared for the DSC for an Extreme or High consequence category dam, there is to be an *independent peer review*. The peer reviewer(s) is to be a senior practitioner widely recognized for their knowledge and experience with the particular dam safety issues. The peer reviewer(s) is to provide the owner with a separate report (Sub-section 6.6).

Is a *hazard analysis* required?

1. The DSC *normal* requirement is that a new, updated or existing valid *hazard analysis* be part of a *safety review* (Sub-section 6.7).

Is *failure modes analysis* required?

1. A *failure modes analysis* is an essential part of a *safety review* of any High or Extreme *consequence category* dam, whether or not a *risk assessment* is to be undertaken (Sub-section 6.8).

Is standards-based analysis required?

1. In a *safety review* the status of the dam in terms of any recognized *standard* or *good practice*, including the appropriate *fall-back flood capacity*, is to be reported (Sub-section 6.9);
2. Compliance with traditional *standards* or *good practice* intended to assure long-term safety will provide an adequate demonstration of dam safety in the long-term subject to the DSC agreeing with the relevant analyses (Sub-section 6.9).

Is risk assessment required

1. Risk assessment is required by DSC where:
    - there are aspects not adequately addressed by traditional *standards* or *good practice* and those aspects are significant in assessing the safety of a dam; or
    - an owner wishes to demonstrate that less costly safety improvements, than those required by standards or good practice, would adequately protect public safety and community interests (Sub-section 6.11);

What general requirements are there for risk assessment?

1. The approach to *risk assessment* is to be that of ANCOLD (2003b). The generic approach is to conform to the national standard AS/NZS 4360:2004 (SA/SNZ 2004). The level of *risk assessment* is to be at least *detailed* and preferably *very detailed* (Table 6.1 of ANCOLD 2003b) – (Sub-section 6.12 of this sheet).

What potential failure scenarios are of interest to the DSC?

1. The DSC is interested in scenarios with a significant adverse effect on the interests of the community;
2. Scenarios involving the operation of a dam in the absence of a failure are not within the charter of the DSC;
3. Risks from failure scenarios with a potential for significant adverse effect on the interests of the community are to be separately aggregated for comparison with the DSC *public safety risk guidelines* (Sub-section 6.13).

What of the estimation of the probabilities of dam failures?

1. The estimation of failure probabilities is to comply with the mathematics of probability wherever practicable (Sub-section 6.14);
2. Account is to be taken of *human factors* for their effect on *probability of failure* (Sub-section 6.14);
3. *Risk analysis* is to capture the varying *probability of failure* during construction on a dam (Sub-section 6.14);
4. An owner is to provide an assessment of the degree of uncertainty of estimated *probabilities* (Sub-section 6.14).

What of the estimation of failure consequences?

1. Estimated *consequences* for review of the current safety of dams are to be based on existing development and known planned development in the near future. Estimated *consequences* for review of the safety of a post-improvement dam are to be based on projected future development (Sub-section 6.15);
2. A recognized methodology, calibrated to dam failure and flash flood experiences, is to be used to estimate the *potential loss of life (PLL)* from dam failure (Sub-section 6.15);
3. A method, calibrated to natural flooding (other than flash flooding) fatality rates, is to be used to estimate PLL for non-dambreak flooding (Sub-section 6.15);
4. For PAR greater than 10,000 the case is to be discussed with the State Emergency Service (SES) to see if the estimated PLL seems reasonable with regard to the time available for evacuation (Sub-section 6.15);
5. For monetary loss:
   - estimated *economic loss* is to be reported separately from any *financial loss* estimate (the two are not necessarily mutually exclusive);
   - *direct* and *indirect losses* are to be separately identified (the two are mutually exclusive);
   - for the preceding categories, both *total* and *incremental loss* are to be reported; and
   - if important issues are at stake, the estimation methodology is to be reviewed by an economist (Sub-section 6.15);
6. Persons qualified in the appropriate scientific disciplines are to undertake or review the estimation of environmental *consequences* of dam failure. Both *total* and *incremental environmental consequences* are to be reported (Sub-section 6.15);
7. Account is to be taken of *human factors* for their effect on *consequences* of failure (Sub-section 6.15);
8. *Risk analysis* is to capture the varying *consequences of failure* as construction on a dam proceeds (Sub-section 6.15);
9. An owner is to provide an assessment of the degree of uncertainty of estimated *consequences* (Sub-section 6.15).

For risk analysis, what information does DSC need?

1. For *risk analysis*, the essential information needed by the DSC is:
   - the inputs to the analysis and the evidence in support of them;
   - full documentation of the methodology followed or citation of the authoritative sources for the methods used;
   - the reasoning in support of the risk values throughout the analysis; and
   - the outputs of the analysis (Sub-section 6.16).

How will the DSC *public safety risk guidelines* be applied?

1. The *public safety risk guidelines* will be applied for existing dams as follows:
   - if the best estimate of *risk to the individual* is in the *negligible region* (less than one in a million per annum) – DSC does not require any further reduction of *risk to the individual*, though any obvious low cost improvements should be made and avoidable risks should be avoided;
   - if the best estimate of *risk to the individual* is in the *intolerable region* (greater than one in ten thousand per annum) – the *normal* DSC requirement is that *risk to the individual* be reduced as soon as reasonably practicable in a short-term and/or medium term improvement (Table 2 of DSC1B) to at least the *limit of tolerability*. Without improvement, the dam does not meet DSC requirements;

- if the best estimate of *risk to the individual* is in the *region of tolerability review* (between one in ten thousand per annum and one in a million per annum) and the owner has other dams with *intolerable risks* – the dam normally meets DSC requirements until all *intolerable* risks on the other dams have been eliminated.
- if the best estimate of *risk to the individual* is in the *region of tolerability review* (between one in ten thousand per annum and one in a million per annum) and the owner has no other dams with *intolerable risks* – the *normal* DSC requirement is that risk be reduced to the *negligible* level on a program agreed with the DSC unless the owner can demonstrate, to the satisfaction of the DSC, that a higher risk is *tolerable*. To be *tolerable*, the risk must be *ALARP* and the owner must demonstrate why it is tolerable to impose that level of risk on known persons. The urgency for improvement is significantly lower than for risks in the *intolerable* region (Table 2 of DSC1B). Without improvement, or a demonstration that the existing risk is *tolerable*, the dam does not meet DSC requirements.
- if the best estimate of *societal risk* is in the *negligible region* (Figure 1 of DSC1B) – DSC does not require any further reduction of *societal risk*, though any obvious low cost improvements should be made and avoidable risks should be avoided.
- if the best estimate of *societal risk* is in the *intolerable region* (Figure 1 of DSC1B) – the normal DSC requirement is that *societal risk* be reduced as soon as reasonably practicable in a short-term and/or medium-term improvement (Table 2 of DSC1B) to at least the *limit of tolerability*. Without improvement, the dam does not meet DSC requirements.
- if the best estimate of *societal risk* is in the *region of tolerability review* (Figure 1 of DSC1B) and the owner has no dams with *intolerable risks* – the *normal* DSC requirement is that risk be reduced to the *negligible* level on a program agreed with the DSC unless the owner can demonstrate, to the satisfaction of the DSC, that a higher risk is *tolerable*. To be *tolerable*, the risk must be *ALARP*. The urgency for improvement is significantly lower than for risks in the *intolerable region* (Table 2 of DSC1B). Without improvement, or a demonstration that the existing risk is *tolerable*, the dam does not meet DSC requirements.
- if the best estimate of *societal risk* is lower than the *limit of tolerability* and the estimated loss of life exceeds 1,000 (within the red box on Figure 1 of DSC1B) – the *normal* DSC requirement is that, for failure modes with an estimated loss of life in excess of 1,000, the dam comply with all relevant *standards* – including PMF capacity for dams without spillway gates or other discharge systems with a potential to malfunction – and with currently recognized *defensive design measures.* If improvement is needed it is to be made as soon as reasonably practicable. Without compliance the dam does not meet DSC requirements (Sub-section 6.17).

2. As a matter of prudence owners should consider the level of uncertainty attaching to the risks. As uncertainty increases, there is a case to reduce risks to levels somewhat below the risk boundaries [mentioned under the nine points above] in order to maintain the defensibility of their position (Sub-section 6.17);

3. For risk-based assessment, new dams or major augmentations are to comply with the DSC *public safety risk guidelines* (see DSC1B – Section 2, under Principle D.3) for those classes of dam according to similar rules to those for existing dams. Normally DSC would expect these dams to achieve *negligible* risk values because the marginal cost of extra safety is usually much less than for existing dams. Moreover, new dams are normally fully compliant with recognized *standards* and *good practice*, in which case a *risk assessment* is unnecessary (Sub-section 6.17).

4. For new embankment dams if it is reasonably practicable to meet the DSC *public safety risk guidelines* (under Principle D.3 of *Background to DSC Risk Policy Context - DSC1B*) during construction of dams they are to be met. If it is not reasonably practicable to meet the *public safety risk guidelines*, the DSC will accept a flood capacity, during those phases of construction with public safety at risk, in the range of the AEP 1 in 500 to 1 in 1,000 flood discharge on the basis of world practice provided the risks are *ALARP* (Sub-section 6.17);
5. For the modification of existing dams the objective is that risks to public safety during construction will not exceed the pre-existing risks. If it is not reasonably practicable to meet that objective, the risks are to be reduced *ALARP* (Sub-section 6.17);
6. For risks during construction, the DSC will judge the *ALARP* requirement against the principles of *prevention, control* and *mitigation (PCM)* as follows:
    - *prevention* – have reasonably practicable measures been taken to prevent failure of the partly completed dam? – the measures include coffer dams, diversion tunnels or channels, and reinforced rockfill to allow substantial overflow;
    - *control* – there is limited scope to control flood failures but there are steps that can be taken as a flood develops. For example, it is necessary to make the edges of partially completed lifts of reinforced rockfill safe against overflow. Having cranes, gabions and men available for this work is a necessary control measure; and
    - *mitigation* – the DSC requires a construction phase *dam safety emergency plan [DSEP]* that has an effective flood warning system, forecast inundation levels in the event of dam failure, effective communication systems and protocols for interaction with the emergency authorities and an effective evacuation and welfare plan to protect those at risk (Sub-section 6.17).

How do we know that public safety risks are tolerable?

1. The need to demonstrate that public safety risks are *tolerable* applies to only those risks within the *region of tolerability review* (Sub-section 6.18);
2. The key principles are:
    - to be *tolerable* a risk must be *ALARP*, it must provide a benefit to society, it must be properly assessed and managed, it must be kept under review and it must be further reduced if future circumstances allow;
    - for a risk to be ALARP, the *sacrifice* (Glossary to ANCOLD 2003b) required in its reduction must be *grossly disproportionate* to the risk reduction that is achieved [Sub-section 6.18];
3. A demonstration of the tolerability of risk requires consideration, definition and costing of the possible *options for risk reduction* (Sub-section 6.18);
4. In demonstrating that a risk is *ALARP* the owner is to consider at least the following factors:
    - The *disproportion* between the *sacrifice* (money, time, trouble and effort) in making the safety improvement and the *risk reduction* that is achieved.
    - the level of risk in relation to the *limit of tolerability* and the *negligible* risk level;
    - the *cost-effectiveness* of safety improvement options;
    - any relevant recognized *good practice*; and
    - any *societal concerns* revealed by the owner's consultation with the community and other stakeholders (Sub-section 6.18);

5. The DSC will not accept a case based on *cost to save a statistical life* alone as a demonstration that risks are *as low as reasonably practicable* [Sub-section 6.18];
6. Consultation with the affected community and other stakeholders (see *Community Consultation and Communication - DSC2I*) is a pre-condition for acceptance of a risk within the *region of tolerability review* as *tolerable* (Sub-section 6.18);
7. The owner is to demonstrate how each of *prevention*, *control* and *mitigation* has been addressed (Sub-section 6.18).

What risk criteria apply?

1. The owner is to develop *risk criteria* (Sub-section 6.19);
2. The owner's *risk criteria* are to at least satisfy these requirements:
    - the DSC *public safety risk guidelines* (DSC1B - Section 2, under Principle D.3);
    - where lives are not at risk or it is clear that public safety should not be the main driver for the safety levels of the dam, the *risk criteria* for economic loss, public health impacts, environmental impacts and any other adverse impacts on society are to be developed by the owner in consultation with representatives of the affected community. These criteria and the reasons in support thereof, are to be provided to the DSC (Sub-section 6.19).

What is the safety status of the dam?

1. For a *safety review*, a conclusion by the owner is required as to the safety status of the dam according to the table at Sub-section 6.20. The basis for that conclusion is to be documented (Sub-section 6.20);
2. *Safety reviews* provided to the DSC are to include a recommendation on the *priority* and *urgency* to be assigned to any safety improvement of the dam together with an indication of the next steps in planning for the improvement (Sub-section 6.20).

What documents does the DSC need?

1. The DSC requires:
    - a letter of transmittal issued under the authority of the dam owner and giving the owner's conclusion on whether or not the dam meets the DSC safety requirements. Where improvement of safety is required the owner is to make a commitment to the improvement and is to state the time horizon for implementation of the improvement;
    - the *safety review* report;
    - the report of the independent peer reviewer(s); and
    - a statement giving an account of the owner's response to the report of the independent peer reviewer(s) (Sub-section 6.21).

What of further actions?

1. An owner's conclusion that the dam does not meet DSC requirements requires:
    - *short-term* improvement – a proposal and program for any such improvement;
    - *medium-term* improvement – an indicative initial program for investigation activities;
    - *long-term* improvement – any useful indications that could be provided (Sub-section 6.22)

3. TERMINOLOGY

Appendix A sets out the terminology adopted for this sheet.

4. BACKGROUND

4.1 Developments in risk assessment

After reviewing the ANCOLD *Guidelines on Risk Assessment*, October 2003, DSC saw that there would be benefits from the introduction of a *risk-based approach* to the safety management of prescribed dams. The outcome is the NSW Government-endorsed *Background to DSC Risk Policy Context - DSC1B*. This sheet, *Demonstration of Safety for Dams - DSC2D,* provides guidance on the integration of a *risk-based approach* with the traditional *standards-based approach* in an owner's demonstration of dam safety.

4.2 The need for change

Early efforts to improve safety focussed on flood capacity with other aspects given little attention by comparison. Over time a better balance to review of safety has been achieved through such developments as the issue of a DSC guidance sheet and ANCOLD guidelines on earthquake safety and the work of the University of New South Wales on methods to assess the vulnerability of dams to internal erosion and piping.

Currently the review of safety is normally triggered by the recommendations of a *surveillance report*. This is a good process but:

- it results in review of different safety aspects at different times – an *ad hoc* approach – whereas modern safety management calls for a comprehensive review at a periodic frequency;
- *failure modes analysis* is not embedded in the current process;
- the DSC *public safety risk guidelines* do not feature prominently in the current process; and
- the current process has not integrated *risk assessment* with the traditional *standards-based approach*.

This guidance sheet aims to overcome these problems.

4.3 How dams become unsafe

A dam designed to recognized standards of safety may become deficient in safety over time because:

- The dam has deteriorated with age. Corrosion of metal conduits and alkali aggregate reaction (AAR) are examples;
- Knowledge of *hazards* has changed through an increasing database of events or improved understanding of the underlying physical phenomena. An example is the large increase in design flood estimates that occurred following the introduction in Australia of generalized procedures for estimation of *Probable Maximum Precipitation (PMP)* in the 1980s;

- Methods of analysis have changed as understanding improves. An example is the abandonment of a simple pseudo-static analysis of embankment dams for earthquake in favour of advanced methods of deformation and liquefaction analysis;
- Reservoir operating rules have changed. Safety is affected if the adequacy of a dam's flood capacity took account of prior reservoir volume (ANCOLD 2000a);
- Downstream development has changed; or
- Safety *standards* have changed.

4.4 Approaches to demonstration of safety

There are now two main approaches to the demonstration of safety:

- The *standards-based approach*; and
- The *risk-based approach* [commonly called *risk assessment*].

ANCOLD [2003b] defines the *standards-based approach* as:

The traditional approach to dams engineering, in which risks are controlled by following established rules as to design events and loads, structural capacity, safety coefficients and defensive design measures.

Risk assessment is defined as:

The process of reaching a decision recommendation on whether existing risks are tolerable and present risk control measures are adequate, and if not, whether alternative risk control measures are justified or will be implemented. Risk assessment incorporates, as inputs, the outputs from the risk analysis and risk evaluation phases.

The two approaches are not mutually exclusive - DSC will rely on both in the demonstration of dam safety.

Note that *defensive design measures* are strictly a sub-set of *standards* but they are mentioned separately in parts of this guidance sheet so that it is absolutely clear that both are to be met.

The *standards-based approach* is an engineering-focussed approach which served a good role in the design of safe dams in past decades. It has value in assessing the safety of existing dams though there are some gaps. It is well understood by dam engineers and will receive only minor coverage in this sheet.

Risk assessment was developed for the hazardous process industries. It enables a more comprehensive approach to safety assessment which extends beyond the dam structure to include all of the potential impacts of dams on society. It is a more recent development in dam engineering.

Faced with competing demands on capital and the complexity of contemporary dam safety decision-making, owners and managers seek a more compelling justification for dam safety improvements than can be provided by the traditional engineering *standards*. *Risk assessment* can meet that need.

4.5 Public safety and the tolerability of risk

It is not reasonably practicable to eliminate risk from large facilities such as dams. There will be some *residual risk* after all reasonably practicable improvements to safety are made. *Risk assessment* needs a yardstick by which the acceptability of the *residual risk* can be judged.

In the hazardous industries, as with dams, the main driver for improvement of safety is usually public safety. For public safety, the most widely recognized tolerability of risk framework in countries with a common law legal system is that developed by the Health and Safety Executive (HSE) in the United Kingdom.

The concept of the HSE tolerability of risk framework is shown in Figure 1.

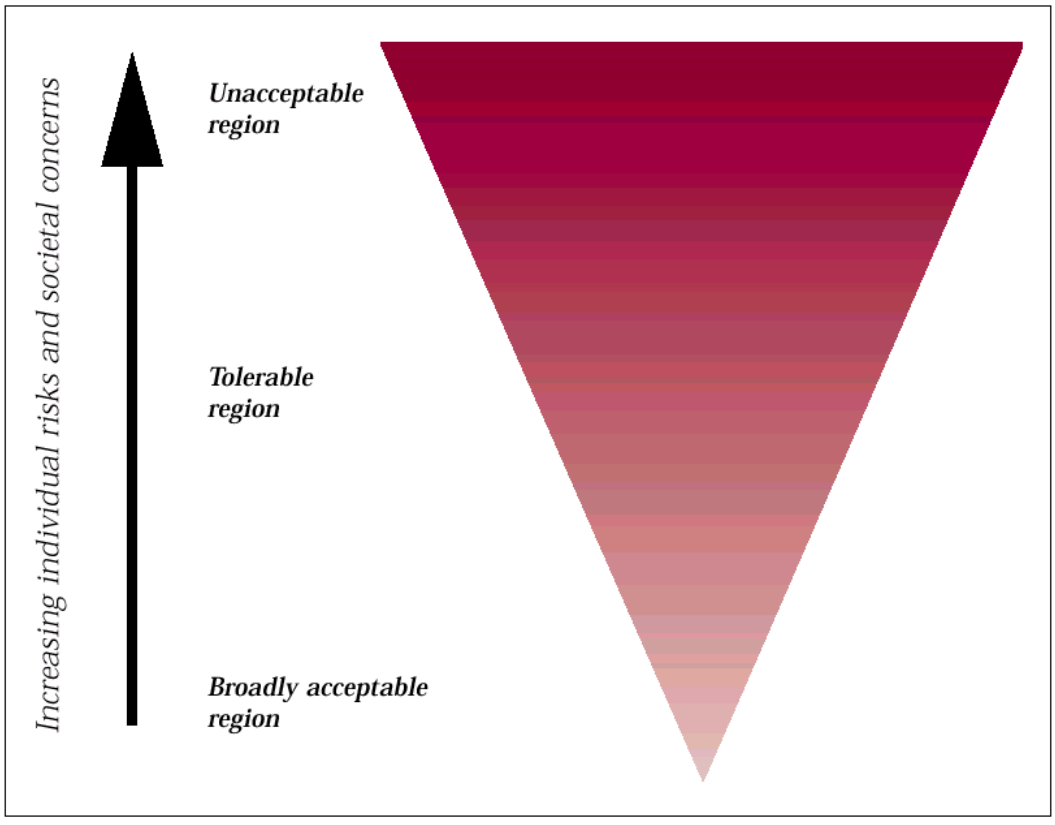


Figure 1 HSE Framework for the Tolerability of Risk (Figure 1 of HSE 2001a)

These points can be made:

1. in the top *unacceptable region* the risks are so high that they must be reduced regardless of any cost considerations. The basis is the principle of *equity* which recognizes that members of society are entitled to a minimum level of protection and are to be treated fairly. The DSC calls this region the *intolerable region;*

2. in the bottom *broadly acceptable region* the risks are low enough that they are not of concern to society and it is not necessary to pursue further risk reduction, though any obvious low cost improvements should be implemented. The DSC calls this region the *negligible region;*

3. in between the *intolerable* and *negligible* regions there is a *tolerable region* which the DSC calls the *region of tolerability review*. Within this region a risk is only *tolerable* provided it brings a benefit for society, it is properly assessed and managed, it is kept under review and it is *as low as reasonably practicable [ALARP]*. The principle of ALARP is enshrined in law in the United Kingdom (a country with a similar legal system to Australia), is a requirement in a number of Australian State safety statutes, and is a policy of the DSC endorsed by the NSW government.

   A risk is not *tolerable* simply on account of being within the region. Figure 2, which has been adapted from a US Army Corps of Engineers proposal, illustrates how the actual level of *tolerable risk* may vary from project to project. In this region the cost of risk reduction is a consideration in judging whether a risk is *tolerable*. The region is governed by the principle of *efficiency* which recognizes that society needs to make the best use of its resources;

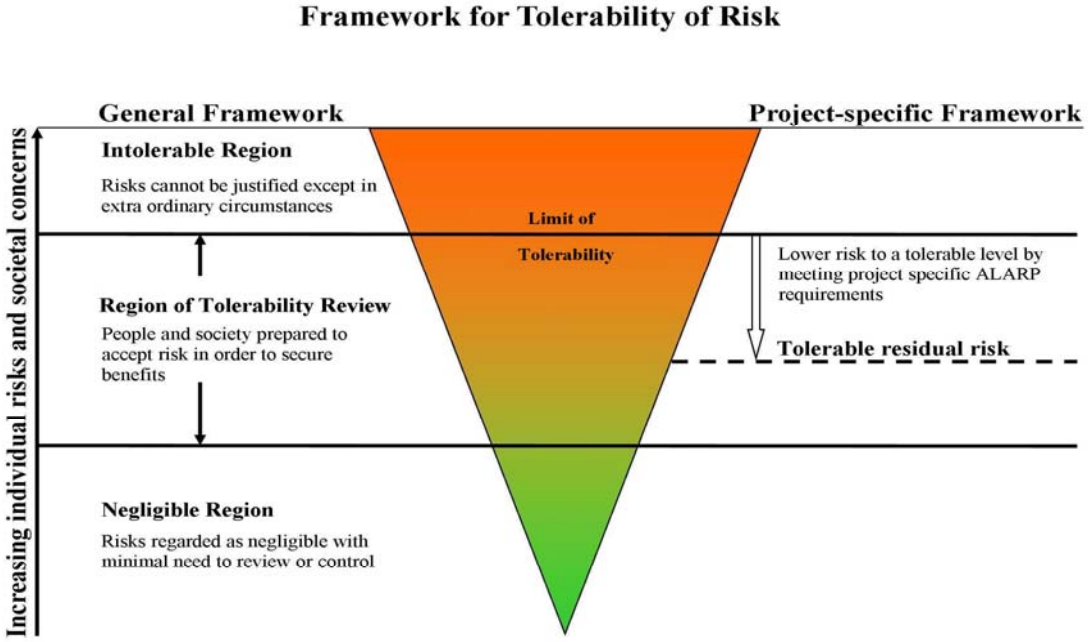


Figure 2 The DSC Framework for the Tolerability of Risk

4. ANCOLD and the DSC have established a boundary between the *unacceptable region* and the *tolerable region* – called the *limit of tolerability*. A risk higher than the *limit* cannot be *tolerable;*

5. in Figure 1 the horizontal width of the triangle at any particular level of risk is an indicator of the effort that ought to be put into risk reduction.

The HSE framework is the main basis for the public safety guidelines proposed by ANCOLD [2003b] and for the DSC *public safety risk guidelines* in the DSC sheet on *Background to DSC Risk Policy Context - DSC1B.*

4.6 The process for demonstration of safety

Safety of a dam is normally to be demonstrated by a *safety review* which follows the process set out in Figures 3 to 5. Owners need to make a case to the DSC to vary the process.

There follows a brief explanation of the process.

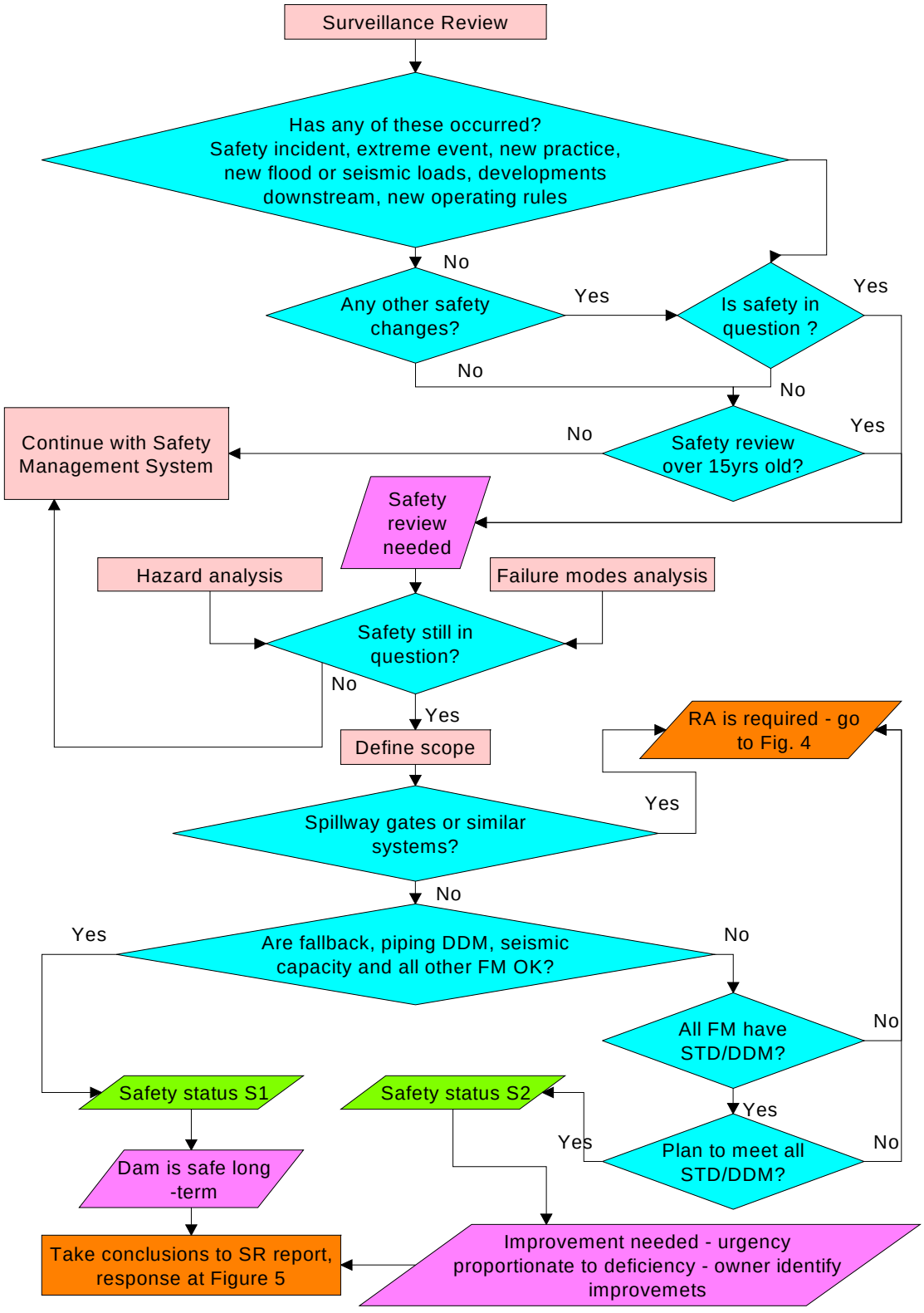


Figure 3 Need for a Safety Review, Standards-based Review

- **Activity – Surveillance review** – this refers to the owner's ongoing watch on dam safety under the Safety Management System (SMS). It includes, but is not limited to, the preparation of a *Surveillance Report;*

- **Decision – Has any of these occurred?**

  - Safety incident - has there been an occurrence with safety implications, such as the appearance of turbid seepage or the cracking and displacement of a mass of earthfill;

  - Extreme event – this refers to rare natural events such as an unusually large flood or earthquake;

  - New practice – this could include new methods of safety analysis or new guidelines on dam safety. Examples are a new method for estimating the stability of concrete gravity dams or a new ANCOLD guideline on design of dams for earthquake;

  - New flood load – this could arise through the issue by the Bureau of Meteorology of a new procedure for the estimation of extreme rainfalls or from revision of earlier flood estimates using improved hydrologic modelling;

  - New seismic load – this could arise through the issue by the seismologists of revised earthquake load estimates based on new data and improved methodology;

  - Development downstream – there may be increased residential and other property development over time. Since dam safety is related to the potential consequences of a failure, such development may alter the safety status of a dam;

  - New operating rules – this issue mainly affects dams of large storage capacity but should be kept in mind for all dams. The flood capacity of some dams takes account of the probable volume in storage prior to the onset of a flood. Any change to the operating regime could affect the dam's flood capacity. Changes to operating rules for spillway gates can affect safety;

- **Decision – Any other safety changes?** – this question aims to capture any other change with a potential to affect safety of a dam. An example would be if a wilderness area downstream of a dam was declared a World Heritage Property. Another example could be if an owner has changed its inspection and monitoring procedure

- **Decision – Is safety in question?** – if there are changes that potentially affect safety the owner needs to determine if the changes are such as to call the dam's safety into question. The owner may need the assistance of a suitably qualified person to reach a decision;

- **Decision – Safety review over 15 years old?** – the owner may conclude that there has been no change that affects the dam's safety status but the DSC seeks assurance on this point if there has been a lapse of fifteen years or more. A suitably qualified person is to track through the process in Figures 3 to 5 and "sign off" that the dam's safety status remains satisfactory. For Significant *consequence category* dams the time lapse is twenty years;

- **Activity – Continue with Safety Management System** – if the owner's watch on safety reveals no occurrences that could adversely affect safety of the dam, and the existing *safety review* is not older than fifteen years (twenty years for Significant *consequence category* dams), then the routine safety management activities would continue;

- **Outcome – Safety review is needed** – this outcome moves the process into the first phases of the safety review;

- **Activity – Hazard analysis** – the aim is to identify all the sources of harm which could affect dam safety. The most obvious hazards are the stored water, floods and earthquakes but bushfire, other fire, landslide, wind, sabotage and terrorism are other examples;
- **Activity – Failure modes analysis** – this activity identifies all of the ways in which failure of the dam could conceivably occur and then selects for analysis those modes which are credible;
- **Decision – Safety still in question?** – a similar question was asked earlier in the process. The question is asked again so that the answer can now be made in light of the *FMA*. A change that was thought to adversely affect safety earlier may now not be an issue because no credible failure mode could be identified;
- **Activity – Define scope** – this activity has a component which precedes *Hazard analysis*. Whilst DSC is interested in dam failure consequences with an adverse impact on community interests, an owner may wish to include its business risks. Also the dam system to be analysed needs to be defined. Such matters can be decided at the outset. However, the decision on the dam failure modes to be examined needs to await the *FMA*. That is why this activity is placed in this location. The activity commences at the outset of the *safety review* but is not completed until the *FMA* is available;
- **Decision – Spillway gates or like systems?** – there is no recognized standard for the reliability of spillway gates. The position of the DSC is that a dam with spillway gates requires *risk analysis* to estimate the dam's flood capacity. In this context, *spillway gates or like systems* includes any flood discharge control system which could fail to function as intended [for example, a fuse-plug of outdated design or reinforced rockfill];
- **Sub-decision – Fall-back OK?** – the DSC will accept the conservative [safer] end of the ANCOLD *fall-back* flood capacity range in Table 8.1 of the flood guidelines [ANCOLD 2000a] as *acceptable flood capacity*. Capacities lower in the range will be considered by DSC provided the owner demonstrates correct transitioning as envisaged by ANCOLD. Pending the issue of the sheet *Acceptable Flood Capacity for Dams - DSC3B*, the DSC acceptance of the *fall-back* capacity is now conditional on the *consequence category* being based on the total *population at risk (PAR)* – prior to any organized or self-evacuation – within the area of the dam-break inundation footprint [including the area affected by natural flooding if the dam did not fail]. If the dam satisfies the DSC *fall-back* flood capacity using total PAR the DSC will accept it as having adequate flood capacity in the long-term – in *risk assessment* inadequate flood capacity would then be regarded as a non-credible failure mode;
- **Sub-decision – Piping DDM [defensive design measures] OK?** – does the dam have the contemporary key *defensive design measures (DDM)* needed for adequate protection against internal erosion and piping. The usual key requirements are that the dam has fully intercepting filters extending from a non-erodible rock foundation to the highest flood level [usually at or close to dam crest level], that the filter media meet contemporary design requirements, that the filters are of adequate thickness, that they are safe against *blow-out* and that they have adequate drainage capacity.

  If the DSC accepts that the dam has adequate DDM the safety against internal erosion and piping will be accepted as adequate in the long-term – in *risk assessment* internal erosion and piping would then be regarded as a non-credible failure mode;
- **Sub-decision – Seismic capacity OK?** – does the dam meet the requirements outlined in *Acceptable Earthquake Capacity for Dam - DSC3C*. If so, the DSC accepts that the dam has adequate earthquake capacity in the long-term – in *risk assessment* inadequate earthquake capacity would then be regarded as a non-credible failure mode;
- **Sub-decision – All other FM [failure modes] OK?** – the question has two elements: a) do all other *failure modes* have a recognized *standard* or *defensive design measures*? and b) does the dam meet those requirements? If the answer to both questions is "yes"

the process moves along the “yes” pathway - otherwise the “no” pathway. Given a “yes” answer, the DSC accepts that the dam has adequate safety in the long-term for the particular failure mode – in *risk assessment* the failure mode would then be regarded as a non-credible failure mode;

- **Decision – All FM have STD/DDM [standards/ defensive design measures]?** – the question is whether all *failure modes* on this pathway have a DSC or industry-recognized *standard* or *defensive design measures* that are accepted as ensuring adequate safety in the long term. If not then *risk assessment* is required;
- **Decision – Plan to meet STD/DDM [standards/ defensive design measures]?** – the owner has a choice. The dam can either be brought into full compliance with all STD and DDM or *risk assessment* will be needed to determine its safety status. A “yes” answer here means that the DSC would normally not require a *risk assessment*. The DSC requires that the *standards-based* safety status be reported in all *safety reviews* whether or not the owner intends to rely on *risk assessment*;
- **Outcome – Safety status S1** – this means there is a DSC or industry recognized *standard* or *defensive design measure* for every *failure mode* and the dam complies with all these STD and DDM;
- **Outcome – Safety status S2** – this status means that there is a recognized *standard* or *defensive design measure* for every *failure mode*, not all STD or DDM are met, and that the owner is committed to bringing the dam into compliance with all STD and DDM on a program agreed with the DSC;
- **Outcome – Dam is safe in long-term** – this means that, given safety status S1, the dam is accepted by the DSC as safe in the long-term subject only to the qualification that future circumstances are unknowable and may change the understanding of the dam’s safety;
- **Outcome – Improvement needed – urgency proportionate to deficiency – owner identify improvements** – given safety status S2, an improvement in safety is required, subject to the DSC agreeing with the owner’s analysis. As a general principle the urgency of improvement would be proportionate to the degree of deficiency, though deficiencies for some failure modes would be more serious than for other failure modes. At this stage the owner identifies safety improvements which would bring the dam into compliance with all recognized *standards* or *defensive design measures* for all credible *failure modes*.
- **Transfer – Transfer conclusions to SR [safety review] report, response at Fig. 5** – the conclusions on the need or otherwise for safety improvements are transferred to Figure 5 for incorporation in the *safety review* report.
- **Outcome – RA [risk assessment] is required – go to Fig. 4** – this means either there are *failure modes* with no recognized *standard* or *defensive design measure* and/or that the owner has chosen to rely on *risk assessment* to determine the safety status of the dam. This outcome moves the process from Figure 3 to Figure 4.

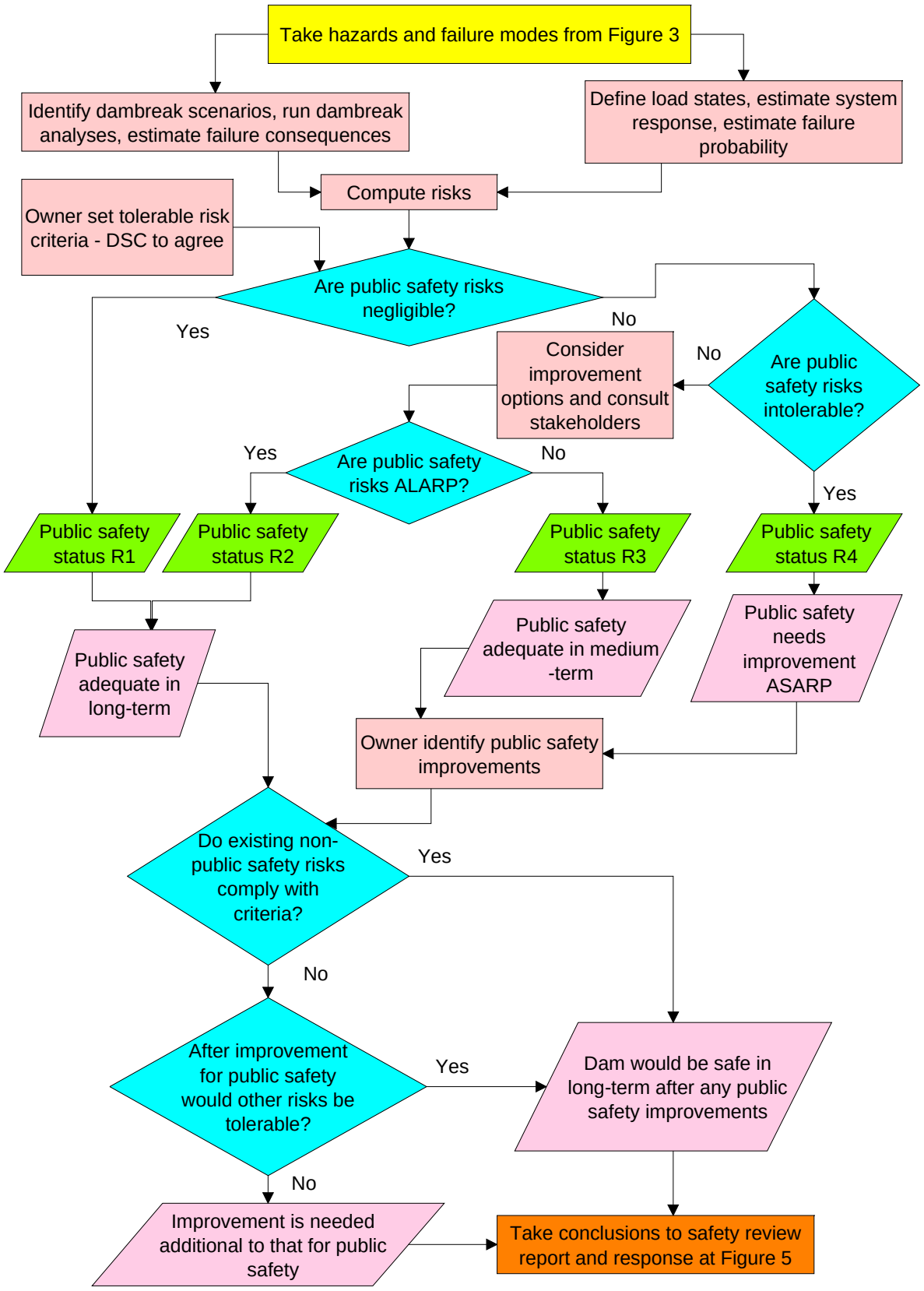


Figure 4 Risk-based Review of Safety

- **Transfer – Take hazards and failure modes from Figure 3** – there is no need to repeat the *hazard analysis* and *failure modes analysis* – the outputs are taken from the previous work;
- **Activity – Identify dam-break scenarios, run dambreak analyses, estimate failure consequences** – these activities are described in the risk guidelines (ANCOLD 2003b);
- **Activity – Define load states, estimate system response, estimate failure probability** – these activities are described in the risk guidelines (ANCOLD 2003b);
- **Activity – Compute risks** – this activity is described in the risk guidelines (ANCOLD 2003b);
- **Activity – Owner set tolerable risk criteria – DSC to agree** – both the Australian national standard AS/NZS 4360: 2004 *Risk Management* and the draft international standard ISO 31000 *Risk Management – Guidelines on Principles and Implementation of Risk Management* require an owner or operator to set *tolerable risk criteria*. Normally those criteria for prescribed dams are to at least meet the requirements of this guidance sheet; in particular the DSC *public safety risk guidelines* set out in *Background to DSC Risk Policy Context - DSC1B*, Section 2, under Principle D.3. The succeeding activities, decisions and outcomes dealing with public safety are judged against the DSC *public safety risk guidelines*. An owner is free to repeat the process against its own criteria which provide greater public safety, except that the DSC would wish to discuss the matter with the owner if such stricter criteria would significantly delay the removal of intolerable risks on other dams within the owner's portfolio. Criteria are to be set for non-public safety risks as well. The DSC needs to agree that the criteria affecting the public interest adequately protect the public interest. The prudent approach is for owners to obtain such agreement before proceeding further with a risk-based review;
- **Decision – Are public safety risks negligible?** – for the answer to be "yes" the best estimate of both *risk to the individual* and *societal risk* must be in the *negligible region* – otherwise the answer is "no";
- **Decision – Are public safety risks intolerable?** – for the answer to be "yes" the best estimate of either *risk to the individual* or *societal risk* must be in the *intolerable region* – otherwise the answer is "no";
- **Activity – Consider improvement options and consult stakeholders** – if the answer to both of the preceding questions was "no" it follows that the best estimate of one or both of *risk to the individual* and *societal risk* must be in the *region of tolerability review*. The question then is whether the risk is *tolerable* and the main consideration then is whether the risk is *as low as reasonably practicable (ALARP)*. To consider that question it is necessary to consider the possibilities for improvement of safety – ANCOLD (2003b) and later sections of this sheet give guidance. A key consideration in judging whether a risk is *ALARP* is *societal concerns*. To fully expose *societal concerns* the DSC requires the owner to undertake stakeholder [including the at risk community] consultation. If an owner does not wish to undertake stakeholder consultation the alternative is to make a commitment to reduce both *risk to the individual* and *societal risk* to the *negligible region* in the *long-term* on a program agreed with the DSC;
- **Decision – Are public safety risks ALARP?** – the answer to this question is a judgment made by the owner following the guidance of ANCOLD (2003b) and of this sheet [including the cited source documents];
- **Outcome – Safety status R1** – this means that the public safety risks are *negligible* and are not of concern to society;
- **Outcome – Safety status R4** – this means that one or both of the public safety risks [*risk to the individual* or *societal risk*] is *intolerable*;

- **Outcome – Safety status R2** – this means that one or both of the public safety risks (*risk to the individual* or *societal risk*) is in the *region of tolerability review* and is *ALARP*, and that if it is one risk only the other is *negligible*;
- **Outcome – Safety status R3** – this means that one or both of the public safety risks (*risk to the individual* or *societal risk*) is in the *region of tolerability review* and is not *ALARP*, and that if it is one risk only the other is either in the *region of tolerability review* and *ALARP* or it is *negligible*;
- **Outcome – Public safety adequate in long-term** - this means that, given safety status R1 or R2, public safety is accepted by the DSC as adequate in the long-term subject only to the qualification that future circumstances are unknowable and may change the understanding of the dam's safety. Nevertheless, safety status R1 is a better level of safety than safety status R2;
- **Outcome – Public safety adequate in medium-term** - this means that, given safety status R3, public safety is accepted by the DSC as adequate in the medium-term but needs improvement in the long-term. Under the concept of *progressive improvement* described in *Background to DSC Risk Policy Context - DSC1B,* the long-term improvement can be either to reduce risks so that they remain within the *region of tolerability review* but are *ALARP* (by recycling through the process) or to reduce risks to the *negligible region*;
- **Outcome – Public safety needs improvement ASARP (as soon as reasonably practicable)** – the need for improvement is urgent. There should normally be a short-term reduction of risk while medium-term improvements are planned to reduce risks into the *region of tolerability review*. The owner needs to make a genuine effort to reduce the risks in the shortest practicable time;
- **Activity – Owner identify public safety improvements** – at this stage the owner identifies safety improvements which would bring the dam into compliance with all public safety risk criteria for all credible failure modes;
- **Decision – Do existing non-public safety risks comply with criteria?** – this refers to the risks of the dam system prior to any improvements;
- **Decision – After improvement for public safety would other risks be tolerable?** – it is possible that after improvements needed for public safety are made the non-public safety risks would then comply with their criteria. This question examines that possibility;
- **Outcome – Dam would be safe in long-term after any public safety improvements** – this means that either the existing dam risks comply with the non-public safety criteria or the risks would comply once the necessary public safety improvements have been implemented;
- **Outcome – Improvement is needed additional to that for public safety** – this means that even after improvements required for public safety are made there would remain some non-public safety risks which do not comply with their criteria;

  Transfer – Transfer conclusions to safety review report and response at Figure 5 – the findings are transferred to Figure 5 for incorporation in the safety review report.

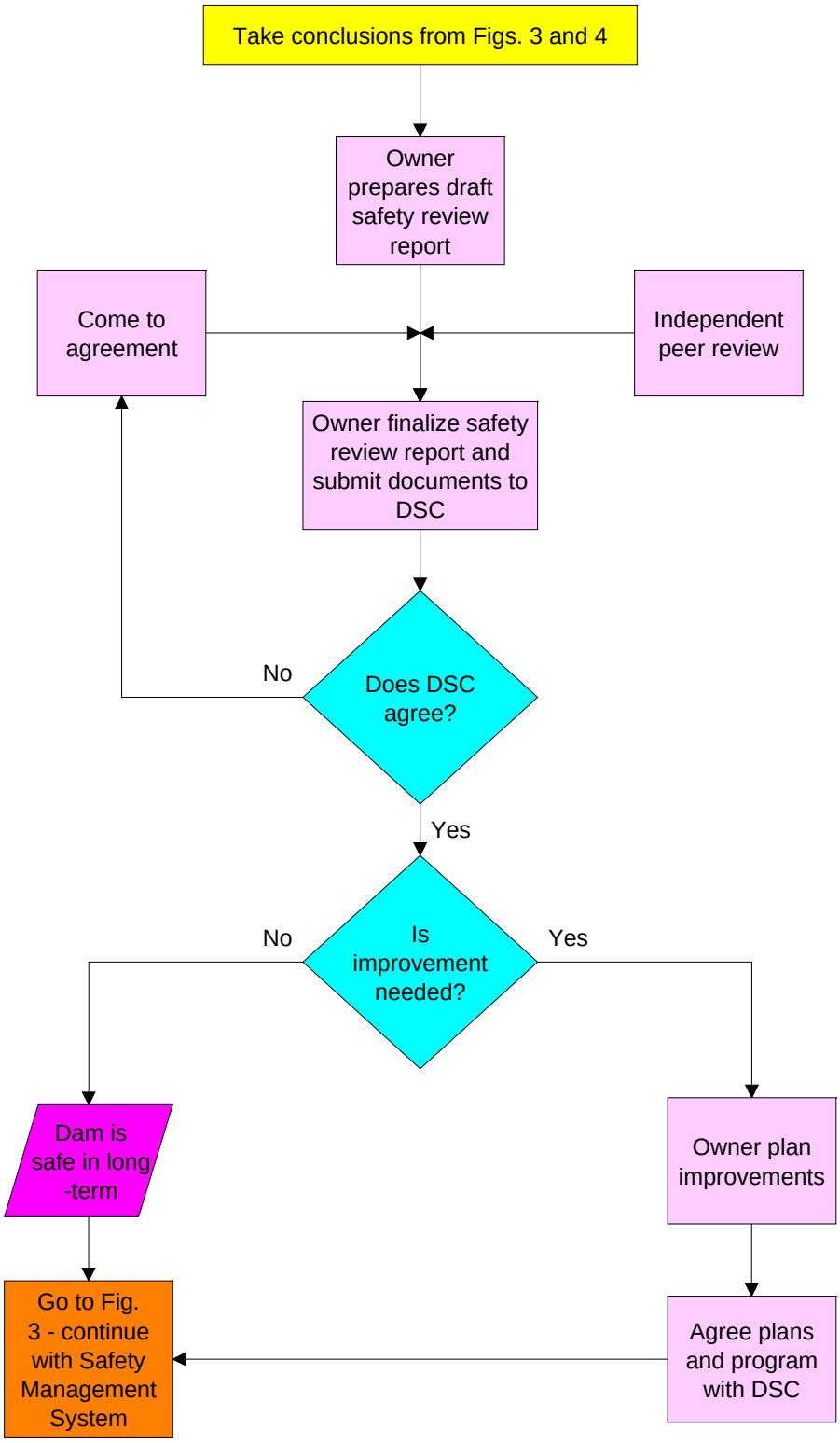


Figure 5 Safety Review Report and Response

- **Transfer – Take conclusions from Figures 3 and 4** – the aim is to capture all of the information for incorporation into the *safety review* report. The key matters are the conclusions from Figures 3 and 4 but they need to be supported by all of the information generated by the total process;
- **Activity – Owner prepares draft safety review report** – the owner arranges a draft report setting out the conclusions of the *safety review* and providing full documentation of all inputs, methods and analyses that support the conclusions;
- **Activity – Independent peer review** – this is the review of the draft *safety review* report by the independent peer reviewer. The reviewer would normally have been involved at earlier stages of the process but this is the point at which the reviewer's opinions are formally documented. The report of the independent reviewer, or reviewers, is a stand-alone document;
- **Activity – Owner finalises safety review report and submits documents to DSC** – having received the report of the peer reviewer(s) the owner finalises the *safety review* report. The report is submitted to the DSC along with the report of the peer reviewer(s), a statement of the owner's response to the peer review report and a letter of transmittal;
- **Decision – Does DSC agree?** – the DSC reviews the documents and decides whether or not it agrees with the owner's assessment of the dam's safety status and any response proposed by the owner;
- **Activity – Come to agreement** – in the event the DSC does not agree with the owner's assessment and proposals, it is necessary that dialogue takes place until agreement is reached. The process would most likely require some amendment of the *safety review* report [as indicated by the closed loop in the flow chart];
- **Decision – Is improvement needed?** – the key outcome of a safety review is whether or not an improvement of safety is required.
- **Outcome - Dam is safe in long-term** - this means that the dam is accepted by the DSC as safe in the long-term subject only to the qualification that future circumstances are unknowable and may change the understanding of the dam's safety;
- **Outcome – Owner plan improvements** – this means a commitment by the owner to undertake improvements and to commence with the planning process. The planning of improvements can take several years and may evolve considerably throughout the process. The demonstration of safety does not encompass the full planning process. It extends to the owner's commitment to bring the dam to a safe condition and to do so within a reasonable time frame;
- **Activity – Agree plans and program with DSC** – this activity acknowledges that the owner is to propose the time horizon for reduction of risks but the DSC needs to agree with that proposal or to enter discussion with the owner on an alternative program. The actual undertaking of safety improvements is beyond the scope of this guidance sheet. The DSC may agree to a program of *progressive improvement* whereby the most serious deficiencies are remedied early and less serious issues are addressed at a later time;
- **Transfer – Go to Fig. 3 - Continue with Safety Management System** – the meaning is as given for Figure 3. The Safety Management System is to continue whilst any improvements in safety are planned.

4.7 The impact of these changes on the cost of safety improvement

The cost implications can be considered with regard to three key areas.

Firstly, on flood capacity, Figure 3 of *Background to DSC Risk Policy Context - DSC1B* shows where the *fall-back* flood capacity for High B and High C flood consequence category dams would sit relative to DSC *societal risk* requirements if the estimated *potential loss of life [PLL]* was equal to the total *PAR*. In that situation it can be seen that the DSC *public safety risk guidelines* could often justify less expenditure. But *PLL* is almost never equal to *PAR*. The only situations where *PLL* approaches *PAR* is for dams [almost always concrete dams] where dam-break results in *high flood severity* as defined by Graham [1999]. For normal embankment dams *high flood severity* is not realistic and *medium flood severity* is the worst situation. From Table 7 of Graham [1999] it can be seen that the *fatality rate* would range from 0.15 to 0.0002 for embankment dams. Even for the upper end *fatality rate* the DSC *public safety risk guidelines* would usually justify less expenditure than required by the *fall-back* capacity. Where the *PAR* is more than about 10km downstream of the dam the fatality rate would be lower and the DSC *public safety risk guidelines* would almost always justify less expenditure than required by the *fall-back* capacity.

Since the *fall-back flood capacity*, based on *total PAR*, is unquestionably an industry standard the DSC would accept such a capacity as adequately safe in the long-term. The qualification *based on total PAR* takes care of two concerns which the DSC has:

1. the ambiguity in ANCOLD (2000b) as to whether *incremental* or *total PAR* was intended; and
2. the fact known to DSC that there is no sound and defensible relationship between *incremental PAR* and *incremental PLL*.

It is unclear from ANCOLD (2000b) whether it is *total* or *incremental* PAR that is meant to be the basis for *consequence categories*. There are problems with *incremental PAR*, it being possible to have zero *incremental PAR* but significant *incremental loss of life* (Hill et al. 2008). That is why the DSC will only accept the *fall-back standard* as demonstrating adequate safety if the consequence category is based on *total* PAR. ANCOLD is currently reviewing the consequence guidelines (ANCOLD 2000b).

The net effect of the DSC requirements is that, given the DSC position on *total PAR* as the basis for consequence categories, risk assessment can reduce, but cannot increase, the cost of providing adequate flood capacity.

Secondly, there are no recognized *standards* for safety against internal erosion and piping for old embankment

dams which lack the contemporary *defensive design measures*. With internal erosion and piping the only conceivable *standard* is fully intercepting filters and the other well-recognized key *defensive design measures*. If those are met the DSC *public safety risk guidelines* are usually more than satisfied. *Risk assessment* may justify lower costs than required by the *standard* for piping safety but it cannot increase costs because a dam with the contemporary key *defensive design measures* is accepted by the DSC as adequately safe in the long-term.

Thirdly, earthquake capacity is only rarely a significant issue for dams [usually only for those few dams with foundation or embankment materials that are susceptible to liquefaction]. Compliance with the DSC *standard,* set out in the DSC's guidance sheet on *Acceptable Earthquake Capacity for Dams - DSC3C,* will be accepted by the DSC as demonstrating adequate safety against earthquake in the long-term. Risk assessment may reduce, but cannot increase, safety improvement costs.

By introducing risk assessment to dam safety, this sheet DSC2D opens the opportunity for dam owners to significantly reduce the costs of dam safety improvements whilst providing adequate protection for public safety and other community interests. Given the process in Figures 3 to 5 of this sheet, risk assessment cannot increase costs over a *standards-based approach.*

5. SURVEILLANCE REPORT

5.1 What is the role of the Surveillance Report in demonstration of safety?

The role of the *Surveillance Report* (see *Surveillance Reports for Dams - DSC2C*) is to conclude, on the basis of present knowledge, that the dam fits one of these descriptions:

- the dam clearly meets DSC requirements (documentation in support of this conclusion must exist); or
- the dam clearly does not meet DSC requirements; or
- the safety status of the dam is uncertain.

If the dam does not meet DSC requirements or safety status is uncertain, the *surveillance report* is to include a recommendation on whether a *safety review* is essential to establish the safety status.

6. SAFETY REVIEW

6.1 How is the safety of a dam to be established?

For a dam older than fifteen years in its existing configuration, an owner is normally required to undertake or update a *safety review* to establish its safety status. For dams less than fifteen years old in the present configuration, a *design report, construction certificate* and *construction report* would normally be accepted in lieu of a *safety review* provided these documents meet DSC requirements.

6.2 What is a *safety review?*

The DSC definition of a *safety review* is in Appendix A.

6.3 What is the scope of a *safety review*?

A *safety review* should normally be comprehensive – covering all scenarios of hazards, load states, and *failure modes*. For a *risk-based approach*, a comprehensive review is required because it is the risks from all hazards, *failure modes* and loading scenarios that are to be compared with the DSC *public safety risk guidelines* (see DSC1B - Section 2, under Principle D.3). A previous *safety review*, or a *surveillance report*, may have established safety at the time and new circumstances may call into question only one or a few aspects of safety. In that case a *safety review* that addresses only that part of the full spectrum of hazards, *failure modes* and loading scenarios which requires updating would be accepted.

A *failure modes analysis* (see later) provides a good basis for determining the scope of a *safety review*.

In defining the scope of a *safety review*, the dam system to be analysed must be defined. The normal DSC requirement is that all dam elements (main dams, saddle dams and other dams) retaining the one storage body should be the subject of a single *safety review*. In *risk assessment*, the *failure modes*, failure probabilities and failure consequences from all of the dams would be used to plot the *societal risk* F-N graph. Departures from this approach need to be agreed with the DSC.

In considering the scope of a *safety review*, owners might note these points:

- Firstly, a comprehensive *safety review* is to the owner's advantage. Once that document exists updates can keep it a living document and the owner will be able to demonstrate at any time the dam's safety status.
- Secondly, where there are existing valid analyses demonstrating safety a citation of those would suffice in the *safety review report* provided the owner can deliver the cited documents upon a request by the DSC and the *safety review* report addresses all credible *failure modes*.
- Thirdly, where DSC agrees that a DSC *standard* or industry-recognized *standard* [DSC *standards* have precedence] is satisfied, that failure mode will be regarded as not a credible failure mode for *risk assessment* purposes and may be excluded from any *risk analyses*.
- Finally, the scale and rigour of a *safety review* should be proportionate to the potential failure consequences.

The scope of a *safety review* is to be as determined by the dam owner but should at least address any issues of interest to the DSC.

6.4 When is a *safety review* required?

An owner is responsible for determining when a *safety review* is necessary. The DSC may endorse the need for a *safety review* or may make its own request to the owner for a review. An endorsement by DSC would normally result from consideration of a *surveillance report* recommendation.

Safety reviews are not required for Low consequence category dams, provided there is confidence that the consequences have not moved to a higher category.

A *safety review* is required whenever the safety of a prescribed dam is in question.

6.5 Who can do a *safety review*?

Persons who prepare *safety reviews* need the qualifications, skills and experience to arrive at a sound conclusion on the safety of dams. The breadth of knowledge needed is usually so wide that a team of analysts will be required.

6.6 Is a peer review required?

Following the failure of Teton Dam, Idaho, United States on 5 June 1976, a group of six eminent persons was appointed to examine the causes of the failure and to make recommendations to prevent a recurrence (TDFRG 1978). One recommendation was:

An independent board of review be convened for each major dam project. This board should review both design and construction at appropriate intervals.

Independent peer review is now established practice for dam engineering in North America and elsewhere. In Australia many dam owners now arrange independent review.

For any *safety review* that is prepared for the DSC for an Extreme or High consequence category dam, there is to be an *independent peer review*. The peer reviewer(s) is to be a senior practitioner widely recognized for their knowledge and experience with the particular dam safety issues. The peer reviewer(s) is to provide the owner with a separate report.

A peer reviewer is independent if:

1. the peer reviewer did not undertake part or all of the *safety review*;
2. the peer reviewer is not an employee of the dam owner;
3. the peer reviewer is not an employee of the entity which undertook the *safety review*.

This guidance is provided:

- The owner is to define the scope of the peer review;
- The peer reviewer(s) is to be selected and engaged by the owner;
- The qualifications and experience of reviewers are to be acceptable to the DSC;
- A team of two or three reviewers will benefit the review through their interchange of views and the wider range of experience. The potential failure consequences and the scope of the review are considerations in deciding whether a team of reviewers is required;

- Reviewers need access to all relevant documents and data;
- Reviewers are best involved at key milestone points in the analysis process – but avoid "capture" by the analysis team;
- The role of reviewers is to pass judgment on the soundness of inputs, analysis methods and outputs;
- It is not the role of reviewers to verify computations - though it makes sense to raise errors noted in passing;
- Reviewers normally raise questions and challenge the owner's analysis team – the peer review shall not shift responsibility to the reviewer;
- The owner, through its analysts and peer reviewers, must be able to defend the validity of the analyses – it must not rely on the DSC to verify the soundness of the work;

The owner shall accept the responsibility for the *safety review* that is submitted to the DSC.

6.7 Is a *hazard analysis* required?

A *hazard analysis* can have two parts:

- identification of all credible *hazards* that could endanger the dam; and
- analysis of the magnitude and likelihood (or probability) of some *hazards* [for example, estimation of a flood frequency curve].

Every conceivable *hazard* should be considered and the reasoning as to why each *hazard* is, or is not, credible is to be documented. Where appropriate, the magnitude versus probability relationships for the hazards requiring further analysis are to be developed.

The DSC *normal* requirement is that a new, updated or existing valid *hazard analysis* be part of a *safety review*. A *hazard analysis* is an essential component of any *failure modes analysis*.

6.8 Is failure modes analysis required?

Failure modes analysis (FMA) is an activity which brings benefits to safety management and which can reduce the scope and cost of a *safety review*. Those who require *FMA*, such as the Federal Energy Regulatory Commission in the United States, are in no doubt that the benefits more than justify the costs. *FMA* will identify the failure modes which require in-depth analysis and those which can be safely neglected.

ANCOLD (2003b) does not define *failure modes analysis* (FMA), though such analysis is based on the principles of *failure modes and effects analysis (FMEA)*, which is defined. FMEA was developed for use in the hazardous process industries. Dams differ from industrial facilities, so the DSC prefers the generic term *failure modes analysis* (defined in Appendix A). Appendix B sets out guidance on *failure modes analysis*.

A *failure modes analysis* is an essential part of a *safety review* for all High and Extreme *consequence category* dams, whether or not a *risk assessment* is to be undertaken. Owners are encouraged to undertake *failure modes analysis* for all dams.

If *failure modes analysis* shows the dam is adequately safe, the DSC may waive the *normal* requirement for a full *safety review*.

The DSC needs these outputs from a *failure modes analysis*:

1. the *failure modes analysis* – stating the dam system elements considered, the *failure modes* considered, those *failure modes* not warranting further analysis, the *failure modes* that do require further consideration and the reasoning that supports these conclusions;
2. the *failure mechanisms*, normally represented in a graphic format such as *event trees* or *fault trees* - but probability values are not required at this stage; and
3. an opinion on the need for a full *safety review*;
4. any need for urgent action as revealed by the *failure modes analysis.*

A failure mode which complies with DSC or industry-recognized *standards [STD]* or *defensive design measures (DDM)* intended to assure safety in the long term is accepted by DSC as not credible. However, the analyses which demonstrate compliance are to be documented in the *failure modes analysis* or *safety review*, or separate documents are to be cited.

6.9 Is standards-based analysis required?

The traditional *standards-based approach* to safety has resulted in safe dams over many decades. *Standards* developed for the design of new dams do not always adequately address the safety of existing dams. For some aspects of dam safety there are no *standards*. The safety against internal erosion and piping of embankment dams without the contemporary *defensive design measures* and the reliability of spillway gates are examples.

In a *safety review* the status of the dam in terms of any recognized *standard* or *good practice*, including the appropriate *fall-back flood capacity*, is to be reported. Any DSC *standard* takes precedence over any corresponding industry-recognized *standard*.

Compliance with traditional *standards* or *good practice* intended to assure long-term safety will provide an adequate demonstration of dam safety in the long-term subject to the DSC agreeing with the relevant analyses.

6.10 Is account to be taken of Base Safety Condition?

Base Safety Condition is a concept related to a *standards-based review* of the flood capacity of dams. The concept recognizes that the *incremental consequences* of dam failure may become *tolerable*, or *negligible*, at an inflow flood significantly smaller than the extreme floods normally assigned as the flood

capacity of dams under the traditional *standards-based approach*. For a fuller description of the concept see:

- *Acceptable Flood Capacity for Dams* (DSC3B, Appendix A);
- Hawk (1991); and
- FERC (1993 – third last paragraph of Sub-section 2-3.1.5 and Appendix II-C, Flowchart 2).

To identify a *Base Safety Condition*, a *standards-based review* would need to consider the *total* and *incremental consequences* of a sufficient number of inflow flood magnitudes. Reliance on *Base Safety Condition* may sometimes avoid or substantially reduce the cost of safety improvement. It would be in the interests of a dam owner to consider the possible benefits of reliance on a *Base Safety Condition* in any *standards-based review* of flood capacity. However, the advice of an experienced engineer should be obtained because analysis for a Base Safety Condition can involve a lot of work and will often not result in a useful outcome.

A properly structured *risk assessment* should automatically identify a *Base Safety Condition*.

6.11 Is risk assessment required?

Risk assessment is required or appropriate where:

1. there are aspects not adequately addressed by traditional *standards* or *good practice* and those aspects are significant in assessing the safety of a dam - *risk assessment* is required by DSC (see Sub-section 6.6 and Figure 3);
2. an owner wishes to demonstrate that less costly safety improvements, than those required by *standards* or *good practice*, would adequately protect public safety and community interests - *risk assessment* is required by DSC;
3. an owner wishes to undertake *risk assessment* as a basis for more informed decision making – *risk assessment* is at owner's discretion.

Areas where *risk assessment* provides information not available from traditional standards-based analysis include:

- comparative risks between the dams of a portfolio;
- comparative risks between components and *failure modes* of a dam;
- case-specific risks to life, property and the environment (as distinguished from the very broad *consequence categories* that drive some safety levels under the *standards-based approach*);
- aggregation of the risks of multiple dam components, hazards and *failure modes* to arrive at an appreciation of the total risk from dam failure;
- the role of *human factors* in contributing to the likelihood of dam failure;

- the likelihood that an intervention can prevent or initiate dam failure;
- the likelihood that emergency preparedness would reduce loss of life;
- the cost-effectiveness of potential safety improvements in reducing risk.

6.12 What general requirements are there for risk assessment?

The approach to *risk assessment* is to be that of ANCOLD (2003b). The generic approach is to conform to the national standard AS/NZS 4360:2004 (SA/SNZ 2004). For a *safety review* the level of *risk assessment* shall be at least *detailed* and preferably *very detailed* (Table 6.1 of ANCOLD 2003b). See *Dam Safety Management System-DSC2A* on *portfolio risk assessment.*

Take particular note of the ANCOLD guidance on:

1. personnel undertaking *risk assessment*;
2. *risk assessment* not to be reliant on one person – risk values to be challenged and debated;
3. documentation of *risk assessments*, including the reasoning in support of all risk values;
4. verification of computations;
5. independent review;
6. comparison of best estimate risk values with criteria; and
7. reporting of uncertainty.

6.13 What potential failure scenarios are of interest to the DSC?

The DSC is interested in scenarios with a significant adverse effect on the interests of the community. It is not interested in scenarios which would affect only the owner and its immediate stakeholders (such as employees and shareholders). Scenarios involving the operation of a dam in the absence of a failure are not within the charter of the DSC.

Here are some example scenarios:

1. a dam breach causes a flood which results in loss of life, injury, property damage and environmental damage – there is a significant adverse effect on the interests of the community - DSC is interested;
2. a saddle dam breaches without causing significant flooding but draining most of a reservoir which is the only water source for a large community. Severe restrictions are applied – there is a significant adverse effect on the interests of the community - DSC is interested;
3. an outlet tower is seriously damaged by an earthquake and the reservoir drains through the outlet conduit. This is the smallest of three dams supplying water to a small community – there is no significant adverse effect on the interests of the community - DSC is not interested;

4. an embankment dam supplying water to a gold mine suffers major distortion from liquefaction under earthquake shaking at a time of reduced reservoir level. The dam has a large freeboard so that there is no loss of water but expensive repairs will be required – there is no significant adverse impact on the community - DSC is not interested (the DSC may be interested to see that the dam is repaired if there is potential for a future threat to community interests – say from a subsequent flood event);

5. spillway gates open inadvertently and cause substantial damage to property downstream. This is a system failure which has adverse impacts on the community - DSC is interested;

6. a spillway gate is opened to release an environmental flow and members of a family picnicking on a downstream rock bar are drowned – this scenario is one of normal operation and not dam failure and does not come within the charter of the DSC.

In a *safety review* the owner may wish to capture scenarios affecting its interests as well as scenarios in which the DSC is interested. Risks from failure scenarios with a potential for significant adverse effect on the interests of the community are to be separately aggregated for consideration by the DSC.

6.14 What of the estimation of the probabilities of dam failures?

The DSC emphasizes four issues.

Coherence and the mathematics of probability

The inputs to *risk analysis* typically have wide uncertainty but the mathematics of probability is precise. Advantage can be taken of this precision to build self-checking routines into spreadsheets if cells are set to sufficient accuracy. Compliance with the mathematics and logic of probability, known as *coherence*, is a fundamental requirement of *risk analysis*. However, output values need to be rounded to acknowledge the uncertainty of the inputs.

There are many sources for the mathematics of probability. Three helpful sources are Benjamin and Cornell (1970), Ang and Tang (1975), and Hartford and Baecher (2004). The former two are out of print but may be available in libraries.

The estimation of failure probabilities is to comply with the mathematics of probability wherever practicable.

Human factors

Human factors analysis is a complex task requiring consideration of such aspects as communication and decision processes, operator training, stress on operators in extreme events, access for personnel, equipment and materials, availability during extreme events, the adequacy of operating and emergency instructions and security arrangements at dams.

Account is to be taken of *human factors*, in terms of errors, lapses or omissions contributing to an increase in the *probability of failure* and deliberate interventions contributing to a reduction or an increase in the *probability of failure*.

Varying risk profile

For the construction of new dams, embankment dams in particular, the risk profile varies with construction stage. *Probability of failure* typically declines rapidly as the embankment is raised. At the same time the *consequences of failure* are rapidly increasing. There may also be a dynamic risk situation with the modification of existing dams.

Risk analysis is to capture the varying *probability of failure* during construction on a dam.

Uncertainty of risk values

Uncertainty of *probability* values can be assessed by methods such as:

- propagation of uncertainties through the analysis by Monte Carlo simulation;
- sensitivity testing of inputs to gauge the effect on the output probabilities; or
- qualitative consideration of the level of uncertainty in the inputs.

An owner is to provide an assessment of the degree of uncertainty of estimated *probabilities*.

6.15 What of the estimation of failure consequences?

The DSC gives particular emphasis to the following points.

Downstream development

A key issue for estimation of *consequences* is whether they are based on the existing or projected future development downstream of the dam.

Where estimated *consequences* are needed to review the current safety of dams they are to be based on existing development and known planned development in the near future. For example, if a development application has been lodged with the consent authority it would be reasonable to base the assessment of safety on that development being in place. Where safety improvements are required, the estimated *consequences* required for review of the safety of the post-improvement dam are to be based on projected future development to ensure that development does not make the dam again unsafe within a period of several years. It is suggested that owners try and ensure the post-improvement dam will remain safe, in terms of downstream development, for a period of at least twenty years.

Reports are to state:

- whether the estimation of *consequences* is based on existing development or projected future development;
- the time horizon over which likely development has been considered; and
- the basis of projections.

Estimated Loss of Life

Potential loss of life (PLL) is usually the main driver for safety levels - estimates of *PLL* are to be as defensible as they can reasonably be.

A recognized methodology, calibrated to dam failure and flash flood events, is to be used to estimate the *potential loss of life [PLL]* from dam failure. An acceptable method is that of Graham (1999). The owner is to obtain the agreement of DSC to the use of other methods. The Graham method is currently under review (Graham 2006).

In estimating *incremental potential loss of life* a method, calibrated to natural flooding (other than flash flooding) fatality rates, is to be used to estimate PLL for non-dambreak flooding. The method proposed by Hill et al. (2008) is acceptable to the DSC. The owner is to obtain the agreement of DSC to the use of other methods. See the Dartmouth Flood Observatory at www.dartmouth.edu/~floods for data on loss of life due to natural flooding.

If PAR is over 10,000 the empirical methods such as Graham (1999) may mislead because the PAR is beyond the range in the database of failures from which the methods were developed. For PAR greater than 10,000 the State Emergency Service (SES) is to be consulted to see if the estimated PLL seems reasonable with regard to the time available for evacuation.

Economic and financial loss

The interest of the DSC is *economic loss* whilst that of the owner is also the *financial loss*. *Financial loss* is the private business of the dam owner unless it has a significant adverse effect on the community. Where a dam failure causes *financial loss* to a private owner, the result could be a reduction in dividends paid to shareholders [which is none of the DSC's business]. But in other cases there could be the need for a substantial increase in Council rates causing community hardship [of concern to the DSC]. The DSC needs disclosure of *financial risks* only to the extent needed to review any judgment on *ALARP* and to know whether there is a significant adverse impact on the community. Both *financial* and *economic loss* can be legitimately counted in estimating the *cost to save a statistical life (CSSL)*, which is a consideration in demonstrating that risks are *ALARP*.

The Queensland guidelines (NRM 2002) and the references cited therein provide useful guidance.

The normal DSC requirements are:

- that estimated *economic loss* be reported separately from any *financial loss* estimate (the two are not necessarily mutually exclusive);
- that *direct* and *indirect losses* be separately identified (the two are mutually exclusive);
- that for the preceding categories, both *total* and *incremental loss* be reported; and
- that where there are important issues at stake, the estimation methodology is reviewed by an economist.

Harm to the environment

Persons qualified in the appropriate scientific disciplines are to undertake or review the estimation of *environmental consequences* of dam failure. Both *total* and *incremental environmental consequences* are to be reported.

Human factors

Account is to be taken of *human factors*, both in terms of errors, lapses or omissions contributing to an increase in the *consequences* of failure and deliberate interventions contributing to an increase or reduction in the *consequences*. This requires consideration of such aspects as the effectiveness of emergency planning, the communication and decision processes, operator training, stress on personnel in extreme events, access for evacuations and emergency personnel, equipment and materials availability during extreme events, and security arrangements at dams.

Varying risk profile

See under this same heading in Sub-section 6.14. *Risk analysis* is to capture the varying *consequences of failure* as construction on a dam proceeds.

Uncertainty of risk values

See what is said under this same heading in Sub-section 6.14. An owner is to provide an assessment of the degree of uncertainty of estimated *consequences*.

6.16 For risk analysis, what information does DSC need?

For *risk analysis*, the essential information needed by the DSC is:

- the inputs to the analysis and the evidence in support of them;
- full documentation of the methodology followed or citation of the authoritative sources for the methods used;
- the reasoning in support of the risk values throughout the analysis; and
- the outputs of the analysis.

Within these generic categories, particular items of information needed by the DSC are outlined in the later relevant sub-sections of this sheet.

6.17 How will the DSC *public safety risk guidelines* be applied?

The *public safety risk guidelines* are in *Background to DSC Risk Policy Context* - DSC1B - Section 2, under Principle D.3.

The *public safety risk guidelines* will be applied for existing dams as follows:

1. if the best estimate of *risk to the individual* is in the *negligible region* (less than one in a million per annum) – DSC does not require any further reduction of *risk to the individual*, though any obvious low cost improvements should be made and avoidable risks should be avoided;
2. if the best estimate of *risk to the individual* is in the *intolerable region* (greater than one in ten thousand per annum) – the *normal* DSC requirement is that *risk to the individual* be

reduced as soon as reasonably practicable in a short-term and/or medium term improvement (Table 2 of DSC1B) to at least the *limit of tolerability*. Without improvement, the dam does not meet DSC requirements;

3. if the best estimate of *risk to the individual* is in the *region of tolerability review* (between one in ten thousand per annum and one in a million per annum) and the owner has other dams with *intolerable risks* – the dam normally meets DSC requirements until all *intolerable* risks on the other dams have been eliminated;

4. if the best estimate of *risk to the individual* is in the *region of tolerability review* (between one in ten thousand per annum and one in a million per annum) and the owner has no other dams with *intolerable risks* – the *normal* DSC requirement is that risk be reduced to the *negligible* level on a program agreed with the DSC unless the owner can demonstrate, to the satisfaction of the DSC, that a higher risk is *tolerable*. To be *tolerable*, the risk must be *ALARP* and the owner must demonstrate why it is tolerable to impose that level of risk on known persons. The urgency for improvement is significantly lower than for risks in the *intolerable* region (Table 2 of DSC1B). Without improvement, or a demonstration that the existing risk is *tolerable*, the dam does not meet DSC requirements;

5. if the best estimate of *societal risk* is in the *negligible region* (Figure 1 of *DSC1B*) – DSC does not require any further reduction of *societal risk*, though any obvious low cost improvements should be made and avoidable risks should be avoided;

6. if the best estimate of *societal risk* is in the *intolerable region* (Figure 1 of DSC1B) – the normal DSC requirement is that *societal risk* be reduced as soon as reasonably practicable in a short-term and/or medium-term improvement (Table 2 of *Background to DSC Risk Policy Context* - DSC1B) to at least the *limit of tolerability*. Without improvement, the dam does not meet DSC requirements;

7. if the best estimate of *societal risk* is in the *region of tolerability review* (Figure 1 of DSC1B) and the owner has other dams with *intolerable risks* – the normal DSC position is that the dam meets DSC requirements until all *intolerable* risks on the other dams are eliminated;

8. if the best estimate of *societal risk* is in the *region of tolerability review* (Figure 1 of DSC1B) and the owner has no dams with *intolerable risks* – the *normal* DSC requirement is that risk be reduced to the *negligible* level on a program agreed with the DSC unless the owner can demonstrate, to the satisfaction of the DSC, that a higher risk is *tolerable*. To be *tolerable*, the risk must be *ALARP*. The urgency for improvement is significantly lower than for risks in the *intolerable region* (Table 2 of DSC1B). Without improvement, or a demonstration that the existing risk is *tolerable*, the dam does not meet DSC requirements.

9. if the best estimate of *societal risk* is lower than the *limit of tolerability* and the estimated loss of life exceeds 1,000 (within the red box on Figure 1 of DSC1B) – the *normal* DSC requirement is that, for *failure modes* with an estimated loss of life in excess of 1,000, the dam comply with all relevant *standards* – including PMF capacity for dams without spillway gates or other discharge systems with a potential to malfunction – and with currently recognized *defensive design measures.* If improvement is needed it is to be made as soon as reasonably practicable. Without compliance the dam does not meet DSC requirements.

The requirements listed above are broadly in line with the proposed requirements for hazardous industry in New South Wales (DOP 2008).

Whilst the DSC applies its public safety risk guidelines on the basis of best estimate risks, as a matter of prudence owners should consider the level of uncertainty attaching to the risks. As uncertainty increases, there is a case to reduce risks to levels somewhat below the risk boundaries [mentioned under the nine points above] in order to maintain the defensibility of their position.

For risk-based assessment, new dams or major augmentations are to comply with the DSC *public safety risk guidelines* (DSC1B – Section 2, under Principle D.3) for those classes of dam according to similar rules to those for existing dams. Normally DSC would expect these dams to achieve *negligible* risk values because the marginal cost of extra safety is usually much less than for existing dams. Moreover, new dams are normally fully compliant with recognized *standards* and *good practice*, in which case a *risk assessment* is unnecessary.

Flood capacity during construction of new dams is an area where *risk assessment* is generally necessary and useful. For new embankment dams if it is reasonably practicable to meet the DSC *public safety risk guidelines* (under Principle D.3 of *DSC1B*) during construction of dams they are to be met. If it is not reasonably practicable to meet the *public safety risk guidelines*, the DSC will accept a flood capacity, during those phases of construction with public safety at risk, in the range of the AEP 1 in 500 to 1 in 1,000 flood discharge on the basis of world practice provided the risks are *ALARP*.

For the modification of existing dams the objective is that risks to public safety during construction will not exceed the pre-existing risks. If it is not reasonably practicable to meet that objective, the risks are to be reduced *ALARP*.

For risks during construction, the DSC will judge the *ALARP* requirement against the principles of *prevention, control* and *mitigation [PCM]* as follows:

1. *prevention* – have reasonably practicable measures been taken to prevent failure of the partly completed dam? – the measures include coffer dams, diversion tunnels or channels, and reinforced rockfill to allow substantial overflow;

2. *control* – there is limited scope to control flood failures but there are steps that can be taken as a flood develops. For example, it is necessary to make the edges of partially completed lifts of reinforced rockfill safe against overflow. Having cranes, gabions and men available for this work is a necessary control measure; and

3. *mitigation* – the DSC requires a construction phase *dam safety emergency plan (DSEP)* that has an effective flood warning system, forecast inundation levels in the event of dam failure, effective communication systems and protocols for interaction with the emergency authorities and an effective evacuation and welfare plan to protect those at risk.

6.18 How do we know that public safety risks are tolerable?

The need to demonstrate that public safety risks are *tolerable* applies to only those risks within the *region of tolerability review*.

The key principles are:

1. to be *tolerable* a risk must be *ALARP*, it must provide a benefit to society, it must be properly assessed and managed, it must be kept under review and it must be further reduced if future circumstances allow;

2. for a risk to be ALARP, the *sacrifice* (Glossary to ANCOLD 2003b) required in its reduction must be *grossly disproportionate* to the risk reduction that is achieved.

A demonstration of the tolerability of risk requires consideration, definition and costing of the possible *options for risk reduction*.

In demonstrating that a risk is *ALARP* the owner is to consider at least the following factors:

- The *disproportion* between the *sacrifice* (money, time, trouble and effort) in making the safety improvement and the *risk reduction* that is achieved.
- the level of risk in relation to the *limit of tolerability* and the *negligible* risk level;
- the *cost-effectiveness* of safety improvement options;
- any relevant recognized *good practice*; and
- any *societal concerns* revealed by the owner's consultation with the community and other stakeholders.

Guidance on *ALARP* is found in HSE (2001a), HSE (2001b), HSE (2003), HSE (2006), HSE (2008a), HSE (2008b), HSE (2008c) and Rimington et al. (2003). All but the last of these sources are on the HSE web site.

The *disproportion* issue – for *risk to the individual* the DSC expects that risk would normally be reduced to the *negligible region* of one in a million chance per annum or less. To make an ALARP case an owner would need to provide a qualitative judgment that there is *disproportion* that warrants the imposition of a higher risk to known persons. For *societal risk* disproportion can be judged by comparison of the *cost to save a statistical life (CSSL)* value for any improvement option with Table 8.6 or Table 8.7 of ANCOLD (2003b) or the interpolated value. The threshold

is the *poor justification* value ($100 million in Table 8.6). The values in the tables should be adjusted in the ratio of per capita GDP (Australia) at the time of analysis to per capita GDP (Australia) in June 2003. Based on United Kingdom measures the values in the ANCOLD tables could be multiplied by 1.6 as of June 2008. Guidance on *CSSL* is at Appendix C. At Appendix C it is shown that the value of CSSL is very sensitive to the selection of the *pre-improvement* and *post-improvement* conditions. The DSC requires that these conditions relate to the safety improvement under analysis. For a dam with existing risks in the *intolerable region*, a case by an owner that an improvement would result in risks in the *region of tolerability review* which are ALARP could only succeed if the CSSL is at least the current threshold value derived from Table 8.6 of ANCOLD (2003b). The DSC will not accept a case based on *CSSL* alone as a demonstration that risks are *ALARP*.

The *level of risk* – for both *risk to the individual* and *societal risk* the higher the level of risk the less weight will be given to the cost of achieving risk reduction. For societal risk, the level of risk is what determines whether the threshold value of *CSSL* in Table 8.6 or Table 8.7 (ANCOLD 2003b) or the appropriate interpolated value should apply.

The *cost-effectiveness* - is a measure which applies to *societal risk* and is judged by the *CSSL* value. The greater the *disproportion* between the *sacrifice* and the risk reduction which is achieved, the poorer is the *cost effectiveness* of safety improvement. For risks at or below the *limit of tolerability* the *CSSL* for further improvement of safety will typically be extremely high, in the billions of dollars. Both ERA (2008) and Marsden et al. (2007) raised the issue of whether safety improvements of such low *cost-effectiveness* are in the best interests of society. The DSC has legal advice that its charter does not permit it to consider whether available funds would be better spent on other health and safety needs of society, such as an improved health system and safer road travel. Thus for DSC, *cost-effectiveness* is a means of comparing the worth of alternative safety improvement options, against the background that very high values of CSSL are one consideration in judging that risks are ALARP.

Good practice - under the *tolerability of risk* framework developed by the HSE (2001a) *relevant good practice* is taken to be an industry consensus of what is *ALARP*. The HSE normally requires that *relevant good practice*, where it exists, is the minimum level of safety. In the HSE understanding *good practice* is an upper limit to *tolerable risk*; that is, the *good practice* is a minimum requirement for the control of risk - *relevant good practice* has a particular meaning as explained in HSE (2003).

There is no evidence that the ANCOLD *fall-back flood capacity* (ANCOLD 2000a Table 8.1) was intended to constitute an *ALARP* position because the guidelines indicate that higher risks could be justified by risk *assessment*. Paragraph 2 of Section 8 of ANCOLD (2000a) refers to *a conservative deterministic fall-back option* (the underline is by the DSC).

Having considered the historical context of safety levels within the industries regulated by HSE and for dams, the DSC has adopted this position:

1. full compliance with a DSC *standard* or *good practice* or an industry-recognized *standard* or *good practice* (where DSC has no position) will normally be accepted by the DSC as a demonstration of adequate safety in the long-term, provided the *standard* or *good practice* was intended to assure safety in the long-term; and

2. the DSC will accept risks higher than those achieved by the *standards* or *good practice* of Point 1 as been adequately safe in the long-term provided the owner can reliably demonstrate that all risks comply with the DSC *public safety risk guidelines* for safety in the long-term.

Societal concerns – these affect an ALARP position for *societal risk* and are a key issue in that regard. HSE say: *Societal concerns can arise when the realization of a risk impacts on society as a whole* (HSE 2001b paragraph 31). *Societal risk* (as measured by F-N plots) is a quantitative sub-set of *societal concerns*. Since the F-N data are judged separately, the issues here are the more subjective aspects of *societal concerns*, such as society's degree of understanding of and control over the risks, issues of dread and issues of equity and trust. Mansfield (2003) has expressed these issues as: *Society's views, fears and expectations about a hazard or risk issue*.

DSC considers that stakeholder and community consultation is needed to fully expose *societal concerns.* The sheet *Community Consultation and Communication (DSC2I)* provides some helpful advice for owners without experience or access to professional assistance. Consultation is a pre-condition for acceptance by the DSC of a risk within the *region of tolerability review* as *tolerable*. An owner could avoid consultation by a commitment to reduce all risks to the *negligible region* on a program agreed with the DSC.

An owner seeking to demonstrate that risks are ALARP is to rate *societal concerns* and is to document the basis for the rating. Aspects of significance are given in Mansfield (2003) where a model for scoring of *societal concerns* is described. The work has been carried forward by Risk Solutions into a working model for rail safety - validated and published by RSSB (2006).

If *societal concerns* rate as low, the DSC may accept a risk within the *region of tolerability review* close to the *limit of tolerability*, provided that the other considerations so indicate. If *societal concerns* rate as high, risks would normally need to be reduced to the *negligible region*. For intermediate ratings, intermediate levels of risk could be accepted.

There is a concept in risk management known as the *bow-tie concept* but more correctly called the *PCM* (*prevention*, *control* and *mitigation*) concept. For a risk to be *ALARP* it is necessary to demonstrate that all reasonably practicable measures have been taken under each of *prevention*, *control* and *mitigation*. *Prevention* refers to measures that will prevent a failure occurring. Fully intercepting filters in an earthfill dam is an example. *Control* refers to measures to arrest the progression of a failure. Sandbagging and filter blanketing of the flow from a piping

pathway is an example. *Mitigation* refers to measures to reduce the consequences of failure. Warning and evacuation of the *population at risk* is an example. Here *mitigation* has a narrower meaning than the broad meaning given for *risk mitigation* in ANCOLD 2003b. The owner is to demonstrate how each of *prevention*, *control* and *mitigation* has been addressed.

Affordability [the capacity of the owner to fund improvements] is not a consideration in judging whether risks are *ALARP* or in the need for the improvements to be implemented. This principle has been well-established by the HSE during its development of the *tolerability of risk* framework. An analogy is the registration of motor vehicles. If inspection reveals that a car needs safety improvements, the capacity of the owner to pay for those improvements is not a consideration in the registration authority's decision to grant a renewal of registration. The car will remain unregistered until the improvements are made, regardless of the owner's financial circumstances. If a dam owner cannot afford to undertake safety improvements the issue must play out through the political process – the DSC will not consider the owner's financial circumstances other than by some possible concessions in the timing of the improvements.

For the dam before improvement and after improvement, the following information is needed in support of a case that risks within the *region of tolerability review* are *tolerable*:

- the best estimate *risk to the individual*;
- the best estimate *societal risk* as an F-N plot superimposed on the DSC chart (Figure 1 of *Background to DSC Risk Policy Context - DSC1B*);
- the best estimate expected value of *potential loss of life* (aggregation of *probability of failure* multiplied by *PLL* over all failure scenarios considered) in lives per annum;
- the best estimate of expected value of *economic loss* and any *financial loss* for the existing dam (aggregation of *probability of failure* multiplied by *dollar loss* over all failure scenarios) in dollars per annum;
- the best estimate of the cost of operating and maintaining the dam in dollars per annum;
- a description of the risk reduction options that have been considered;
- for each risk reduction option, the annual time series of expenditures needed to reduce the risks;
- for each option, the *discount rate* and *analysis period* used for cost-benefit analysis, and the basis for their selection (note the requirements of NSW Treasury 2008 but see also HSE 2008c page 3, bullets 3 and 4 under "Analysis Features");
- for each option, the estimated *cost to save a statistical life (CSSL)* and where the *CSSL* rates on the Table 8.6 of ANCOLD (2003b), with the values in the table adjusted for growth in per capita *gross domestic product (GDP)*. As of June 2008 the values can be multiplied by 1.6;

- a description and results of the stakeholder and community consultation that has been undertaken to assess any *societal concerns*;
- for each option, a rating of *societal concerns*;
- for each option, the measures in place or proposed to reduce risks under each of the headings of *prevention*, *control* and *mitigation*;
- a statement of the benefits which the dam brings for society;
- the reasons of the owner for concluding that the risk within the *region of tolerability review* is *tolerable*, having regard to the foregoing information and the requirement that risks are to be *ALARP*.

On receipt of the information specified in this Sub-section 6.18, the DSC would review each case on its merits and would advise the owner if the risk is accepted as *tolerable*.

The considerable effort involved in demonstrating that risks are *ALARP* is avoided if an owner makes a commitment to reduce risks to the *negligible region* or if the owner is relying fully on the *standards-based approach* to assure safety.

6.19 What risk criteria apply?

The owner is to develop risk criteria. The national standard AS/NZS 4360:2004 and the international standard ISO 31000 say that an owner is to set risk criteria. That is compatible with the owner being responsible for dam safety. The owner's criteria need to satisfy the DSC *public safety risk guidelines*.

The DSC does not say that compliance with its requirements would discharge the dam owner's common law duty of care - owners should seek their own advice. The DSC is not competent to give owners legal advice.

For dams where lives are at risk, public safety considerations will normally be the main driver that determines the required safety levels. Where lives are not at risk or public safety risk is insignificant, other adverse impacts on society would determine the required safety levels.

The DSC has not established guidelines for the tolerability of risks that do not directly affect public safety – such as those involving economic loss, public health impacts, environmental impacts or other adverse impacts on society. Some of these impacts are subject to other legislative and regulatory requirements. The severity of the impacts tends to be case-specific to the circumstances of the affected communities.

Where the risks to public safety, to public health, to heritage values and to the environment are negligible the DSC could be guided by minimization of the total economic costs – that of dam safety improvement plus the expected value of dam failure losses.

The owner's risk criteria are to at least satisfy these requirements:

- the DSC *public safety risk guidelines* (DSC1B - Section 2, under Principle D.3);

- where lives are not at risk or it is clear that public safety should not be the main driver for the safety levels of the dam, the *risk criteria* for economic loss, public health impacts, environmental impacts and any other adverse impacts on society are to be developed by the owner in consultation with representatives of the affected community. These criteria and the reasons in support thereof, are to be provided to the DSC.

6.20 What is the safety status of the dam?

For a *safety review*, a conclusion by the owner is required as to the safety status of the dam according to the DSC rating scheme given in the table below. The basis for that conclusion is to be documented.

Safety status is to be assigned in accordance with the table below.

The normal DSC position will be:

- S1 – no safety improvement is needed – the dam is safe in the long-term;
- S2 – the owner has elected to rely on *standards* or *defensive design measures* and improvement is needed to bring one or more *failure modes* into compliance;
- R1 – risks are acceptable in the long-term;
- R2 – risks are *tolerable* and are acceptable in the long-term;
- R3 – risks are not *tolerable* but are acceptable in the medium-term;
- R4 – risks reduction is required *as soon as reasonably practicable.*

Approach	Safety Rating	Description
Standards-based [rated for the dam where all *failure modes* have recognized STD or DDM]	S1	Pass – for every failure mode *standards* or *good practice* are met or sufficient *defensive design measures* are in place.
	S2	No pass – *standards* or *good practice* are not met or some key *defensive design measures* are not present.
Risk Assessment [Total risks from dam failure]	R1	Risks are *negligible*
	R2	Risks are in the *region of tolerability review* and judged as *ALARP*
	R3	Risks are in the *region of tolerability review* and judged as not *ALARP*
	R4	Risks are *intolerable*

Owners need to recognize two points:

- The sheet, *Background to DSC Risk Policy Context - DSC1B,* allows for the *progressive improvement* of safety - the question is whether the dam has adequate safety for the particular stage (*short-term, medium-term* or *long-term*) of the improvement process; and
- Safety status cannot be final in the sense that safety is to be periodically reviewed and it is not possible to foresee what future circumstances will be. The question is whether safety is assessed as adequate on present understanding.

The conclusion by the owner on safety status completes the *safety review* report, subject only to any additional information sought or questions raised by the DSC. The DSC will judge each *safety review* on its merits and will advise the owner whether or not it agrees with the owner's conclusion on safety.

Safety reviews provided to the DSC are to include a recommendation on the *priority* and *urgency* to be assigned to any safety improvement of the dam together with an indication of the next steps in planning for the improvement.

7. SAFETY REVIEW DOCUMENTS TO BE SUBMITTED TO THE DSC

7.1 What documents does the DSC need?

The DSC requires:

- a letter of transmittal issued under the authority of the dam owner and giving the owner's conclusion on whether or not the dam meets the DSC safety requirements. Where improvement of safety is required the owner is to make a commitment to the improvement and is to state the time horizon for implementation of the improvement;
- the *safety review* report;
- the report of the independent peer reviewer(s); and
- a statement giving an account of the owner's response to the report of the independent peer reviewer(s).

7.2 What of further actions?

An owner's conclusion that the dam does not meet DSC requirements requires:

1. *short-term* improvement – a proposal and program for any such improvement;
2. *medium-term* improvement – an indicative initial program for investigation activities;
3. *long-term* improvement – any useful indications of improvements in mind that the owner could provide.

Indicative timeframes for improvements are given in *Background to DSC Risk Policy Context - DSC1B*, Table 2.

8. REFERENCES

- Abelson, P., 2003, *The Value of Life and Health for Public Policy*, Economic Record, 79, S2-S13.

- ANCOLD (Australian National Committee on Large Dams), 2000a, *Guidelines on Selection of Acceptable Flood Capacity for Dams*, March.

- ANCOLD (Australian National Committee on Large Dams), 2000b, *Guidelines on Assessment of the Consequences of Dam Failure*, May.

- ANCOLD (Australian National Committee on Large Dams), 2003a, *Guidelines on Dam Safety Management*, August.

- ANCOLD (Australian National Committee on Large Dams), 2003b, *Guidelines on Risk Assessment*, October.

- Ang, A.S. and Tang, W., 11085, *Probability Concepts in Engineering Planning and Design,* John Wiley and Sons, Inc., New York.

- Barneich, J., Majors, D., Moriwaki, Y., Kulkarni, R. and Davidson, R., 110106, *Application of Reliability Analysis in the Environmental Impact Report (EIR) and Design of a Major Dam Project,* Proceedings of Uncertainty 110106, Geotechnical Engineering Division, ASCE, August.

- Benjamin, JR and Cornell, CA 1970, *Probability, Statistics and Decision for Civil Engineers*, McGraw-Hill Book Company.

- Chilton, S, Dolan, P, Jones-Lee, M, Loomes, G, Robinson, A, Carthy, T, Covey, J, Spencer, A, Hopkins, L, Pidgeon, N and Beattie, J, 2000, *Valuation of Benefits of Health and Safety Control*, Contract Research Report 283/2000 prepared for Health and Safety Executive by Department of Economics, University of Newcastle-upon-Tyne, Department of Economics, University of York, School of Psychology, University of Wales and Experimental Psychology, University of Sussex.

- CIRIA [Construction Industry Research and Information Association, United Kingdom], 11088, *Rationalization of Safety and Serviceability Factors in Structural Codes*, Report 63, July.

- Dartmouth Flood Observatory

- www.dartmouth.edu/~floods

- DOP (NSW Department of Planning), 2008, *Risk Criteria for Land Use Safety Planning (Consultation Draft)*, HIPAP No.4, July.

- ERA (Economic Regulation Authority, Western Australia), 2008, *Revised Final Report – Inquiry on Harvey Water Bulk Water Pricing*, 22 June.

- FERC (Federal Energy Regulatory Commission, United States), 110103, *Selecting and Accommodating Inflow Design Floods for Dams*, Chapter 2, Engineering Guidelines for the Evaluation of Hydropower Projects, October.

- FERC (Federal Energy Regulatory Commission, United States), 2005, *Dam Safety Performance Monitoring Program*, Chapter 14, Engineering Guidelines for the Evaluation of Hydropower Projects, 1 July.

- Fell, R, Wan, C-F and Foster, M, 2004, *Methods for Estimating the Probability of Failure of Embankment Dams by Internal Erosion and Piping – Piping through the Embankment*, UNICIV Report R-428, University of New South Wales, May

- Fell, R and Wan, C-F, 2005, *Methods for Estimating the Probability of Failure of Embankment Dams by Internal Erosion and Piping in the Foundation and from Embankment to Foundation*, UNICIV Report R-436, University of New South Wales, January

- Graham, W.J., 1101010, *A Procedure for Estimating Loss of Life Caused by Dam Failure*, DSO-1010-06, U.S. Department of the Interior, Bureau of Reclamation, Denver Colorado.

- http://www.usbr.gov/research/dam_safety/documents/dso-1010-06.pdf

- Graham, W.J., 2006, *Dam Failures in the United States and a Procedure for Estimating the Consequences of Future Failures*, DSO-2006-01, U.S. Department of the Interior, Bureau of Reclamation, Technical Service Center, Denver, Colorado; Sedimentation and River Hydraulics Group, Draft 28 October.

- Haasl, D.F., Roberts, N.H., Vesely, W.E. and Goldberg, F.F., 11080, *Fault Tree Handbook,* US Nuclear Regulatory Commission, NUREG-04102, March.

- Hartford, D N D and Baecher, G B, 2004, *Risk and Uncertainty in Dam Safety*, CEA Techmologies Dam Safety Interest Group, Thomas Telford Ltd, London.

- Hawk, J K, 110101, *A Comprehensive Approach to the Evaluation of Spillway Adequacy*, Association of State Dam Safety Officials Conference, San Diego, California, USA, September/October.

- Hill, P., McDonald, L. and Payne, E., 2008, *Incremental Consequences of Dam Failure and the ANCOLD Hazard Classification System*, NZSOLD/ANCOLD Dam Safety Workshop, Queenstown, New Zealand, 21 November.

- HSE (Health and Safety Executive, United Kingdom), 2001a, *Reducing Risks, Protecting People,* Her Majesty's Stationery Office, London, www.hse.gov.uk/risk/theory/r2p2.pdf .

- HSE (Health and Safety Executive, United Kingdom), 2001b, *Principles and Guidelines to Assist HSE in its Judgements that Duty-Holders Have Reduced Risk As Low As Reasonably Practicable,* Internal Guide, www.hse.gov.uk/risk/theory/alarp1.htm, December.

- HSE (Health and Safety Executive, United Kingdom), 2003, *Assessing Compliance with the Law in Individual Cases and the Use of Good Practice,* Internal Guide, www.hse.gov.uk/risk/theory/alarp2.htm, May.

- HSE (Health and Safety Executive, United Kingdom), Nuclear Safety Directorate-Business Management System, 2006, *Technical Assessment Guide: Demonstration of ALARP*, T/AST/005, www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast005.pdf, 6 December.

- HSE (Health and Safety Executive, United Kingdom), 2008a, *ALARP "at a glance",* www.hse.gov.uk/risk/theory/alarpglance.htm, April (download date).

- HSE (Health and Safety Executive, United Kingdom), 2008b, *HSE Principles for Cost Benefit Analysis (CBA) in Support of ALARP Decisions,* www.hse.gov.uk/risk/theory/alarpcba.htm, April (download date).

- HSE (Health and Safety Executive, United Kingdom), 2008c, *Cost Benefit Analysis (CBA) Checklist,* www.hse.gov.uk/risk/theory/alarpcheck.htm, April (download date).

- ICOLD (International Commission on Large Dams), 2005, *Risk Assessment in Dam Safety Management – A Reconnaissance of Benefits, Methods and Current Applications,* Bulletin No. 130.

- Le Guen, J, 2008, *Tolerability of Risk: UK Principles for Controlling Work Activities*, Workshop on Tolerable Risk Evaluation sponsored by US Army Corps of Engineers, US Bureau of Reclamation and US Federal Energy Regulatory Commission, Alexandria, Virginia, USA, 18-110 March.

- Mansfield, D, 2003, *Gauging Societal Concerns*, Hazards XVII Conference and Workshops, IChemE North West Branch, UMIST, Manchester, UK, 24-28 March.

- Marsden, J, McDonald, L, Bowles, D, Davidson, R and Nathan, R, 2008, *Dam Safety, Economic Regulation and Society's Need to Prioritise Health and Safety Expenditures*, NZSOLD/ANCOLD Workshop *Promoting and Ensuring the Culture of Dam Safety*, IPENZ Proceedings of Technical Groups, Vol. 33, Issues 1 and 2 (LD), ISSN 0111-10532, Queenstown, New Zealand, 21 November.

- New South Wales Treasury, Office of Financial Management, 2008, *NSW Government Guidelines for Economic Appraisal*, Treasury Policy and Guidelines Paper TPP08-5, July.

- NRM (Department of Natural Resources and Mines, Queensland), 2000, *Queensland Dam Safety Management Guidelines*, February.

- NRM (Queensland Department of Natural Resources and Mines), 2002, *Guidance on the Assessment of Tangible Flood Damages*, September.

- Rimington, J, McQuaid, J and Trbojevic, V, 2003, *Application of Risk-based Strategies to Workers' Health and Safety Protection: UK Experience*, August.

- RSSB (Rail Safety and Standards Board, United Kingdom), 2006, *Development and Calibration of a Model for Gauging Societal Concern for the Railway Industry*, Report No. D4182R3,

- http://www.rssb.co.uk/pdf/reports/research/t518%20modelling%20societal%20concerns.pdf

- SA/SNZ (Standards Australia/Standards New Zealand), 2004a, *Risk Management,* AS/NZS 4360:2004.

- SA/SNZ (Standards Australia/Standards New Zealand), 2004b, *Risk Management Guidelines,* Companion to AS/NZS 4360:2004.

- TDFRG (Teton Dam Failure Review Group), 11088, *Failure of Teton Dam – A Report of Findings*, April.

- Vroman, N D, Sills, G L, Cyganiewicz, J, Fell, R, Foster, M and Davidson, R R, 2008, *A Unified Method for Estimating Probabilities of Failure of Embankment Dams by Internal Erosion and Piping*, NZSOLD/ANCOLD Conference on Dams, Queenstown, New Zealand, 110-20 November.

Appendix A

Terminology for this Sheet

In the first place, the terminology recognized in this guidance sheet is that given in the Glossary to ANCOLD (2003b), except for these modified definitions:

Complementary cumulative distribution function (CCDF)	*The integral of the probability density function calculated in the direction of decreasing values of the random variable. Thus the probability that the random variable takes on values greater than a particular value can be read from the CCDF.*
F-N curves	*Curves that relate F (the probability per year of causing N or more fatalities) to N. Such curves may be used to express societal risk to life criteria and to describe the safety levels of particular facilities (such as a dam).*
Risk evaluation	*The process of examining and judging the significance of risk. The risk evaluation stage is the point at which values (societal, regulatory, legal and owner's) and judgements enter the decision process, explicitly or implicitly, by including consideration of the importance of the estimated risks and the associated social, environmental, economic, and other consequences, in order to evaluate a range of alternatives for managing the risks (ANCOLD 2003b). Risk evaluation involves a comparison of the estimated risks with risk criteria (SA/SNZ 2004).*
Risk mitigation	*A selective application of appropriate techniques and management principles to reduce consequences in the event a risk is realized.*

In the second place, for any definitions not given in ANCOLD (2003b), the definitions of ANCOLD (2003a) will apply, except as follows:

Safety review	*The assessment of dam safety by methodical examination of all design and surveillance records and reports, and by the investigation and analysis of matters not addressed previously or of items subject to new design criteria or possible deterioration (ANCOLD 2003a). It is a procedure for systematically assessing the safety of a dam after its original construction (NRM 2002). Such a review is based on contemporary knowledge, guidelines, sources, analysis methods and information, including information obtained by investigations specifically undertaken for the review. A safety review may be comprehensive (covering all aspects of the safety of the dam) or particular (covering only nominated aspects of safety – for example, flood capacity).*

In the third place, all definitions from ANCOLD guidelines that are not covered in the first and second place, just outlined, will apply. DSC has adopted the following additional definitions:

Failure modes analysis	*A systematic process for identifying the credible failure modes and failure mechanisms that could potentially endanger a dam. For each credible hazard (identified from hazard analysis), the analyst considers the way in which the dam and its constituent elements could fail to function as intended so as to result in a partial or complete loss of function and ultimate failure of the dam. Failure modes analysis includes the identification of failure mechanisms, the succession of failures required at various levels in the dam system to result in failure of the dam.*
Potential loss of life (PLL)	*The best estimate of the loss of life in the event of a flood. The term "flood" is qualified as "due to the unlikely failure of a dam" or as "due to a natural flood without dam failure".*

Appendix B

Failure Modes Analysis

The sources cited in this appendix are listed under References to the main text of this sheet.

What is the Relationship of Failure Initiators, Failure Mechanisms, Failure Modes and Failure Effects?

ICOLD (2005) states:

A failure mode describes how element or component failures must occur to cause loss of the sub-system or system function.

And again:

Each failure mode can be due to one or more hazards or failure mode initiators. Typically for dams, these failure mode initiators are extreme storms, earthquakes, design and construction flaws in conjunction with normal hydraulic loads, and human agency (mis-operation, sabotage etc.).

And:

A failure mechanism describes the physical processes and states that must occur, in accordance with natural laws, for the failure mode to progress from failure mode initiation (cause) through to the realisation of ultimate failure effect of interest.

And:

A failure effect is a consequence (not to be confused with the downstream consequences of dam-break flooding) of a failure mode in terms of the operation or performance of the dam system. Failure effects are propagated through the system along the failure mechanisms.

The relationship can be understood by considering a typical event tree used in risk analysis of dam safety. For example, consider an event tree for piping that initiates under high flood surcharge. Figure A.1 (after Vroman et al. 2008), which is not an event tree, shows the steps in the piping process. In this example:

1. the whole process is the failure mode – piping;
2. the failure initiator is the high reservoir water level;
3. the failure mechanism is the sequence of events represented by the event tree that describes the process; and
4. the effect is the consequence for the next step in the process of the outcome at the step of interest.

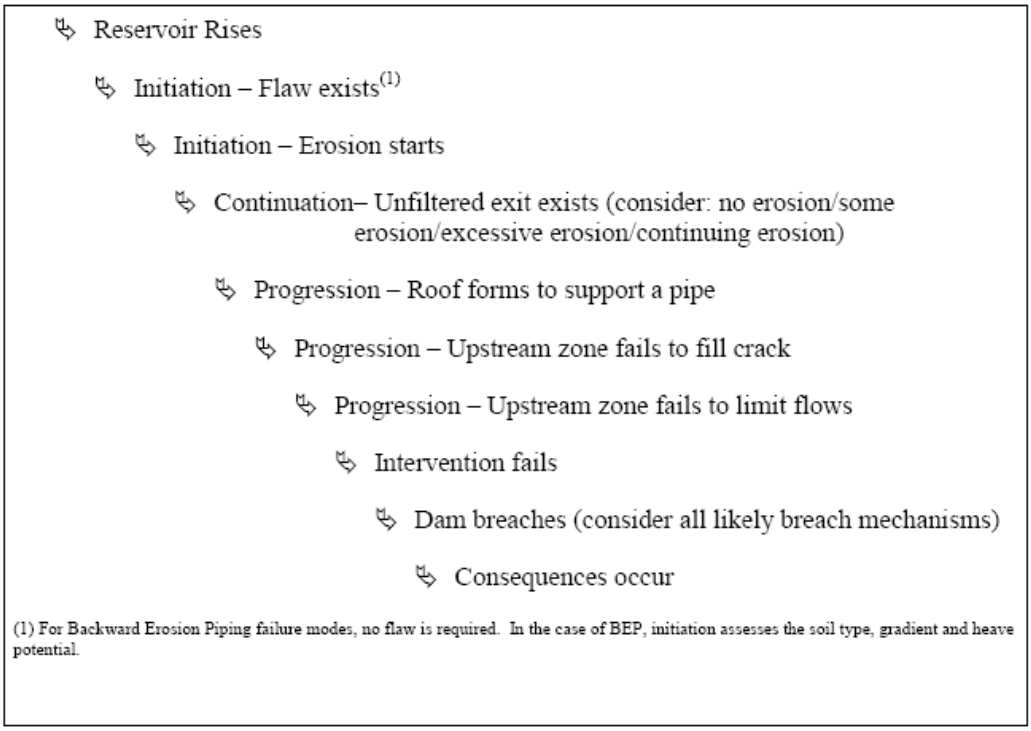
How is *failure modes analysis* to be undertaken?

Guidance is available in ANCOLD (2003), ICOLD (2005), FERC (2005) or any text or source that describes Failure Modes and Effects Analysis (FMEA).

The essential steps in *failure modes analysis* are:

1. list all key elements of a dam, the failure of which to function as intended could affect safety (the filter zone is such a key element, the guardrail on the dam crest may not be a key element);
2. for each hazard, identified from *hazard analysis*, list all conceivable ways in which the element may fail to function as intended;
3. rate the likelihood that the element will fail to function as intended;

4. rate the consequences (for the safety of the dam system – not downstream of the dam) if the element fails to function as intended;
5. from the preceding steps, build up the *failure mechanisms* that could occur (normally using logic systems such as *event trees* or *fault trees*); and
6. decide which *failure modes* (combination of *hazards* and *failure mechanisms*) are sufficiently plausible to require analysis in a *safety review.*



B.1 – Piping Failure Process (after Vroman et al. 2008)

Appendix C

Some Notes on Cost to Save a Statistical Life [CSSL]

The sources cited in this appendix are listed in the references to the main text.

The Aim

ANCOLD has based its interpretation of the ALARP principle on the understanding developed by the United Kingdom Health and Safety Executive (HSE 2001a). There are several considerations in reaching a judgment that risks are ALARP [ANCOLD 2003b]. The aim here is to provide an understanding of the concept of *cost to save a statistical life* (CSSL) and its significance to the ALARP principle.

The Computation of CSSL

The CSSL value is effectively the value that would need to be assigned to a life to obtain a cost/benefit ratio of 1.0. The formula for computation of CSSL is:

$$CSSL = \frac{C_{PA} - \left[E(L)_B - E(L)_A\right] - \left[(O)_B - (O)_A\right]}{\left[E(PLL)_B - E(PLL)_A\right]}$$

where

CSSL = the cost to save a statistical life, dollars

C_{PA} = the annualized cost of safety improvements, dollars per annum

$E(PLL)_B$ = the product of probability of failure and potential loss of life before improvement, lives per annum. We obtain this value by taking the product for each failure scenario and then summing over all scenarios

$E(PLL)_A$ = the product of probability of failure and potential loss of life after improvement, lives per annum. We obtain this value by taking the product for each failure scenario and then summing over all scenarios

$E(L)_B$ = the product of probability of failure and dollar losses before improvement, dollars per annum

$E(L)_A$ = the product of probability of failure and dollar losses after improvement, dollars per annum

$(O)_B$ = the annual cost of operation and maintenance before improvement, dollars per annum

$(O)_A$ = the annual cost of operation and maintenance after improvement, dollars per annum

Measurement Issues

How *CSSL* is measured has a major impact on the resultant value.

On Figure C.1 the vertical axis is a conceptual representation of the numerator of the *CSSL* formula given under the preceding sub-heading. The horizontal axis represents the denominator, though it runs in the opposite direction from the normal convention. The slope of a line or curve on the graph is thus a representation of *CSSL*. The left hand end of the curved line represents an existing condition of high public safety risk which is above the *limit of tolerability* [represented by the vertical dashed line]. The right hand end of the curved line is an ultimate safety position where risk is well below the *limit of tolerability*. The curved line itself represents a track of infinitesimally small increments of safety improvement.

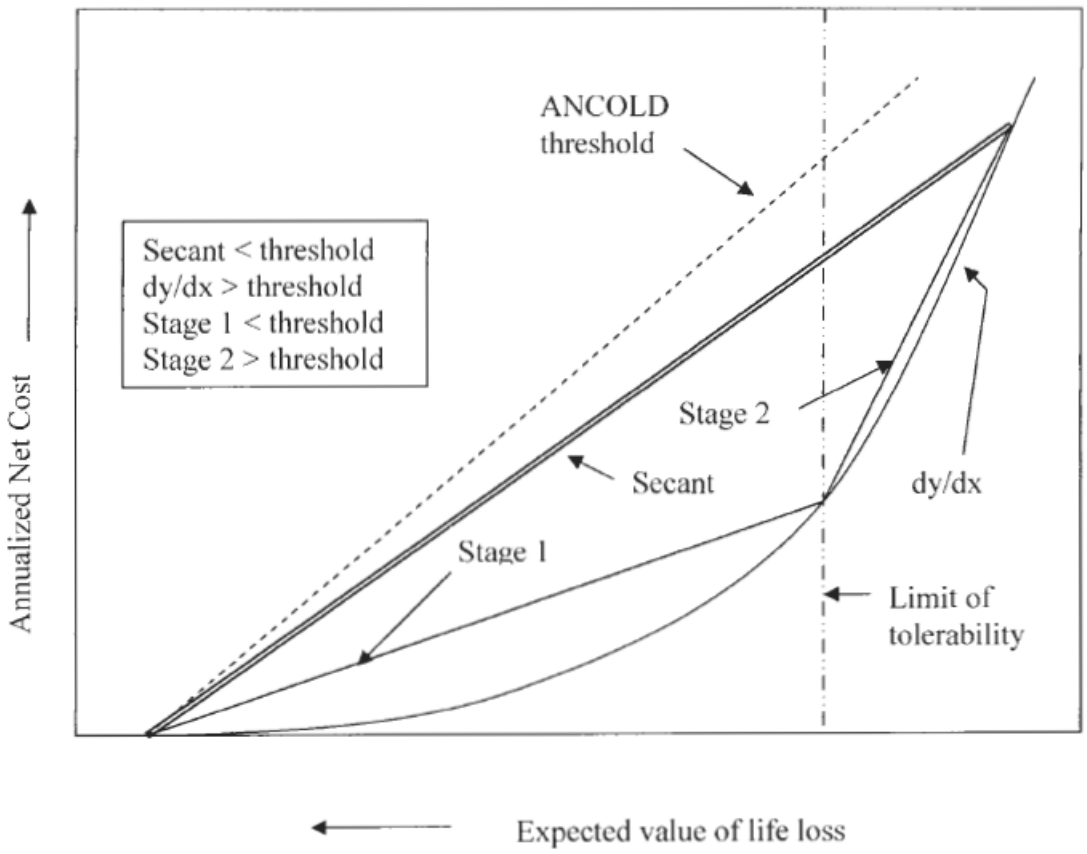


Figure C.1 – Variation of CSSL with Measurement Basis

These points are seen:

1. if safety is improved in one stage from the existing condition to the ultimate condition [the line labeled *secant*] the *CSSL* is less than the ANCOLD threshold [represented by the sloping dashed line];
2. if risks are reduced to the *limit of tolerability* in a first stage of improvement and a later second stage of improvement takes risks to the ultimate condition, the first stage *CSSL* is well below the ANCOLD threshold but the second stage *CSSL* is well above the threshold; and
3. any further improvement beyond the ultimate condition [represented by the slope of the curved line at the ultimate condition] the *CSSL* will be even higher still.

Analysts experienced in estimating CSSL recognize these realities.

The Concept of a Proportion Factor

The concept of *gross disproportion* (*Edwards v. The National Coal Board* judgment), led the HSE to develop a form of cost-benefit analysis to aid in the judgment as to whether risks are ALARP. HSE (2001a – Appendix 3) and HSE (2001b) give the fundamental concepts of the demonstration of ALARP as:

1. the *risk reduction* achieved by safety improvements;
2. the *sacrifice* required to achieve the improvements;
3. *gross disproportion* between the two in favour of safety.

With regard to public safety, those concepts are expressed in these terms:

1. the VPF (*value in preventing a fatality*);

2. the CPF (*cost of preventing a fatality*), called by ANCOLD (2003b) the CSSL (*cost-to-save-a-statistical-life*);
3. the *proportion factor* (the ratio of CPF to VPF).

The VPF is found from *willingness to pay* studies. The study underlying the value of £1,000,000 used by HSE [2001a] is reported by Chilton et al (2000). That value had been adjusted as at March 2008 to £1,583,000 [Le Guen, 2003]. The CSSL values in the ANCOLD [2003b] Tables 8.6 and 8.8 could be increased in proportion – that is, multiplied by 1.583 – say by 1.6 at June 2008. ANCOLD (2003b) recognized the HSE value because no *willingness to pay* values had been found for Australia at that time [2003]. Australian values are now available and Abelson [2003] has proposed a VPF of AUD2,700,000 - which could now be escalated according to the growth in Australian per capita GDP.

The CPF [CSSL in DSC terminology] is found from cost-benefit analysis of the particular safety improvements and is the value that would need to be placed on a life to achieve benefits equal to costs. The *proportion factor* is the ratio of CPF to VPF. A sufficiently high *proportion factor* means there is *gross disproportion*.

Values of the Proportion Factor

HSE has developed a sliding scale of *proportion factor*, according to the existing level of risk. In the 1949 case in England of *Edwards vs The National Coal Board*, the Court of Appeal held that (HSE, 2001b – paragraph 6):

> *…..in every case, it is the risk that has to be weighed against the measures necessary to eliminate the risk. The greater the risk, no doubt, the less will be the weight to be given to the factor of cost.*

(The underline is that of DSC.)

HSE (2001b – paragraph 26) say:

> *…..we believe it is right that the greater the risk, the higher the proportion may be before being considered 'gross'. But the disproportion must always be gross.*

Some documented values for the *proportion factor* are available. Paragraph 10 of HSE (2002) is worth quoting:

If the ALARP demonstration employs a comparison of costs and risk reduction benefits to rule out an improvement, it must be shown that the costs of the improvement would be "grossly disproportionate". The law does not recognize an acceptable region other than when ALARP has been met so there is unlikely to be any sympathy in the courts for parity of costs and benefits even at the TOR (tolerability of risk) *broadly acceptable level. Advice from HSE solicitors is that the courts would still seek "gross disproportion". There is no precise legal factor or HSE algorithm for gross disproportion. For the purposes of this TAG* (technical assessment guide)*, it is suggested that the evidence given by John Locke, then Director General of HSE, at the Sizewell B Public Inquiry provides a starting point. Although this evidence was produced sometime ago, no subsequent legal proceedings or public inquiries have countered these views or provided alternatives. In his evidence John Locke suggested a proportion factor of up to 3 for workers. For risks to the public the factor would depend on the level of risk, and where the risks were low (consequence and likelihood) a factor of about 2 is suggested, whereas for higher risks the factor would be about 10 times.*

(Paragraph on radiation doses omitted).

For our purposes, it is suggested that a factor of less than 10 in the vicinity of the intolerable region is unlikely to be acceptable and, for hazards that can cause large consequences, the factor may need to be larger still.

(The underline is that of DSC.)

Rimington et al. (2003 – sub-section 2.5.5), speaking of hazardous industry risks generally (not just nuclear), say:

It is taken as axiomatic that at all levels of risk there should be some bias in favour of safety, so that for risks above the broadly acceptable level we should be prepared to pay rather more than the estimated value of any increment of risk reduction to achieve it. (Less relevant text omitted). *HSE have suggested in the past a multiplicand of 3 applied to the estimated value of an increment of risk reduction at risk levels near the tolerability limit* (in this context, means the *broadly acceptable* level), *but higher figures up to a multiplicand of 10, have also been suggested at the topmost area of the tolerability region.*

(The underline is that of DSC.)

Interpretation Underpinning ANCOLD Tables 8.6 and 8.7 [ANCOLD 2003b]

In the HSE approach, we can recognize a sliding scale of *proportion factors* as follows:

- for risks in the *intolerable region* (above the *limit of tolerability*) – an infinite *proportion factor*;
- for risks within the upper part of the *region of tolerability review* – a *proportion factor* of about 10, though *societal concerns* or a large number of fatalities may require a higher value;
- for risks within the lower part of the *region of tolerability review* – a *proportion factor* of 2 (HSE, 2002 – point 9 of sub-section 5.2) or 3 (Rimington et al., 2003 – sub-section 2.5.5), though *societal concerns* or a large number of fatalities may require a higher value;
- for risks within the middle of the *region of tolerability review* – a *proportion factor* of say 6 [by interpolation], though *societal concerns* or a large number of fatalities may require a higher value;
- for risks within the *negligible region* – nobody worries too much about further risk reduction unless there are some obvious low cost improvements that could be made (Rimington et al., 2003 – sub-section 2.4).

Note that Rimington et al. (2003) say this at sub-section 2.4:

> *a broadly acceptable level* [the DSC *negligible* level] *of risk, i.e., one so low that it is not worth searching for further reduction, though any obvious inexpensive precautions would be taken…..*

So this discussion of *proportion factors* is what underlies the relativity of values in Tables 8.6 and 8.8 in ANCOLD (2003b).

Judgement that Risks Are ALARP is not an Exercise in Mathematics

Paragraph 14, Appendix 3 of HSE [2002a] states:

Moreover, it is also important to note that when HSC/E regulate, VPF [value of preventing a fatality] *is not the only factor in balancing costs against risks since a CBA* [cost benefit analysis] *informs, but does not determine, the decisions on measures that should be adopted to control the risk. As already explained, the final decision may take into account wider political and equity considerations as to whether costs are grossly disproportionate to benefits.*

(The underline is that of DSC.)

The formal position of HSE is that they do not have a numerical guide to the *proportion factor*. For instance, they say (HSE, 2001b – paragraph 27):

HSE has not formulated an algorithm which can be used to determine the proportion factor for a given level of risk. The extent of the bias must be argued in the light of all the circumstances.

This Guidance Sheet is one of a series available from our Website at:

http://www.damsafety.nsw.gov.au

In order to read this file you need a Portable Document Format (PDF) reader. A free PDF reader is available from http://www.adobe.com/

For any further information please contact:

NSW Dams Safety Committee
Level 3, Macquarie Tower
10 Valentine Avenue, Parramatta NSW 2150

PO Box 3720, Parramatta NSW 2124

(02) 9842 8073 (02) 9842 8071

dsc@damsafety.nsw.gov.au

ISSN 1039-821X