

# TABLE OF CONTENTS

Page

|         |   |        |
|---------|---|--------|
| A-9     | Governance and Guidelines .....                   | A-9-1  |
| A-9.1   | Key Concepts .....                                | A-9-1  |
| A-9.1.1 | Background .....                                  | A-9-1  |
| A-9.1.2 | Terminology/Definitions.....                      | A-9-2  |
| A-9.1.3 | Agency References .....                           | A-9-3  |
| A-9.2   | Risk Framework.....                               | A-9-3  |
| A-9.2.1 | Risk Analysis .....                               | A-9-5  |
| A-9.2.2 | Risk Assessment .....                             | A-9-5  |
| A-9.2.3 | Risk Management .....                             | A-9-5  |
| A-9.2.4 | Risk Communication .....                          | A-9-6  |
| A-9.3   | Types of Risk .....                               | A-9-6  |
| A-9.3.1 | Incremental Risk .....                            | A-9-7  |
| A-9.3.2 | Non-Breach Risk.....                              | A-9-7  |
| A-9.3.3 | Residual Risk .....                               | A-9-8  |
| A-9.4   | Risk Measures.....                                | A-9-8  |
| A-9.4.1 | Individual Risk.....                              | A-9-9  |
| A-9.4.2 | Background Risk.....                              | A-9-9  |
| A-9.4.3 | Individual Risk Concepts from Other Agencies..... | A-9-10 |
| A-9.4.4 | Societal Risk/Annualized Life Loss.....           | A-9-12 |
| A-9.4.5 | Societal Risk Concepts from Other Agencies.....   | A-9-14 |
| A-9.4.6 | Annualized Probability of Failure.....            | A-9-15 |
| A-9.4.7 | Other Potential Measures of Risk .....            | A-9-16 |
| A-9.5   | Risk Analysis .....                               | A-9-18 |
| A-9.5.1 | Portrayal of Risk .....                           | A-9-19 |
| A-9.5.2 | Risks Considered by Agencies.....                 | A-9-19 |
| A-9.5.3 | Building the Dam or Levee Safety Case.....        | A-9-23 |
| A-9.6   | Risk Assessment .....                             | A-9-23 |
| A-9.6.1 | Principles.....                                   | A-9-24 |
| A-9.6.2 | Tolerable Risk/Justification to Take Action.....  | A-9-24 |
| A-9.6.3 | ALARP .....                                       | A-9-27 |
| A-9.6.4 | Other Considerations .....                        | A-9-29 |
| A-9.6.5 | Uncertainty.....                                  | A-9-29 |
| A-9.6.6 | Confidence .....                                  | A-9-29 |
| A-9.6.7 | The Safety Case .....                             | A-9-30 |
| A-9.6.8 | Approach to Making Risk Informed Decisions.....   | A-9-30 |
| A-9.6.9 | Example Comparison of f-N and F-N.....            | A-9-32 |

|       | Page                     |        |
|-------|--------------------------|--------|
| A-9.7 | Risk Management .....    | A-9-34 |
| A-9.8 | Risk Communication ..... | A-9-39 |
| A-9.9 | References.....          | A-9-41 |

## Tables

|       | Page  |        |
|-------|---|--------|
| A-9-1 | Risk, Confidence, and Actions.....                                    | A-9-26 |
| A-9-2 | Example Potential Failure Mode Event Tree End Branch<br>Summary ..... | A-9-32 |
| A-9-3 | Cumulative Curve Development.....                                     | A-9-33 |
| A-9-4 | Joint Federal Risk Categories .....                                   | A-9-37 |

## Figures

|       | Page  |        |
|-------|---|--------|
| A-9-1 | Relationship between risk analysis, risk assessment, and<br>risk management. ....   | A-9-4  |
| A-9-2 | The four inundation scenarios.....  | A-9-7  |
| A-9-3 | Residual risk.....  | A-9-8  |
| A-9-4 | Background probability of death (from the CDC, 2005).....   | A-9-10 |
| A-9-5 | Framework for dealing with risk (LeGuen 2008).....  | A-9-11 |
| A-9-6 | Milestones in the development of societal risk guidelines<br>(Adapted from Ball and Floyd 1998).....  | A-9-13 |
| A-9-7 | Reclamation's Dam Safety Public Protection Guidelines<br>(Reclamation 2011).....  | A-9-20 |
| A-9-8 | USACE Risk Guidelines for Existing Dams (USACE 2014).<br>(a) – Individual Guideline for Incremental Risk;<br>(b) – Societal Guideline for Incremental Risk..... | A-9-21 |
| A-9-9 | Comparison of f-N and F-N plots.....  | A-9-35 |

## A-9 Governance and Guidelines

### A-9.1 Key Concepts

#### A-9.1.1 Background

Agencies, owners, and regulators have been using risk for quite some time to inform decisions within various industries across the world. In particular, the United States, the United Kingdom, the Netherlands, and Hong Kong have integrated risk into safety decisions in various ways since the 1960s (Ball and Floyd 1998). In the UK, the Health & Safety Executive (HSE) (2001) was one of the first agencies to address individual and societal risk concerns through regulation of worker safety. Although not specifically related to dams, the HSE risk framework provided the basis for much of today's international dam safety risk guidelines.

Those that analyze, evaluate, and manage risks have found that risk provides a rigorous, systematic, and thorough process that improves the quality of, and support for, safety decisions. In addition, several international entities in the dam safety industry have been using risk to inform decisions since the late 1980s. Notably, the Australian National Committee on Large Dams (ANCOLD) (2003) and British Columbia Hydro (BC Hydro) (1995) adopted risk management strategies to assess and manage risks for their dams.

For entities that own or regulate dams, various decisions are made regarding an individual structure or a portfolio of structures, including decisions about:

- The safety of a structure
- Necessary actions to reduce risks
- Prioritization of actions for a portfolio of structures

In 1979, a committee of Federal agency representatives commissioned by the President developed the Federal Guidelines for Dam Safety (Federal Emergency Management Agency 2005) to promote prudent and reasonable dam safety practices among Federal agencies. While the Federal Guidelines recognized that risk-based analysis was a recent addition to the tools available for assessing dam safety, they encouraged agencies to conduct research to refine and improve the techniques necessary to apply risk-based analysis to dam safety issues:

*The agencies should individually and cooperatively support research and development of risk-based analysis and methodologies as related to the safety of dams. This research should be directed especially to the fields of hydrology, earthquake hazard, and potential for dam failure. Existing agency work in these fields should be continued and expanded more specifically into developing risk concepts useful in evaluating safety issues. (see Federal Coordinating Council for Science Engineering and Technology 2004).*

Although decisions can be made amongst various alternatives based on relative risks, it is also useful to compare risk estimates to established risk guidelines to help in making decisions with respect to the need to further reduce risk. The Bureau of Reclamation (Reclamation) and the United States Army Corps of Engineers (USACE) operate their dam safety programs under such guidelines. Although there are some fundamental differences with respect to the way the guidelines are viewed and exercised, in general they are very similar, and are similar to guidelines developed by other water resources agencies. However, it must be stressed that these are guidelines and were never intended to be operated as strict criteria, since risk estimates can only be regarded as approximate.

### A-9.1.2 Terminology/Definitions

This section relies on the definitions contained in the Federal Guidelines for Dam Safety Risk Management (Federal Emergency Management Agency 2015). Some of these definitions conflict with other industries as noted by The Office of Management and Budget (OMB) in its guidance to agencies related to risk procedures (OMB 2007). Some of these definitions are different than the definitions included in agency-specific documents and guidance. USACE has opted to use the OMB definitions. However, for the purposes of this document, the definitions contained in the Federal Guidelines for Dam Safety Risk Management are presented.

**Risk** – The product of the likelihood of a structure being loaded, adverse structural performance, (e.g., dam failure), and the magnitude of the resulting consequences.

**Risk Analysis** – A qualitative or quantitative procedure that identifies potential modes of failure and the conditions and events that must take place for failure to occur. A quantitative risk analysis yields a numerical estimate of the risk of adverse consequence, multiplying the probability of load times the probability of dam failure given the load times the magnitude of adverse consequence given dam failure.

**Risk Assessment** – The process of considering the quantitative or qualitative estimate of risk, along with all related social, environmental, cost, temporal, and other factors to determine a recommended course of action to mitigate or accept the risk.

**Risk Evaluation** – The qualitative or quantitative description of the nature, magnitude, and likelihood of the adverse effects associated with a hazard. A risk evaluation often includes one or more estimates of risk, a risk description, risk management options, economic and other evaluations, and estimates of changes in risk attributable to the management options.

**Risk Management** – Actions implemented to communicate the risks and either accept, avoid, transfer, or control the risks to an acceptable level considering associated costs and benefits of any action taken.

### A-9.1.3 Agency References

Primary documents that provide agency policy on risk guidelines include:

- Bureau of Reclamation, Dam Safety Public Protection Guidelines, Dam Safety Office, Denver, Colorado, August 2011 (Reclamation 2011).
- U.S. Army Corps of Engineers (USACE), Safety of Dams – Policy and Procedures, ER-1110-2-1156, March 31, 2014 (USACE 2014)
- USACE, Levee Safety Program – Policy and Procedures, EC 1110-2-6072, in draft.

## A-9.2 Risk Framework

Using risk to inform decisions involves three distinct components. These components, each having their own purpose and function, are:

- Risk analysis
- Risk assessment
- Risk management

Figure A-9-1 shows how risk analysis, risk assessment, and risk management relate to each other. While the main components of risk-informed decision making are risk analysis, risk assessment, and risk management, there are activities that dominate the completion of each component:

- For risk analysis, the key activity is risk estimation
- For risk assessment, the key activity is risk evaluation
- For risk management, the key activity for dams with high risk is risk reduction

Risk communication, although not specifically identified on figure A-9-1, is a critical part of each component of risk management.



**Figure A-9-1.—Relationship between risk analysis, risk assessment, and risk management.**

The term risk, when used in the context of dam safety, is comprised of three parts:

1. The likelihood of occurrence of a load (e.g., flood, earthquake, etc.)
2. The likelihood of an adverse structural response (e.g., dam failure, damaging spillway discharge, etc.) given the load
3. The magnitude of the consequences resulting from that adverse event (e.g., life loss, economic damages, environmental damages, etc.) given that it occurs

Typically, the direct consequences of dam failure are estimated. Indirect consequences could also result, in which failure of the dam results in loss or failure of key facilities, which can ultimately lead to additional economic consequences or loss of life. If indirect consequences can be identified and estimated, they can be incorporated into the risk estimates. In some cases, it may not be possible to capture all of the indirect consequences.

Risk estimates typically reflect the risk at a given dam at the snapshot in time when the risk analysis is performed. It is recognized that the conditions at the dam will likely change in the future and the consequences of dam failure may also change as development occurs within potential dam failure inundation boundaries. This potential future increase in consequences and failure probability due to deterioration can be taken into account as part of a long-term consideration of risk.

### **A-9.2.1 Risk Analysis**

Risk analysis is the first component of risk management. It is the portion of the process in which the potential failure modes, structural performance, and adverse consequences are identified. It is also the process during which a quantitative or qualitative estimate of the likelihood of occurrence and magnitude of consequence of these potential events is made. A critical first step in a risk analysis is identifying the specific potential failure modes that are most likely at a given dam. The frequency of occurrence of the loadings (e.g., reservoir load levels, floods, earthquakes, ice loading, etc.) that could initiate potential failure and then cause adverse consequences is estimated and considered as part of a risk analysis.

### **A-9.2.2 Risk Assessment**

Risk assessment is the process of examining the safety of a specific structure and recommending decisions on a given dam or project using risk analysis, risk estimates, and other information that have the potential to influence the decision. The risks are assessed by the dam owner and, if applicable, the regulator, owner's engineer, or other decision-makers and stakeholders. The assessment considers all factors (e.g., likelihood, consequences, cost, environmental impacts, etc.) and may also use evaluation criteria established by the owner or regulator. Decisions to take action to reduce or better understand risk may include additional or enhanced monitoring; additional investigations, evaluations or analyses; interim risk reduction actions; structural modifications; operational changes; abandonment of the dam; or the decision could be to take no additional actions at this time.

### **A-9.2.3 Risk Management**

Risk management is the overarching activity when risk is used to inform dam safety decision making and builds on risk analysis and risk assessment phases. It encompasses activities related to making risk-informed decisions, prioritizing evaluations of risk, prioritizing risk reduction activities, and making program decisions associated with managing a portfolio of facilities. Risk management includes evaluating the environmental, social, cultural, ethical, political, and legal considerations during all parts of the process. These activities include potential

structural and nonstructural actions on a given dam or project, as well as activities such as routine and special inspections, instrumented monitoring and its evaluation, structural analyses, site investigations, development and testing of emergency action plans, and many other activities. All of the activities described above relate to risk control which involves dam safety actions to reduce risk and activities to identify issues early before potential failure modes can initiate.

#### **A-9.2.4 Risk Communication**

Risk communication is a critical component of an effective risk-informed decision process. It is not a separate component of the process; it must be integrated into all aspects of the process. Risk communication is essential within an owner/regulator organization and with other individuals/organizations that have a stake in the dam or would be impacted by its failure.

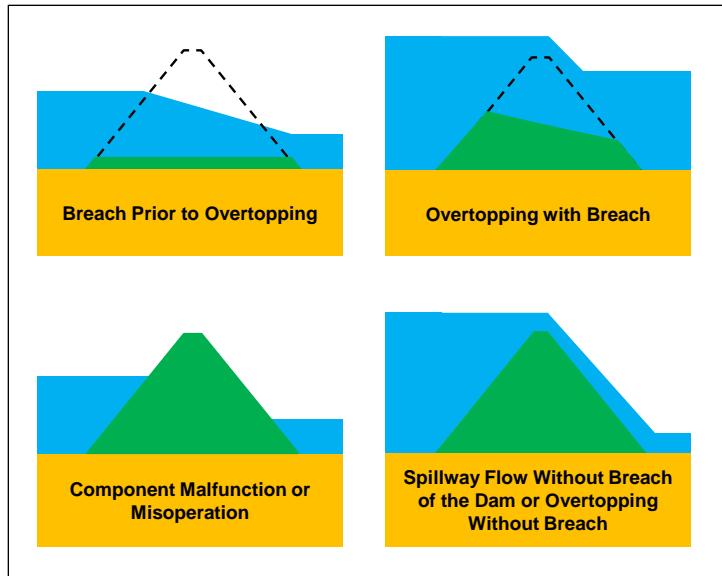
### **A-9.3 Types of Risk**

The flood risk associated with a dam or levee may arise from four inundation scenarios shown on figure A-9-2. These are:

- Breach prior to overtopping
- Overtopping with breach
- Inundation resulting from the malfunction of dam or levee components or misoperation, or interior drainage capacity exceeded behind the levee
- Spillway flow without breach of the dam or overtopping without breach (non-breach)

“Spillway flow” means controlled release of water through the outlet works or spillway up to and including full outlet works or spillway discharge.

From these four different inundation scenarios, three different risk measures can be estimated. These risk measures include incremental risk, non-breach risk, and residual risk. These risks are described in the sections below. Each of these risk measures focus on a different aspect of risk. Not all risk measures are necessarily estimated or used by each agency.



**Figure A-9-2.—The four inundation scenarios.**

### **A-9.3.1 Incremental Risk**

The ‘incremental risk’ is the risk (likelihood and consequences) to the pool area and downstream floodplain occupants that can be attributed to the presence of the dam should the dam breach prior or subsequent to overtopping, or undergo component malfunction or misoperation, where the consequences considered are over and above those that would occur without dam breach. The consequences typically are due to downstream inundation, but loss of the pool can result in significant consequences in the pool area upstream of the dam.

### **A-9.3.2 Non-Breach Risk**

The pool area and the downstream affected floodplains may remain in a state of high risk even if the dam functions as intended. This risk in the pool area and affected downstream floodplains is due to ‘normal’ dam operation of the dam (e.g. large spillway flows within the design capacity that exceed channel capacity) or ‘overtopping of dams without breach’ scenarios. Likewise for levees, the landside area may remain in a state of high risk even if the levee functions as intended (e.g. the level of designed protection may not be that great). This is referred to as the ‘non-breach’ risk. In the spirit of transparency and full disclosure, the USACE dam and levee safety programs will carefully and systematically assess, communicate, and consider in safety decisions the “non-breach” risks associated with the dams and levees in its portfolio. At Reclamation, non-breach risks are handled in a different organizational context since Reclamation’s Dam Safety Office is concerned primarily with incremental risks due to dam failure.

### A-9.3.3 Residual Risk

The risk in the pool area and downstream of the dam and the landside area behind a levee at any point in time (i.e., prior to, during, or after implementation of risk reduction measures) is herein referred to as ‘residual risk’, i.e. the risk that remains. The residual risk associated with a dam consists of two components as shown on figure A-9-3. It should be noted that the value of residual risk is the same as the incremental risk for scenarios where there is no non-breach risks (e.g., normal operation potential failure modes with spillway or outlet works flows that do not exceed safe channel capacity.) Understanding the two components that comprise residual risk is important.

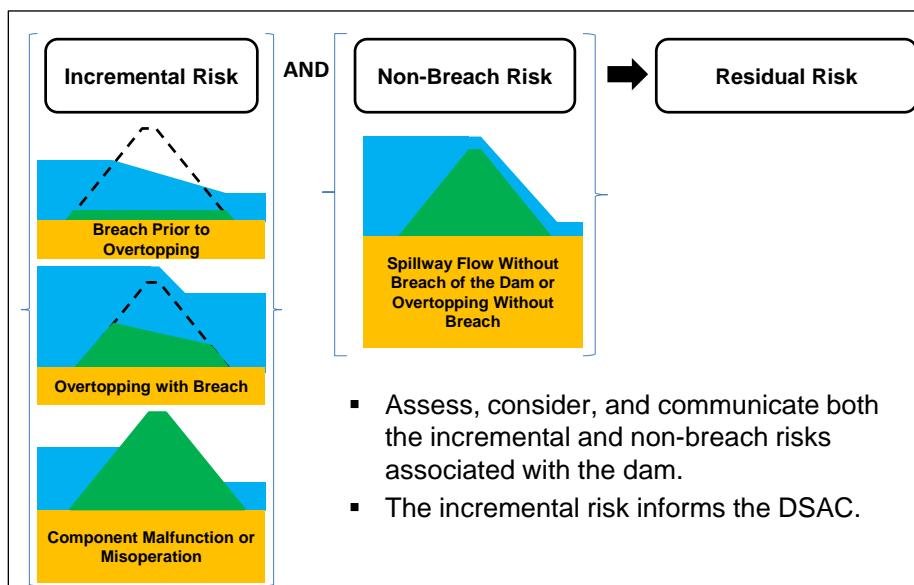


Figure A-9-3.—Residual risk.

### A-9.4 Risk Measures

The terms individual and societal risk as used here are consistent with definitions used by other water resource organizations. Societal risk deals with the notion that as the consequences increase, society in general expects the probability of those consequences to decrease. If high consequence events occur at a higher rate than society is willing to tolerate, legislation usually follows (as was the case for dam safety legislation in the U.S.). Thus, societal risk guidelines typically require a decreasing probability of failure for increasing consequences. Annualized life loss is a measure of societal risk. Reclamation uses the term “annualized life loss” in their public protection guidelines. Individual risk deals with the risk to the most exposed individual. Individual risk guidelines are therefore aimed at providing a level of protection even if the consequences are not large.

Reclamation has chosen to use annualized failure probability to represent individual risk, the assumption being that the most exposed individual is in harm's way all the time. The USACE uses the concept of individual risk.

#### **A-9.4.1 Individual Risk**

Individual risk is a term that is associated with the most exposed individual who is placed in a fixed relation to a hazard, such as a dam. Individual risk is the sum of the risks from all potential failure modes associated with the hazards that affect that person. The similarity to annualized failure probability is apparent when life loss of that individual is virtually certain (because the failure probability multiplied by a life loss of one person is equal to the failure probability).

The individual risk/annualized failure probability guideline is generally taken as 1 in 10,000 per year. In the water resources industry, this threshold is consistent with individual risk guidelines established by the UK Health & Safety Executive (2001) (BC Hydro 1995), ANCOLD (2003), New South Wales Dam Safety Committee (2006), and the Canadian Dam Association (2007).

The first infrastructure-related document that refers to this limit can be found in the original HSE efforts to use risk to manage the UK oil and gas industry in the 1990's following the Piper Alpha oil platform explosion of 1988. This threshold has apparently proven useful and rational for a number of organizations and applications, as the limits remain the same today.

#### **A-9.4.2 Background Risk**

It is important to place the 1 in 10,000 annualized failure probability (or individual risk) threshold in the context of the background mortality probability to individuals from all causes. The goal of the individual risk/annualized failure probability guideline is to keep hazards posed by dams from increasing the probability of death for an individual in the inundation areas significantly above the background levels the individual would already be exposed to. Driving the threshold lower would reduce this contribution, but it would come at a cost. Costs increase dramatically for each order of magnitude the threshold is lowered, and at some point the incremental reduction in risk contribution is inconsequential. Wise use of resources requires avoiding expenditures of excessive amounts to reduce risks to "near zero." Therefore, a reasonable and balanced threshold must be selected. A threshold limit of no more than 1 chance in 10,000 of failure per year reasonably balances the competing requirements of wise stewardship of resources and maintaining structural reliability (and public safety) of the facilities in which the nation has invested.

Figure A-9-4 shows quantitatively the average fatality rate as a function of age for all U.S. citizens from all causes. It can be seen that the threshold value of 1 in 10,000 is below the total for all age groups, and over the course of an average lifetime, is well below the total. This suggests that on the average, dam failure would contribute a small portion of the risk to even the most exposed individual living below a dam in the U.S. if the annualized failure probability is 1/10,000 or less. In general, the number of fatalities compared to the number of people in an inundation zone has been small (typically a few percent or less), and therefore the background chance of dying from dam failure for all those living in any dam break inundation zone in the U.S. is actually very small.

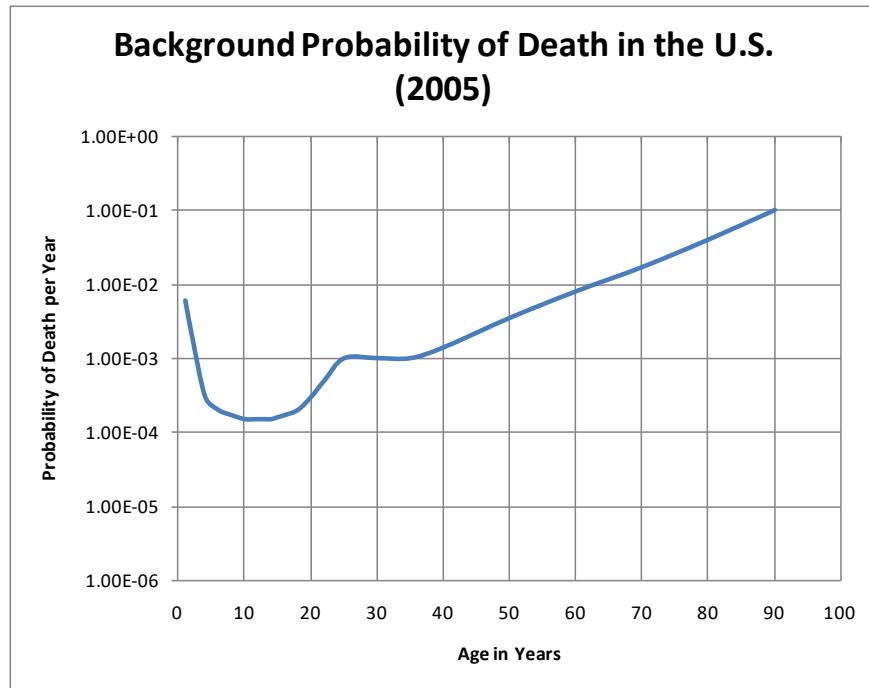


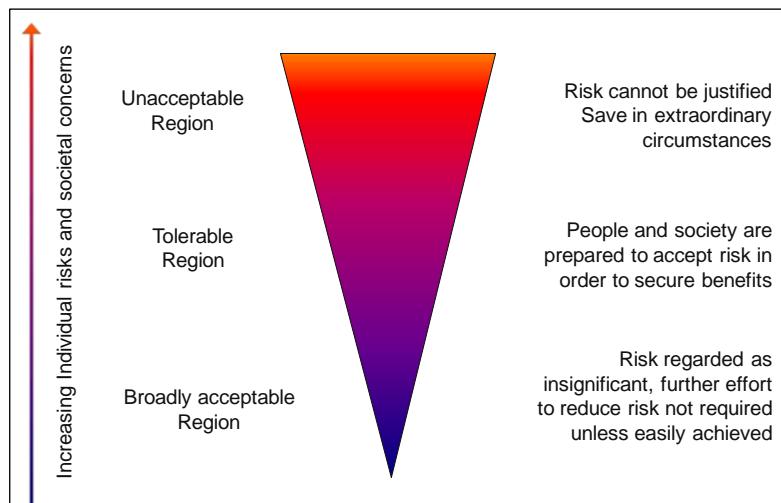
Figure A-9-4.—Background probability of death (from the CDC, 2005).

### A-9.4.3 Individual Risk Concepts from Other Agencies

#### A-9.4.3.1 Health & Safety Executive (UK)

The HSE uses the inverted triangle shown on figure A-9-5 to illustrate their framework for dealing with risk (LeGuen 2008). The “width” of the triangle indicates the amount of attention and resources focused on a particular situation. More attention and resources are directed towards situations where risks are high and there is a point where the risk becomes negligible (and hence no significant resources need be applied) as risks are reduced to the downward point of the triangle.

## Chapter A-9 Governance and Guidelines



**Figure A-9-5.—Framework for dealing with risk (LeGuen 2008).**

HSE lists “tolerable limits” for individual risk across all industries as follows (BC Hydro 1995):

*In our document on the tolerability of risks in nuclear power stations, we suggested that an individual risk of death of one in a thousand per annum should on its own represent the dividing line between what would be just tolerable for any substantial category of workers for any large part of a working life, and what is unacceptable for any but fairly exceptional groups. For members of the public who have a risk imposed on them ‘in the wider interest of society’ this limit is judged to be an order of magnitude lower [than for workers] – at 1 in 10,000 per annum.*

### A-9.4.3.2 Australian National Committee on Large Dams

The ANCOLD guidelines set the limit for individual risk as follows (HSE 2001):

*For existing dams, an individual risk to the person or group, which is most at risk, that is higher than 10-4 per annum is unacceptable, except in exceptional circumstances. For new dams or major augmentations of existing dams, an individual risk to the person or group, which is most at risk, that is higher than 10-5 per annum is unacceptable, except in exceptional circumstances.” The document goes on to say: “Life safety risks should be reduced below the limit of tolerability to the extent that is dictated by the ALARP principle.*

### A-9.4.3.3 New South Wales Dam Safety Committee

The New South Wales Dam Safety Committee states the following for individual risk in their guidelines (New South Wales Government Dams Safety Committee 2006):

*For existing dams, the DSC's limit of tolerability is 1 in 10,000 per annum, which is the same as that of ANCOLD and of the Health and Safety Executive, United Kingdom (HSE). For proposed dams and major augmentations, the DSC's limit of tolerability is 1 in 100,000 per annum, which is the same as that of ANCOLD.*

### A-9.4.3.4 Canadian Dam Association

The Canadian Dam Association guidelines consider the following with respect to individual risk (Canadian Dam Association 2007):

*The individual risk should be considered in terms of the ‘maximally exposed individual’ that is permanently resident downstream of the dam. Typically the maximally exposed individual is exposed to the hazard significantly more than 50% of the time. The maximum level of individual risk should generally be less than 10-4/year.*

### A-9.4.4 Societal Risk/Annualized Life Loss

Societal risk is the probability of adverse consequences from hazards that impact society as a whole and that create a social concern and potential political response because multiple fatalities occur in one event. Society is increasingly adverse to hazards as the magnitude of the consequences increases.

Ball and Floyd (1998) provide a thorough examination of societal risk guideline development in the U.K., Hong Kong, and the Netherlands through 1998. Originally developed by Ball and Floyd, figure A-9-6 has been updated for this document to include some key incidents in the United States.

Conceptually, societal risk/ annualized life loss guidelines are thresholds used to reflect the notion that society is increasingly averse to single high consequence events. For example, on any given day more than 100 people may die on U.S. highways in individual car accidents. Most people will not hear about any of these. On the other hand, if an airliner went down and more than 100 people were to perish in this single event, it would be national and international news. To reflect this concept, as the consequences increase for any single event, the probability of that event must decrease. This can be illustrated on the f-N or F-N diagram by a negatively sloping line. (Note: f-N and F-N diagrams are discussed in section 5.1). **For dam and levee safety, consequences are taken as “incremental”, or those over and above the consequences that would have occurred had the dam or levee not failed due to a flood.** Generally for normal operating and seismic loadings, there are no non-breach consequences, and the term “incremental” may not always be applied when describing consequences for those loadings.

## Chapter A-9 Governance and Guidelines

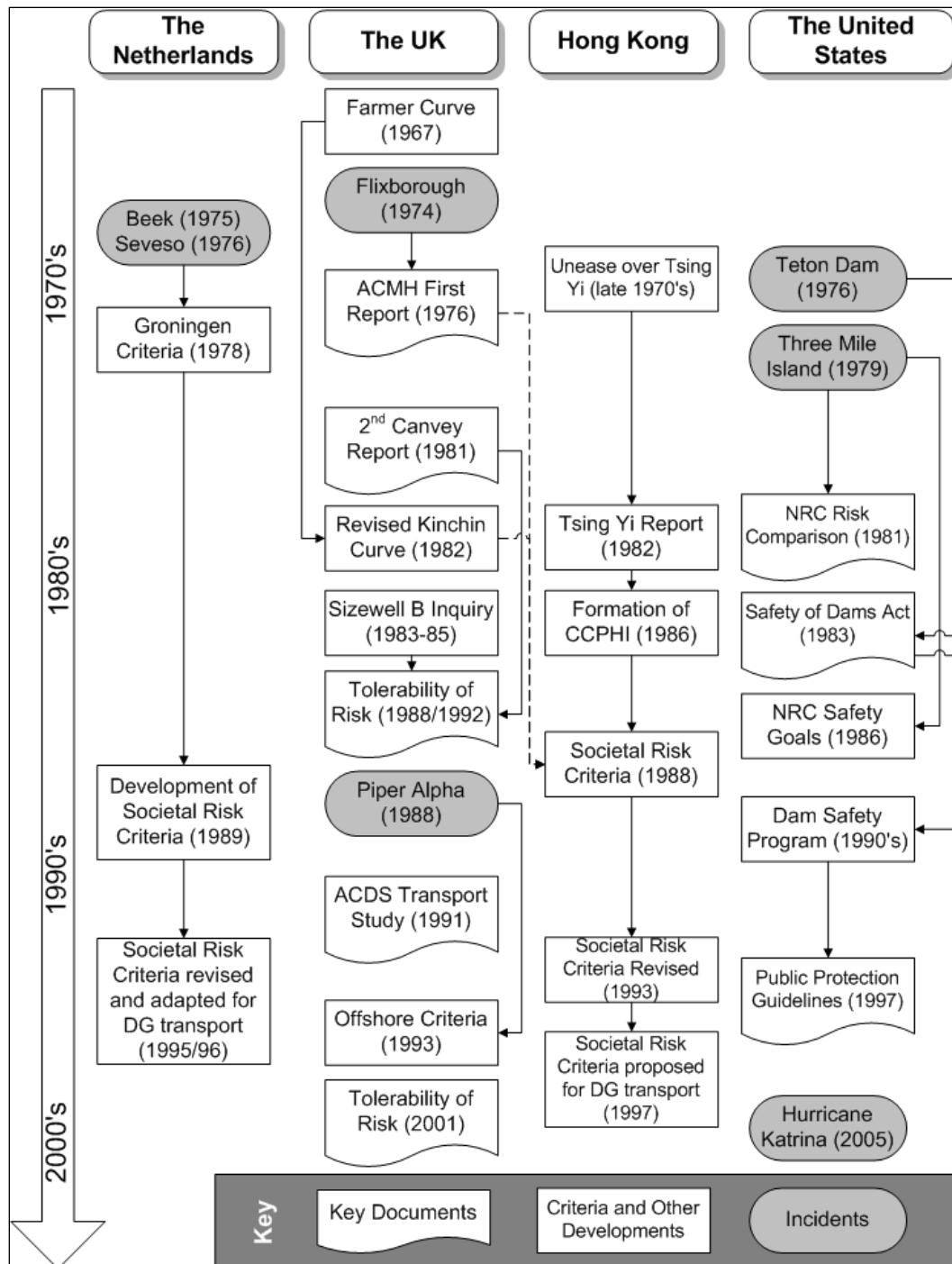


Figure A-9-6.—Milestones in the development of societal risk guidelines (Adapted from Ball and Floyd 1998).

### A-9.4.5 Societal Risk Concepts from Other Agencies

#### A-9.4.5.1 Health & Safety Executive (UK)

In the U.K., the development of societal risk concepts can be traced as far back as 1960's from work done by the U.K. Atomic Energy Authority and the eventual development of the "Farmer Curve" that regulated the frequency of Iodine-131 releases. Progress continued in many sectors, in some cases spurred by large accidents such as the Piper Alpha oil platform disaster in 1988. In 1995 HSE defined societal risk as:

*The risk of widespread or large scale detriment from the realization of a defined hazard, the implication being that the consequence would be on such a scale as to provoke a socio/political response, and/or that the risk (ie the chance combined with the consequence) provokes public discussion and is effectively regulated by society as a whole through political processes and regulatory mechanisms.*

#### A-9.4.5.2 Australian National Committee on Large Dams

In 1994, ANCOLD published its societal risk curve for existing dams that corresponded to a probability of losing 1 or more lives at less than 0.001 (less than  $10^{-4}$  for 10 or more lives, etc.), but included a horizontal truncation at an annualized probability of  $10^{-6}$ . This truncation was elevated to  $10^{-5}$  in their 2003 revision. For new dams or major augmentations, the societal risk guideline curve and the truncation were reduced by an order of magnitude. They note in their 2003 guidelines (HSE 2001) that:

*The horizontal truncations . . . are without precedent, but represent ANCOLD's present judgment of the lowest risks that can be realistically assured in light of:*

- Present knowledge and dams technology
- Methods available to estimate the risks

*In the case of existing dams, many were built long ago using very poor technology. Whilst some aspects of safety can be improved, it is simply impracticable to bring such dams full up to the safety levels of a well designed and constructed modern dam. The choice is to either accept the horizontal truncation or to abandon the dam. Since dams are of significant benefit to society, it is considered that the horizontal truncation is justified.*

#### A-9.4.5.3 New South Wales Dam Safety Committee

The New South Wales Dam Safety Committee (DSC) established societal risk guidelines as follows (Planning NSW 2008):

## **Chapter A-9 Governance and Guidelines**

*Where safety is judged by reference to the DSC public safety risk guidelines, the DSC requirement for the long-term is that societal risk be below the limit of tolerability [probability of losing 1 or more lives at less than 0.001, less than  $10^{-4}$  for 10 or more lives, etc] to the extent dictated by the ALARP principle. . . The DSC is aware of two key considerations:*

- *The potential for loss of many lives is of great concern and loss of over 1,000 lives would be seen by society as catastrophic at the international scale. In addition, the economic costs of such large tragedies are so great that it may be that the Federal Government would have to intervene*
- *It is increasingly difficult to reliably estimate probability of failure as it reduces and little confidence could be attached to estimates of probability lower than 1 in 100,000 per annum*

*In judging whether the risks of an existing dam with potential for loss of more than 1,000 lives could be accepted, the DSC will weigh these facts very carefully.*

The last two considerations and associated commentary led to the establishment of a special case for existing dams where the annualized failure probability was estimated to be less than  $10^{-6}$ , and the life loss was estimated to be greater than 1,000. If risks are estimated to fall in this area, the need for action is determined by a critical review of the risks, and costs and benefits of alternative actions.

### **A-9.4.5.4 Canadian Dam Association**

The Canadian Dam Association published societal risk guidelines (Canadian Dam Association 2007) as follows:

*[The guideline is] based on the understanding that the maximum level of societal risk for life safety should be less than  $10^{-3}$ /year for loss of one life that was not explicitly foreseen and identified in advance of the failure; a higher risk is considered ‘unacceptable’.*

### **A-9.4.6 Annualized Probability of Failure**

Statistical data compiled in the mid-1980s on U.S. dam failures and accidents Von Thun (1985) and Hatem (1995) indicate an overall dam failure rate somewhat greater than 1/10,000 per dam year of operation. This is not surprising since the statistics would be somewhat more influenced by the time period prior to the implementation of dam safety legislation and modern dam safety programs. These evaluations considered all types, ages and heights of dams. The database includes dams which were constructed without a design provided by an engineer. Von Thun’s evaluation compared failure and accident rates on the basis of type of dam; type of failure; Eastern versus Western United States; dams built before 1930,

1930-1960, and after 1960; and dams less than 50 feet high, 50-100 feet, 100-300 feet, and >300 feet. The annual failure rate range for any category (e.g., western U.S. embankment dams less than 50 feet high built after 1960 that failed by piping) was typically from  $1 \times 10^{-3}$  to  $1 \times 10^{-4}$  per dam year of operation where a reasonable number of dams were in the data base. The overall failure rate was about  $1.4 \times 10^{-4}$  per dam year of operation. This rate was strongly controlled by earth dams less than 50 feet in the eastern U.S. due to the large number of dams in this category. Hatem also considered failure rates for numerous categories, including a break out for failure rates after 5 years of successful operation. His overall failure rate was estimated to be  $2.6 \times 10^{-4}$  per dam year of operation and his estimate for dams that survived at least 5 years of successful operation was  $1.1 \times 10^{-4}$  per dam year of operation.

More recent evaluations by Foster et al. (1998) and Douglas et al. (1998) indicate failure rates for dams that survived their first 5 years have reduced somewhat, to about  $0.8 \times 10^{-4}$  per annum for both concrete and embankment dams, indicating that the number of dam failures is decreasing as the number of successful dam years of operation is increasing. Continuing to strive to reduce dam failure rates as far below  $10^{-4}$  as reasonably practicable will help ensure this will continue to be the case.

### **A-9.4.7 Other Potential Measures of Risk**

In the context of managing dam and levee safety, life safety is paramount. The primary measures of risk, i.e. the probability and severity of adverse consequences, involve societal risk and annualized life loss. However, adverse consequences from dam or levee failure will likely involve significant economic and environmental consequences. Dam and levee safety decision making should consider these other measures of risk, as appropriate based on the specific factors at a particular facility.

#### **A-9.4.7.1 Economic Consequences**

##### **A-9.4.7.1.1 Direct**

Economic considerations to help inform risk management decisions include both the direct losses of the failure of a dam and other economic impacts on the regional or national economy. Part of the direct losses is the damage to property located downstream from the dam due to dam failure or landslide of the levee due to failure of the levee. These include damage to private and public buildings, contents of buildings, vehicles, public infrastructure such as roads and bridges, public utility infrastructure, agricultural crops, agricultural capital, and erosion losses to land. Direct losses also include the value from the loss in services provided by the dam or levee such as hydropower (incremental cost to replace lost power), water supply (municipal, industrial, irrigation), flood damage reduction,

navigation (incremental cost for alternate transportation - if available), and recreation. Another category is the emergency response for evacuation and rescue and the additional travel costs associated with closures of roads and bridges. The sudden loss of pool due to a dam or levee failure could result in losses to property and infrastructure within the pool area. These losses are commonly included in computing direct economic loss due to dam or levee failure.

One potential direct loss is the cost of repairing the damage to the dam or levee. This is a complicated issue and to some degree depends on the extent of damage to the dam or levee. If the dam or levee can be repaired, these repair costs may or may not be counted as an economic cost. In the case of catastrophic failure, these rebuilding costs are typically not included in the direct costs, as the decision to rebuild the dam or levee depends on the post-failure benefits which would be a separate analysis).

#### **A-9.4.7.1.2 Indirect**

Indirect economic impacts are those associated with the destruction of property and the displacement of people due to the failure. The destruction due to the failure flood can have significant impacts on the local and regional economy as businesses at least temporarily close resulting in loss of employment and income. Similarly, economic activity linked to the services provided by the dam or levee will also have consequences. These would include economic impacts on business that provide goods and services for the recreation activities associated with the reservoir. All these indirect losses then have ripple or multiplier effects in the rest of the regional and national economy due to the resulting reduction in spending on goods and services in the region. In this way, a dam or levee failure can have widespread economic losses throughout the region. These losses are the increment to flood losses above those that would have occurred had the dam or levee not failed. These are often difficult to estimate or substantiate.

#### **A-9.4.7.2 Environmental and Other Non-Monetary Consequences**

A dam and levee failure has both direct and indirect consequences that cannot be measured in monetary terms. These stem from the impacts of the failure flood and loss of pool on environmental, cultural, and historic resources. In most cases, the assessment of the impacts of dam failure will be the reporting of area and type of habitat impacted, habitat of threatened and endangered species impacted, number and type of historic sites impacted, and the number and type of culturally significant areas impacted.

An additional indirect non-monetary consequence could be the exposure of people and the ecosystem to hazardous and toxic material released from landfills, warehouses, and other facilities. An estimate of the locations and quantities should be compiled identifying where significant quantities are concentrated. A potential additional source of hazardous and toxic material is the sediment

accumulated behind the dam. Identifying and enumerating these indirect hazards could be important enough to require additional risk assessments including estimating additional fatalities due to exposure to these hazards. Although these non-monetary consequences may not provide the sole basis for risk reduction, they can provide additional risk information for decision making. They can also be used to identify risks to be managed separately from dam or levee modifications.

Intangible consequences are those that have no directly observable physical dimensions but exist in the minds, individually and collectively, of those affected. Such consequences are real and can support decisions. Intangible consequences identified in ANCOLD (HSE 2001) include such things as:

- The grief and loss suffered by relatives and friends of those who died
- The impact of multiple deaths on the psyche of the community in which they lived
- The stress involved in arranging alternative accommodations and income
- The sense of loss by those who enjoyed the natural landscape destroyed
- The fear of lost status and reputation of the dam or levee owning organization and its technical staff

The effect of these intangible consequences can be observed more tangibly in terms of increased mental health expenditures and increased suicides.

## **A-9.5 Risk Analysis**

Risk analysis is typically a quantitative process (i.e., the inputs and outputs for a risk assessment are numeric). However, risk may also be expressed qualitatively. Risk analyses can provide valuable input to decisions made at various stages of a project and serve other important purposes. Risk analysis can include decisions made for a single dam or within an inventory of dams. The first step common to all types of risk analyses is identifying the site-specific potential failure modes. Risks are typically quantitatively evaluated by failure mode. The failure modes are then rolled up within a decision framework at a particular structure. For a given dam or project, all of the relevant types of loadings that may be experienced should be considered when identifying potential failure modes.

Methods to calculate and estimate risks are constantly evolving. The current state-of-the-practice within Reclamation and USACE for analyzing dam and levee safety risks is described in other chapters and sections of the Best Practices in Dam and Levee Safety Risk Analysis document.

### **A-9.5.1 Portrayal of Risk**

Risk analysis results are typically portrayed with plots that graphically portray the risk estimates (i.e., likelihood of failure versus potential life loss) and have an accompanying table that provides the input data used to generate the graphs. Two types of graphs are typically used: (1) the f-N plot and (2) the F-N plot.

An f-N plot shows individual failure modes that portray the potential for life loss as the estimated number of lives that would be lost (N) on the x axis and the annualized probability of the failure (f) associated with the life loss on the y axis. An f-N plot depicts societal (impacting society as a whole) risk. In addition to displaying discrete risk estimates for individual potential failure modes, the total risk for the facility considering all potential failure modes is plotted.

An F-N plot shows the cumulative risk posed by all failure modes and the associated potential life loss (discrete estimates for individual potential failure modes are not shown). On the F-N plot, the end branch probabilities are accumulated by consequence level irrespective of failure mode. The F-N plot is beneficial for dam and levee failure scenarios where different end branches resulting in failure have a wide range of different consequences, so the cumulative probability associated with different consequences is represented. A cumulative curve is developed and plotted showing the probability of N or more lives lost. An F-N plot depicts societal risk. Both f-N and F-N plots require quantitative risk estimates. Figures A-9-7 and A-9-8 are examples of f-N and F-N plots.

Both the fN and FN charts display basically the same information. FN plots are generally more common with other industries. fN plots have been useful in illustrating individual PFM's relative to agency guidelines.

Plots for the portrayal of risk for levees are currently in draft.

### **A-9.5.2 Risks Considered by Agencies**

The following is a brief summary of the types of risk that each agency considers. Much of this is derived from agency policy documents and is based in part on the specific mission or authorization of the agency. Some risk measures may or may not be considered depending on the project, purpose of the risk analysis, and other factors.

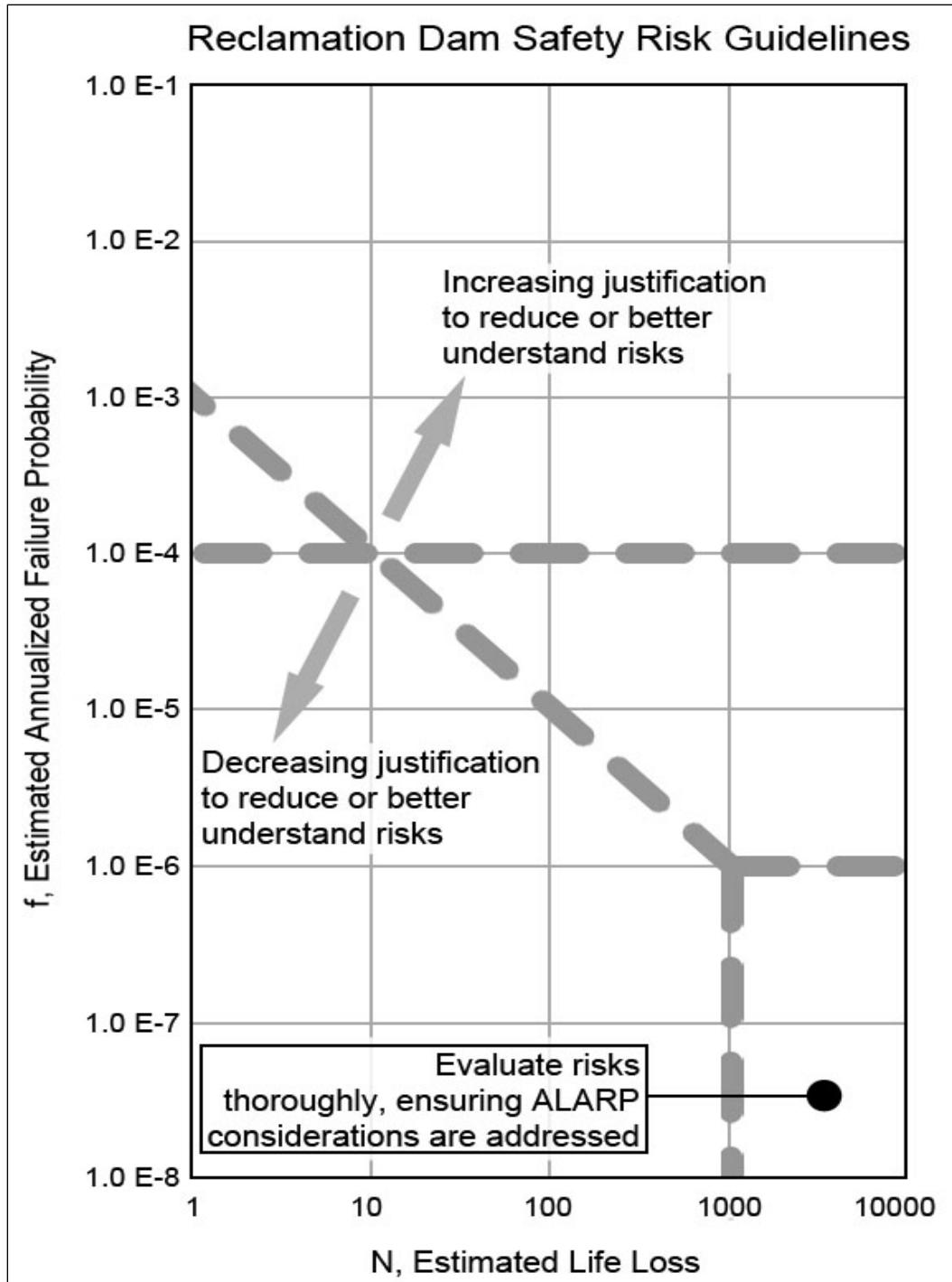
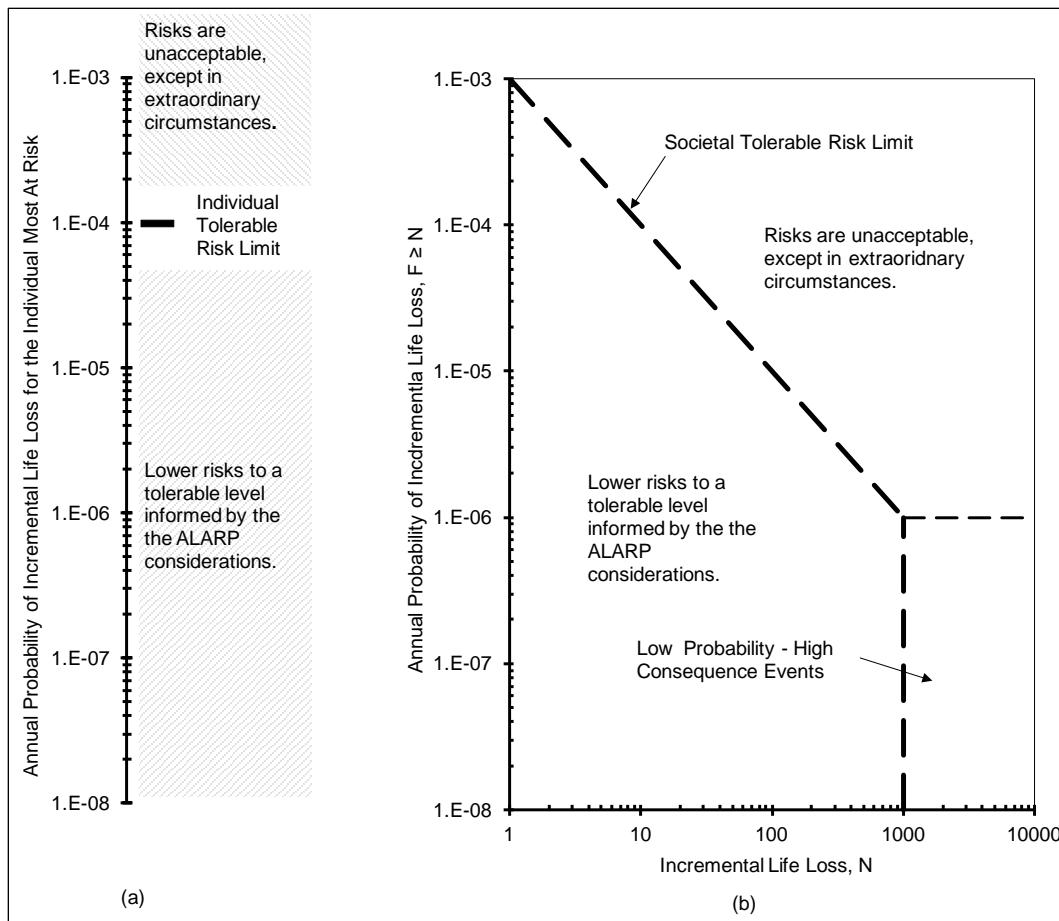


Figure A-9-7.—Reclamation's Dam Safety Public Protection Guidelines (Reclamation 2011).



**Figure A-9-8.—USACE Risk Guidelines for Existing Dams (USACE 2014).** (a) – Individual Guideline for Incremental Risk; (b) – Societal Guideline for Incremental Risk.

#### A-9.5.2.1 *Reclamation*

Two primary types of risk measures are evaluated by Reclamation (2011):

1. Annualized failure probability
2. Annualized Life Loss, or life safety risk, which is based on incremental risk expressed as Average Annual Life Loss due to dam breach (f-N chart)

Economic and environmental considerations are also considered as part of the risk assessment and decisionmaking process at Reclamation.

**A-9.5.2.2 U.S. Army Corps of Engineers**

Four types of risk measures are evaluated by USACE dam safety program (USACE 2014):

1. Annual probability of failure
2. Life safety risk, which is based on incremental and non-breach risk. Two types of life safety risk guidelines are evaluated by USACE:
  - a. Individual incremental life safety flood risk.
  - b. Societal incremental life safety flood risk expressed in two different ways:
    - i. Probability distribution of potential life loss due to dam breach (F-N chart)
    - ii. Average Annual Life Loss due to dam breach ( $f-\bar{N}$  chart)
3. Economic risk, which is based on incremental and non-breach risk.
4. Environment and other non-monetary risks, which is based on incremental and non-breach risk.

Three types of risk measures are evaluated by USACE levee safety program (in draft):

1. Life safety risk, which is based on incremental and non-breach risk. Two types of life safety risk guidelines are evaluated by USACE:
  - a. Individual incremental life safety flood risk.
  - b. Societal incremental life safety flood risk expressed in two different ways:
    - i. Probability distribution of potential life loss due to dam breach (F-N chart)
    - ii. Average Annual Life Loss due to dam breach ( $f-\bar{N}$  chart)
2. Economic risk, which is based on incremental and non-breach risk.
3. Environment and other non-monetary risks, which is based on incremental and non-breach risk.

### **A-9.5.3 Building the Dam or Levee Safety Case**

Numerical risk estimates are based on judgments, in which case they are typically subjective, and include varying degrees of uncertainty. Even numerical calculations of probability and consequences typically include significant uncertainty. These numerical estimates should not be the sole basis to inform decisions. Understanding the basis of the risk estimates is as important as the risk numbers themselves. The safety case is a logical and objective set of arguments used to advocate a position that either additional safety-related action is justified, or that no additional safety-related action is justified. The safety case should cite the most compelling information and evidence that supports the risk estimates and the overall findings. Confidence and uncertainty identified in the risk analysis should also be discussed, including identifying the sources of uncertainty, describing actions that could be taken to reduce uncertainty, and addressing the level of confidence in all three components of the risk estimate (load probability, structural response likelihood, and consequences).

The arguments combine together key evidence regarding the three basic risk components (load probability, response likelihood, and consequences) in order to support decisions related to a dam's or levee's existing condition or ability to withstand future loading. The safety case should initially be developed in the risk analysis phase and completed as part of the risk assessment for a given dam or levee. The risk analysis team will be in the best position to provide the supporting arguments for the risk analysis estimates, and those arguments should be well documented for decision makers. If necessary (i.e. if risks exceed tolerable risk limits or there is increasing justification to take action), the risk analysis team should also identify a suite of options for additional actions to better define or reduce risk. An independent group should review the draft risk analysis report and the safety case and then provide additional input and possibly revisions to any proposed actions. This independent group may identify additional factors to consider in the risk assessment or additional options for refining or reducing risk. Individuals who have the authority in the organization to make safety decisions will have the final input and determination on adopting recommended actions. The safety case is completed once the final actions (which may include a decision to take no action) have been determined within the organization. Additional information is included in "chapter A-10, "Building the Case."

## **A-9.6 Risk Assessment**

When dam safety became prominent in the late 1970s, decisions were primarily based on the standard hazard classification of the dam (e.g., high, significant, or low). Thus, a dam with an estimated potential life loss of more than one person in the event of dam failure was classified and treated in the same way as a dam with a potential life loss of several thousand people. This lack of discrimination between the levels of consequences among high hazard dams led to proposals of

criteria that would take the magnitude of loss into consideration. Among others, ANCOLD (2001), BC Hydro (2003), and Reclamation (2011) proposed or developed evaluation criteria or guidelines.

### **A-9.6.1 Principles**

A number of principles apply to risk assessments:

- Remedial actions should do no harm.
- The goal of remedial actions is to reduce risk.
- Some remedial actions may have unintended consequences. In order to implement some remedial actions, construction risks may be excessive during certain phases of the work.
- A remedial action to address a specific potential failure mode can increase the probability of another potential failure mode.
- Decisions should be risk-informed, not risk-based.
- Decisions should be based on consideration of the results of a risk analysis as a key input, but other factors, such as the uncertainty and confidence in the risk estimates, should also be considered.
- Decisions should not be based solely on where risk estimates plot on an f-N or F-N chart.
- The decisions made should consider the risk estimates, including the uncertainty and confidence in the risk estimates, the likely outcomes if dam safety actions are completed, and other factors important to an agency's mission.

Interim risk reduction measures should be considered and implemented where needed. While the ultimate goal may be to reduce risks to certain levels at a given dam, IRRMs can achieve timely incremental risk reduction, often at a reasonable cost.

### **A-9.6.2 Tolerable Risk/Justification to Take Action**

**Tolerable risk** is defined as a risk within a range that society can live with so as to secure the benefits provided by the dam or levee. It is a risk that is not to be regarded as negligible or ignored, but needs to be kept under review and reduced further if appropriate and possible.

## **Chapter A-9 Governance and Guidelines**

Reclamation's Public Protection Guidelines do not use the term "tolerable risk". However, their guidelines suggest that there are risks above which there is justification to take action, and as the risk increases so does the justification. This serves a similar purpose to tolerable risk guidelines.

Inherent in the use of risk analysis and risk-informed guidelines and, specifically, in risk assessment, is the recognition and understanding of tolerable risk/justification to take action.

Risk assessment teams, which include the organization's decision makers, can make a variety of decisions that might involve better defining risk, reducing risk, or taking no action and continuing to monitor the facility and periodically review risk. Table A-9-1 illustrates the general process of how risk results and confidence can lead to potential actions.

Risk reduction actions might involve interim risk reduction measures until a permanent solution can be implemented. Permanent risk reduction alternatives might involve non-structural solutions (e.g. reservoir restriction) or structural modifications.

The risk remaining after risk reduction actions are implemented, related to a specific dam or levee safety issue, is considered a tolerable risk. It can also be thought of, considered, or called the residual risk. It is the risk that remains after prudent actions to address the risk have been taken, or the remote risk associated with a condition that was judged to not be a credible dam safety issue.

Threshold values are typically established to help guide decisions on tolerable risk/ justification to take action. While the threshold guideline values are generally consistent within the dam safety community, agencies may elect to use different values to address their unique mission.

The intent is generally to drive the risks as low as reasonably practicable. In this context, another way of describing or thinking about tolerable risk/ justification to take action is that, after hearing all the facts and information related to an issue or issues on a dam or project, an organization decides that further action is not reasonably practicable. When a judgment is made that risks are as low as reasonably practicable, this is often determined by comparing the effectiveness of reducing risk further (evaluated by considering the cost to further reduce risk and the amount of risk reduction achieved, and then comparing it to other risk reduction actions implemented by the agency). If the costs to achieve an additional level of risk reduction are disproportional to achieving the same

## Chapter A-9 Governance and Guidelines

**Table A-9-1.—Risk, Confidence, and Actions**

|      |   | <b>Confidence</b>   |   |
|------|---|---|---|
|      |   | <b>Low</b>  | <b>High</b>   |
| Risk | Increasing Justification/Risk Intolerable | <b>Second Priority</b>  | <b>First Priority</b>   |
|      |   | <p><b>Potential Actions</b></p> <ul style="list-style-type: none"> <li>• Take action to increase confidence</li> <li>• Collect data and/or perform studies           <ul style="list-style-type: none"> <li>•</li> </ul> </li> <li>• Reevaluate risk</li> </ul> <p><b>Likely Outcomes</b></p> <ul style="list-style-type: none"> <li>• Stay in area of increasing justification/risk intolerable, but with greater confidence</li> <li>• Moves to area of decreasing justification/tolerable risk, but with greater confidence</li> </ul>   | <p><b>Potential Actions</b></p> <ul style="list-style-type: none"> <li>• Initiate studies/investigations to reduce risk (potentially high urgency)</li> <li>• Identify interim risk reduction measures</li> </ul> <p><b>Likely Outcomes</b></p> <ul style="list-style-type: none"> <li>• Reservoir restrictions (temp or perm)</li> <li>• Modify dam           <ul style="list-style-type: none"> <li>•</li> </ul> </li> <li>• Implement non-structural measures</li> </ul> |
| Risk | Decreasing Justification/Risk Tolerable   | <b>Third Priority</b>   | <b>Fourth Priority</b>  |
|      |   | <p><b>Potential Actions</b></p> <ul style="list-style-type: none"> <li>• No action may be justified</li> <li>• Take action to increase confidence           <ul style="list-style-type: none"> <li>•</li> </ul> </li> <li>• Collect data and/or perform studies</li> <li>• Reevaluate risks</li> </ul> <p><b>Likely Outcomes</b></p> <ul style="list-style-type: none"> <li>• Move to area of increasing justification/risk intolerable, but with greater confidence</li> <li>• Stay in area of decreasing justification/risk tolerable, but with greater confidence. If this outcome is likely, actions may be considered low priority.</li> </ul> | <p><b>Potential Actions</b></p> <ul style="list-style-type: none"> <li>• No action</li> <li>• Reasonable and prudent, low cost actions</li> </ul>   |

## **Chapter A-9 Governance and Guidelines**

magnitude of risk reduction at other dams, the current risk may be as low as reasonably practicable. There are many factors besides the numerical estimate of risk that can contribute to the decision that no further action is justified, including:

- The cost to reduce risks further
- The level of certainty or uncertainty on various aspects of the problem
- A precedent of comparable decisions on other projects
- The possibility that the concern is not reasonable to address in a practical manner
- The chance of success of an action
- Time to perform the remediation
- Other considerations

It should also be recognized that regardless of what actions are taken or not taken, there will always be a certain level of residual risk. Therefore, rather than ignoring or supposing that the risk is zero, it is appropriate that tolerable risk levels for various aspects of the dam be discussed and identified.

Risk-informed safety decision making implies that decisions are made considering risk estimates and many other contributing factors that might include confidence in the risk estimates, risk uncertainty, and the overall safety case in addition to other local or regional considerations. Both the USACE and Reclamation utilize risk-informed dam safety decisionmaking.

Risk-based safety decision making implies that a comparison of a risk estimate to risk criteria is the basis for decision-making, as opposed to risk-informed decision making where only general guidelines are established and other factors are considered.

Interim risk reduction measures should be considered and implemented where needed. While the ultimate goal may be to reduce risks to certain levels at a given dam or levee, IRRMs can achieve timely incremental risk reduction, often at a reasonable cost.

### **A-9.6.3 ALARP**

ALARP is an acronym for “as low as reasonably practicable” and is used as an adjective to describe risk level. The answers to the questions: “When are risks low enough?” “What actions are reasonable?” and “What actions are

## **Chapter A-9 Governance and Guidelines**

practicable?” are key ALARP risk considerations that require subjective judgment. These considerations provide a way to address efficiency in reducing risks. The general ALARP risk concept is that risk reduction beyond a certain level may not be justified if further risk reduction is impracticable or if the cost is grossly disproportional to the benefits obtained by the risk reduction.

Both the USACE and Reclamation guidelines include an area on the f-N chart bounded by an annualized failure probability of  $1 \times 10^{-6}$  on the top and 1,000 lives lost on the left, similar to those of the New South Wales Dam Safety Committee (New South Wales Government Dams Safety Committee 2006). If risks are judged to fall to the right and below this region, a careful evaluation of the tradeoffs in costs and effort to reduce risks should be undertaken, and ALARP or “as low as reasonably practicable” principles applied to the decision making. In these cases, the decisions could involve stakeholders, with public involvement if risk and cost tradeoffs are significant. The importance and visibility of the structure may necessitate a study of modifications that include redundant defensive measures which would reduce the risk of the structure. In some cases, this may not be a cost-effective way to reduce the risk. In any case, the manner and approach to reach a decision will require substantial coordination between risk estimators and decisionmakers.

ALARP considerations may be taken into account when risks are lower than the risk guidelines, for those risks above the risk guidelines that have potentially extraordinary circumstances, or for those cases of very low failure probability but very large consequences as described above. ALARP only has meaning in evaluating risk reduction measures – it cannot be applied to an existing risk without considering the options to reduce that risk. Consideration of ALARP is a matter of judgment. To make a judgment on whether risks are ALARP, the following should be taken into account (adapted from New South Wales Government Dams Safety Committee [2006]):

- The level of risk in relation to the established risk guidelines
- The disproportion between the sacrifice (money, time, trouble and effort) in implementing the risk reduction measures and the subsequent risk reduction achieved
- The cost-effectiveness of the risk reduction measures
- Any relevant recognized good practice
- Societal concerns as revealed by consultation with the community and other stakeholders.

The general intent of ALARP is to evaluate whether risks should be reduced, and if so, how far. A balance between equity and efficiency is implied by using the principle.

### **A-9.6.4 Other Considerations**

Reclamation's guidelines suggest that the target for risk reduction actions related to major rehabilitation be an order of magnitude below the annualized failure probability and annualized life loss guidelines to ensure that uncertainty, hazard creep, and robustness are considered in the decision process. Although the cost effectiveness of reaching this level of risk reduction must be considered before deciding to pursue such an alternative, it is typically achieved. The USACE also expects new dams or major modifications to be lower than these guidelines.

Low hazard dams, levees, and canal embankments are typically not subject to the risk guidelines as the life loss consequences are typically not severe enough to justify expenditure of safety funding. However, there may be other consequences, such as economic, environmental, cultural, or socio that might warrant an evaluation of those risks and perhaps risk reduction efforts.

### **A-9.6.5 Uncertainty**

There are three components that can contribute to an increase in risk:

- As consequences increase, risk increases
- As the likelihood of failure increases, risk increases
- As the uncertainty increases, risk borne by the dam or levee owner also increases

Every attempt is made to reduce uncertainty in risk estimates, but it is recognized that this is not always possible or even cost-effective. Uncertainty is typically not a primary decision parameter. Nevertheless, uncertainty is used in the prioritization process. Therefore, it is important to give decision makers some sense of the uncertainty, what might be done to reduce the uncertainty, and which direction the risk is likely to go with additional information, if there is a sense of this. In some cases, the likelihood of exceeding the guidelines is estimated, which provides the decision makers with additional quantitative information.

### **A-9.6.6 Confidence**

Risk analyses should include a discussion of the confidence in the risk estimates. This provides decision makers with the understanding of how confident the risk estimators were given the information that was available to them in making their

risk estimates. This understanding is an important factor in assessing risks. High confidence indicates the risk estimators had high quality data, inputs, analytical results, and established processes in which to base their estimates and that the collection of additional information, performance of additional analyses, etc. would not be expected to change the estimates significantly. On the other hand, low confidence indicates that the risk estimators did not have adequate information in which to base their estimates, perhaps due to little available information, the information was of questionable quality, or the information may conflict such that the collection of additional information or performance of additional engineering analyses would be beneficial so that the risk estimates could be confirmed or revised.

### **A-9.6.7 The Safety Case**

The risk estimates and the recommended actions need to be coherent. Uncertainty is inherent in each assertion. The arguments should also address whether confidence is high enough for the assertions to stand on the basis of existing evidence.

The safety case and the identification of risk management options are recognized as essential elements to ensure public protection. They represent the understanding of existing conditions and predicted future behavior stated as objectively as possible.

### **A-9.6.8 Approach to Making Risk Informed Decisions**

When Reclamation began implementing its risk guidelines in the early 1990's, it was recognized that risk estimates developed with the information that is typically available would not be sufficiently precise or accurate to compare to a distinct criteria. Therefore, the levels established for annualized failure probability and annualized life loss were intended to be advisory rather than prescriptive. Continued diligence is necessary to ensure that they continue to be seen as "gradational", such that risks portrayed just below "the line" are seen to be similar to those portrayed just above the line, and are not interpreted as criteria.

Both Reclamation (2011) and the USACE (2014) have adopted guidelines similar to the New South Wales Dam Safety Committee (2006) guidelines for existing dams, as shown on figures A-9-7 and A-9-8. There are some subtle differences between the two. First, Reclamation's guidelines are intended to be used with f-N risk pairs, whereas both f-N and cumulative F-N data are to be used with the USACE guidelines. The implications of this will be discussed later. Secondly, the terminology used in expressing the guidelines is somewhat different. Reclamation refers to their guidelines as "Public Protection Guidelines" to put the emphasis on protecting the public rather than tolerating risk. They also use the terminology "increasing justification" and "decreasing justification" to further

## **Chapter A-9 Governance and Guidelines**

emphasize the fact that they are guidelines. USACE has adopted the language from the UK Health & Safety Executive, which is also used by most of the British Commonwealth countries, where the terms “unacceptable” and “tolerable” are used. This connotes a more regulatory stance, even though the USACE also applies them as guidelines rather than hard and fast criteria.

Decisions related to structures for low failure probabilities combined with high consequences have been difficult to address for both decision-makers and risk estimators. Predicting the probability of events with annual exceedance probabilities more remote than about 1 in a million results in extreme uncertainty that must be factored into the decision process.

There is a lower bound of the likelihood of events beyond which results become of questionable reliability. There is also a threshold beyond which the magnitude of the consequences necessitates extraordinary measures to control risks.

However, Reclamation and the USACE have chosen not to set a horizontal threshold below which risk reduction measures need not be evaluated. Likewise, setting a vertical threshold to the right of which risks are unacceptable irrespective of the likelihood of the event could necessitate decommissioning projects whose societal benefits are extremely valuable. Therefore, it is appropriate to treat low probability and high consequence situations with care and ensure everything reasonable has been done to reduce risks. Decisions should be made in those cases considering all relevant information rather than using uncertain risk calculations to avoid a potentially difficult decision.

Structures that have the potential to cause more than about 1,000 deaths are generally large in size and highly visible; are important to the local community, the region, and the economy; and the public is generally aware of their proximity to the reservoir. Because of this, these structures generally receive added attention during all parts of the risk management process by both decision-makers and technical staff. The existence of structures that have the potential to cause severe catastrophes indicates that the trade-off between the hazards posed by the structure and the benefits secured by it should not be taken lightly. It will not always be possible to quantify numerical estimates to the point where estimators will be able to adequately defend the precision and robustness of the risk estimates. There will also always be uncertainties with respect to the conditions of the structures. This does not mean that structures which fall into this category should be ignored or that an attempt should not be made to obtain the best information possible. The opposite is true, although the costs of obtaining the information should be carefully weighed against the potential to gain useful insights that could be used to support a decision. ALARP principles should be considered and actions weighed according to their costs, risk reduction benefits, and the residual risks posed by the structure.

### A-9.6.9 Example Comparison of f-N and F-N

Consider the following example. A dam has three potential failure modes, the event tree end branches of which are summarized in table A-9-2. The first potential failure mode has two paths to failure, one of which results in large consequences and the other which results in more moderate consequences. The second potential failure mode results in nearly identical consequences for any given load range, suggesting the pool level and breach would be nearly constant with a change in loading. The third potential failure mode results in increasing consequences, perhaps due to an increasing pool level.

**Table A-9-2.—Example Potential Failure Mode Event Tree End Branch Summary**

| End Branch               | Annualized Failure Probability | Incremental Life Loss | Annualized Life Loss |
|--------------------------|--------------------------------|-----------------------|----------------------|
| Potential Failure Mode 1 |                                |                       |                      |
| 1                        | 2.2E-04                        | 34                    | 7.48E-03             |
| 2                        | 1.1E-05                        | 225                   | 2.48E-03             |
| 3                        | 7.5E-05                        | 34                    | 2.55E-03             |
| 4                        | 3.2E-06                        | 225                   | 7.20E-04             |
| Total                    | 3.09E-04                       | 43                    | 1.32E-02             |
| Potential Failure Mode 2 |                                |                       |                      |
| 1                        | 3.3E-05                        | 125                   | 4.13E-03             |
| 2                        | 6.7E-06                        | 125                   | 8.38E-04             |
| 3                        | 1.2E-06                        | 125                   | 1.50E-04             |
| Total                    | 4.09E-05                       | 125                   | 5.11E-03             |
| Potential Failure Mode 3 |                                |                       |                      |
| 1                        | 3.6E-05                        | 15                    | 5.40E-04             |
| 2                        | 1.1E-05                        | 34                    | 3.74E-04             |
| 3                        | 7.3E-06                        | 57                    | 4.16E-04             |
| 4                        | 4.5E-06                        | 82                    | 3.69E-04             |
| 5                        | 1.3E-06                        | 114                   | 1.48E-04             |
| Total                    | 6.01E-05                       | 31                    | 1.85E-03             |
| Summation                |                                |                       |                      |
| Grand Total              | 4.10E-04                       | 49                    | 2.02E-02             |

Although f-N pairs and the cumulative F-N plot are different and typically are presented on separate plots, it can be instructive to show both on a single plot to see a comparison of what would be provided to decision makers. The f-N pairs

## Chapter A-9 Governance and Guidelines

are typically plotted by potential failure mode. The annualized failure probability multiplied by the incremental life loss gives the annualized life loss. Both the annualized failure probability and annualized life loss are summed (assuming common cause has been accounted for – see section on combining and portraying risk). The potential failure mode is then plotted on the f-N diagram at the summed annualized failure probability and at a weighted consequence level, calculated as the annualized life loss divided by the annualized failure probability. Similarly, the total risk is plotted by summing the individual failure modes and calculating a total weighted consequence level.

To plot the cumulative curve, the end branches must first be sorted by descending consequences (regardless of failure mode). Annualized failure probabilities for a given consequence level are then summed. Annualized failure probabilities are then summed incrementally, starting with the highest consequence level, as shown in table A-9-3.

**Table A-9-3.—Cumulative Curve Development**

| Potential Failure Mode | End Branch | Consequences | Annualized Failure Probability | Cumulative Failure Probability |
|------------------------|------------|--------------|--------------------------------|--------------------------------|
| 1                      | 4          | 225          | 3.2E-06                        | 1.42E-05                       |
| 1                      | 2          | 225          | 1.1E-05                        |                                |
| 2                      | 3          | 125          | 1.2E-06                        | 5.51E-05                       |
| 2                      | 2          | 125          | 6.7E-06                        |                                |
| 2                      | 1          | 125          | 3.3E-05                        |                                |
| 3                      | 5          | 114          | 1.3E-06                        | 5.64E-05                       |
| 3                      | 4          | 82           | 4.5E-06                        | 6.09E-05                       |
| 3                      | 3          | 57           | 7.3E-06                        | 6.82E-05                       |
| 3                      | 2          | 34           | 1.1E-05                        | 3.74E-04                       |
| 1                      | 3          | 34           | 7.5E-05                        |                                |
| 1                      | 1          | 34           | 2.2E-04                        |                                |
| 3                      | 1          | 15           | 3.6E-05                        | 4.10E-04                       |

The plot starts at the highest consequence level and proceeds stepwise (stepping up first to the next highest annualized failure probability and then left to the next lower consequences) toward the lowest consequence level using the incrementally summed (accumulated) annual failure probabilities.

The plots are shown on figure A-9-9. From the f-N data it can be seen that all three potential failure modes exceed the societal risk/ annualized life loss guidelines, and that potential failure mode 1 exceeds both the societal risk/ annualized life loss guidelines and the annualized failure probability (and perhaps individual risk) guidelines. These data also show that potential failure mode 1 contributes most to the total risk. The cumulative curve indicates that there are some failure scenarios with as much as 225 estimated fatalities, and some with as little as 15. The cumulative curve portrays the likelihood and variability of consequences across the full domain of failure scenarios. Note that this is not the same as the uncertainty in the life loss estimate for a specific scenario (or collection of scenarios) that is typically portrayed using uncertainty bars on the f-N chart. The cumulative plot shows that societal risk guidelines are exceeded for all failure scenarios, and the individual risk guidelines may also be exceeded for some failure scenarios. In the end both plots portray similar and complementary information. Reclamation has found the f-N plot to be easier for decision makers to understand and therefore uses it exclusively. USACE has found the F-N plot offers additional information for decision makers to consider and therefore uses it to supplement the f-N plot.

It should be noted that some organizations have attempted to convert f-N plots to F-N charts and vice versa. Reclamation and the USACE have chosen not to do this. Therefore, the plots shown on figure A-9-9 are essentially what the decision makers would see if overlaid on top of each other.

### **A-9.7 Risk Management**

Risk management encompasses activities related to making risk-informed decisions, prioritizing evaluations of risk, prioritizing risk reduction activities, and making program decisions associated with managing an inventory of facilities. Risk management processes vary with respect to an organization's governance. Risk management is greatly facilitated and enhanced by having the knowledge base supplied by the risk analyses and risk assessment inputs for the dams as described above. Such knowledge allows a logical and consistent basis for substantiating and prioritizing risk reduction activities and/or making program decisions associated with managing an inventory of facilities. Risk management, also considers economic, environmental, social, cultural, ethical, political, and legal factors that can be difficult to quantify. Risk management should be regarded as an ongoing and iterative process that needs to adapt to new information.

The primary goal of risk management is to implement actions to either: accept, further monitor or evaluate, control, or reduce risk, while considering the cost and benefits of any actions taken. When reducing risk either at a single dam or levee

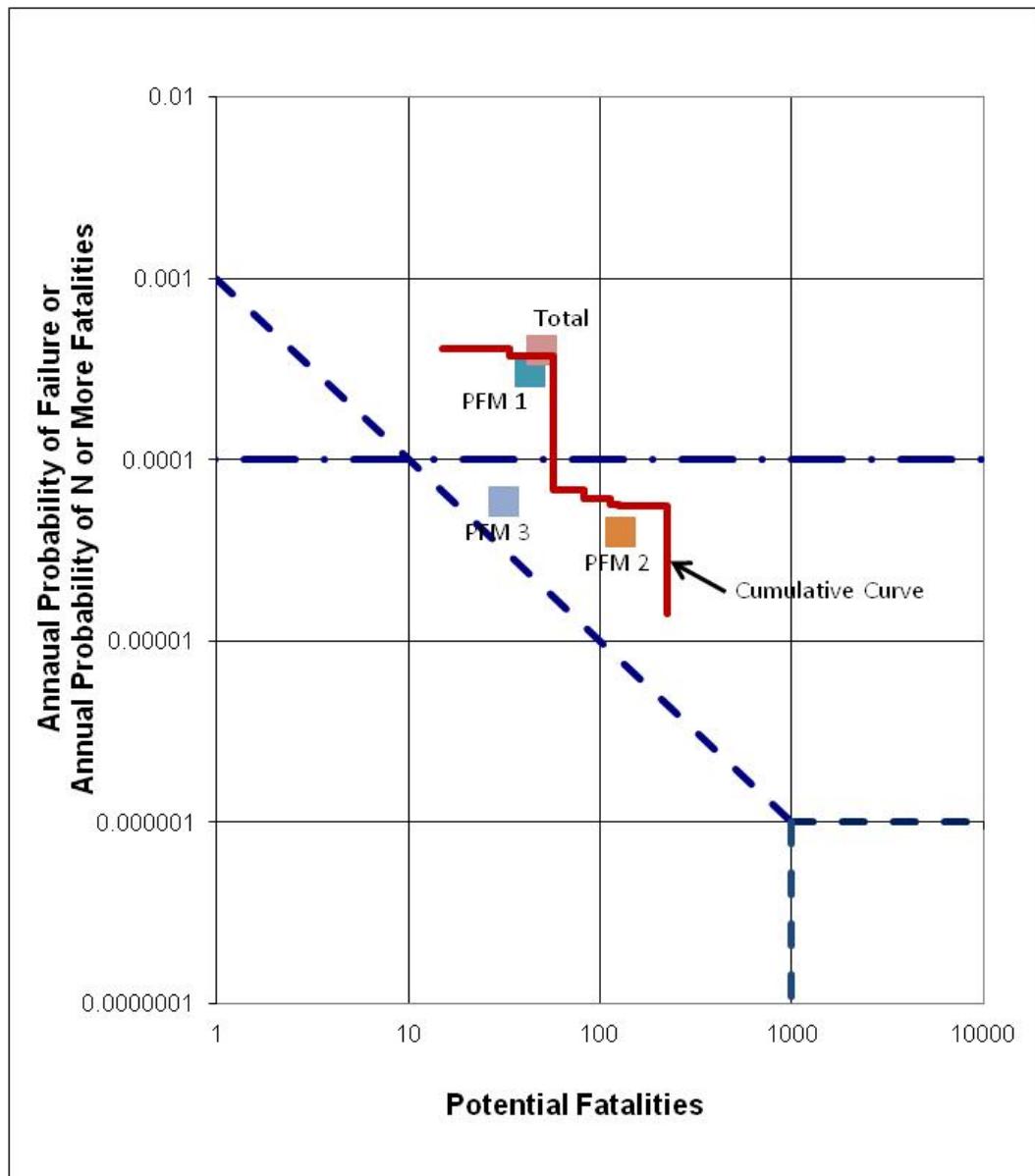


Figure A-9-9.—Comparison of f-N and F-N plots.

## **Chapter A-9 Governance and Guidelines**

or within a portfolio of dams or levees, actions should be taken as quickly and as efficiently as possible, recognizing that there will likely be limits on available funding. Consideration should be given to how much risks are reduced compared with the costs necessary to achieve risk reduction. Generally, the priorities will be to address the dams or levees with the highest perceived risk first, assuming there is confidence in the risk estimates; however, if the cost of reducing risk at the highest risk dam or levee is disproportional to the risk reduction achieved or takes away from implementing actions at several other structures, it may be appropriate to consider risk reduction activities at other structures first.

Organizations recognize that the methods used to calculate risk do not provide precise numerical results. Therefore, it would not be appropriate to rely solely on the numeric estimates in comparison to guideline values. Decisions are usually more complex than can be portrayed using only the numerical results of a risk analysis. The strength of the safety case should also be considered in the risk management phase.

In order to effectively prioritize safety actions, information on the cost and duration of the actions and the risk reduction potential is needed. This type of information is necessary to evaluate the efficiency of risk reduction actions and can be used to fine-tune safety actions. A record of the baseline risks, the safety case and rating, and updates that resulted from risk reduction activities should be maintained for each structure in an agency's inventory.

For Federal owners with large inventories, or for private owners with large inventories, it is important to prioritize safety actions because funding will limit how quickly actions can be completed. If an owner is dealing with a large inventory, a risk categorization scheme may be helpful in making an initial cut at prioritizing safety actions. Table A-9-4 shows a method of categorizing dams by risk that will provide an initial sorting of dam safety actions.

To prioritize actions within a category, consider each of the following factors, which will contribute to increasing the priority of actions at a given dam:

- Both the failure probability and the annualized life loss exceed the threshold guideline values
- The failure probability or the annualized life loss is driven by a single potential failure mode
- The failure probability or the annualized life loss is driven by a potential failure mode manifesting itself during normal operating conditions

## Chapter A-9 Governance and Guidelines

**Table A-9-4.—Joint Federal Risk Categories**

| Urgency of Action            | Characteristics and Considerations   | Potential Actions  |
|------------------------------|--|--|
| I – VERY HIGH URGENCY        | <p><b>CRITICALLY NEAR FAILURE:</b> There is direct evidence that failure is in progress, and the dam is almost certain to fail during normal operations if action is not taken quickly.</p> <p>OR</p> <p><b>EXTREMELY HIGH RISK:</b> Combination of life or economic consequences and likelihood of failure is very high with high confidence.</p> | <ul style="list-style-type: none"> <li>• Take immediate action to avoid failure. Communicate findings to potentially affected parties.</li> <li>• Implement IRRMs.</li> <li>• Ensure that the emergency action plan is current and functionally tested.</li> <li>• Conduct heightened monitoring and evaluation. Expedite investigations and actions to support long-term risk reduction.</li> <li>• Initiate intensive management and situation reports.</li> </ul> |
| II - HIGH URGENCY            | <p><b>RISK IS HIGH WITH HIGH CONFIDENCE, OR IT IS VERY HIGH WITH LOW TO MODERATE CONFIDENCE:</b> The likelihood of failure from one of these occurrences, prior to taking some action, is too high to delay action.</p>  | <ul style="list-style-type: none"> <li>• Implement IRRMs.</li> <li>• Ensure that the emergency action plan is current and functionally tested.</li> <li>• Give high priority to heightened monitoring and evaluation. Expedite investigations and actions to support long-term risk reduction.</li> <li>• Expedite confirmation of classification.</li> </ul>  |
| III - MODERATE URGENCY       | <p><b>MODERATE TO HIGH RISK:</b> Confidence in the risk estimates is generally at least moderate, but can include facilities with low confidence if there is a reasonable chance that risk estimates will be confirmed or potentially increase with further study.</p>   | <ul style="list-style-type: none"> <li>• Implement IRRMs.</li> <li>• Ensure that the emergency action plan is current and functionally tested.</li> <li>• Conduct heightened monitoring and evaluation. Prioritize investigations and actions to support long-term risk reduction.</li> <li>• Prioritize confirmation of classification as appropriate.</li> </ul>   |
| IV – LOW TO MODERATE URGENCY | <p><b>LOW TO MODERATE RISK:</b> The risks are low to moderate with at least moderate confidence, or the risks are low with low confidence, and there is a potential for the risks to increase with further study.</p>  | <ul style="list-style-type: none"> <li>• Ensure that routine risk management measures are in place.</li> <li>• Determine whether action can wait until after the next periodic review.</li> <li>• Before the next periodic review, take appropriate interim measures and schedule other actions as appropriate.</li> <li>• Give normal priority to investigations to validate classification, but do not plan for risk reduction measures at this time.</li> </ul>   |
| V – NO URGENCY               | <p><b>LOW RISK:</b> The risks are low and are unlikely to change with additional investigations or studies.</p>  | <ul style="list-style-type: none"> <li>• Continue routine dam safety risk management activities and normal operations and maintenance.</li> </ul>  |

## **Chapter A-9 Governance and Guidelines**

- The range of risk estimates is tightly clustered and the mean and median are similar (for detailed uncertainty analyses only) and/or sensitivity studies instill confidence
- Risk reduction or confirmation is relatively easy and inexpensive

The above bulleted factors can also be considered if a dam appears to border two categories in the table. If a dam owner has a small inventory of dams, the above bulleted factors alone can be used as the basis for establishing priorities. The initial effort to place the actions in one of the five risk categories would have limited value for small dam inventories.

Prioritization of dam safety actions can be done on a facility basis (where total risk is the focal point, and the goal is to reduce total risk to tolerable levels) or on an individual potential failure mode basis (where single potential failure modes are addressed).

The Reclamation and USACE dam safety programs use risk classification systems Dam Safety Priority Rating (DSPR) and Dam Safety Action Classification (DSAC), respectively, to help guide key decisions within the program. These classification systems are similar to that shown in table A-9-4 and portray the need for urgency of action and the priority for responding to risk associated with Reclamation and USACE dams. The DSPR and DSAC assignment is informed by the ‘incremental risk’.

The USACE levee safety program makes use of a risk classification system named Levee Safety Action Classification (LSAC) to help guide key decisions within the program. Like the DSAC system, LSAC is informed by the ‘incremental risk’, although typically an LSAC is assigned for both prior to overtopping and overtopping categories.

A number of principles apply to risk management. These principles are discussed below.

Reducing risk at a given dam or within an inventory of dams will typically require setting priorities. Factors to consider will be the magnitude of risk at a given dam and the confidence in the risk estimates, the costs of implementing risk reduction actions, and the timeframe required to achieve the risk reduction. All of these factors should be considered when establishing priorities. The objective of an organization should be to reduce dam safety risk as effectively and as efficiently as possible.

Each organization should have a transparent process for establishing priorities and the urgency of completing dam safety actions. Within an organization, the

responsibility for the inventory of dams will often be divided among a number of offices. Having a transparent process will develop confidence within the organization that decisions are made objectively and fairly.

Prioritizing work within an inventory of dams will typically be a dynamic process. While priorities can be established annually, new safety issues that have a high priority may develop in between annual prioritization activities. This requires flexibility in prioritizing work within a portfolio, allowing for adjustments in planned work as new, high priority issues are identified.

Use a dedicated, established group to review and prioritize proposed safety actions within a portfolio of dams or levees or when establishing urgency for action at a specific dam or levee. This will help ensure consistency in establishing priorities and will improve efficiency because a consistent group will maintain knowledge of the overall inventory.

Independent review is critical to the credibility of risk management. This will help ensure that biases and individual preferences do not dominate the decision making process.

The urgency of completing safety actions should be commensurate with risk. In general, dams or levees with the highest estimated risk should receive the highest priority because they are the most likely to fail in the inventory and/or would have the highest consequences should they fail.

## **A-9.8 Risk Communication**

Communication is important in all aspects of safety within an organization, with the public, and with the specific owners or stakeholders of a project. However, communication about the work associated with risk is particularly important because of the fears, sentiments, perceptions, and emotions surrounding the word risk and the use of risk analysis in engineering. Thus, it is important to understand and have a good plan for communicating risk, including:

- What information is available at a given dam or levee related to potential failure modes and how the information is considered in a risk analysis
- How risk will be considered by an organization
- What the results of the risk analyses are
- What decisions were reached and what risk remains

## **Chapter A-9 Governance and Guidelines**

This communication can help create an awareness of potential dam safety issues and help all parties gain a greater understanding. Creating an understanding of risk and dam safety issues is important for those who have varying degrees of connections to the dam and the associated potential impacts. These diverse groups have a variety of backgrounds, experience, and sophistication. Communication plans and strategies should be developed for the following:

- Internal to a safety organization
- Owners and stakeholders
- Dam or levee site and project personnel
- Local organizations
- Technical organizations or consultants
- Decision makers
- The public

The following principles apply to risk communication:

1. Enhance communication with the public, internally within dam owning and regulating organizations, and Emergency Management Agencies.
2. Emergency Action Plans and communication with the public are important and integral aspects of reducing risk to life.
3. Communications should be open and transparent.
4. When presenting safety issues at a given dam or levee, focus on the benefits and the risks posed by the infrastructure.
5. Integrate risk communications early in the process of responding to safety issues.
6. Provide context for risk communications (compare with other risks).
7. Focus communications on actions that individuals/organizations need to take.
8. Discuss uncertainty in risk estimates and the safety case:
  - What is certain
  - What is likely, but not certain
  - What is possible, but not likely

## **A-9.9 References**

- Australian National Committee on Large Dams (ANCOLD). 2003. Guidelines on Risk Assessment. ANCOLD, Sydney, New South Wales, Australia.
- Ball, D.J. and P.J. Floyd. 1998. Societal Risks. Report prepared for UK Health & Safety Executive.
- BC Hydro (see British Columbia Hydro).
- British Columbia Hydro (BC Hydro). 1995. Seminar and Workshop on Risk-Based Dam Safety Evaluations. Sponsored by BC Hydro.
- Bureau of Reclamation (Reclamation). 2011. [Dam Safety Public Protection Guidelines](#). Dam Safety Office, Denver, Colorado.
- Canadian Dam Association. 2007. Dam Safety Guidelines. Canadian Dam Association, Edmonton, Alberta, Canada.
- Douglas, K.J., M. Spannagle, and R. Fell. 1998. Analysis of Concrete and Masonry Incidents, UNICIV Report No. R-373. The University of New South Wales, Sydney, Australia.
- Federal Emergency Management Agency. 2004. [Federal Guidelines for Dam Safety](#). Federal Coordinating Council for Science Engineering and Technology. Interagency on Dam Safety, Washington, D.C.
- Federal Emergency Management Agency. 2005. Federal Guidelines for Dam Safety.
- \_\_\_\_\_. 2015. Federal Guidelines for Dam Safety Risk Management, FEMA P-1025.
- Foster, M.A., R. Fell, and M. Spannagle. 1998. Analysis of Embankment Dam Incidents, UNICIV Report No. R-374. The University of New South Wales, Sydney, Australia.
- Hatem, G.A. 1985. Development of a Data Base on Dam Failures in the United States: Preliminary Results. A Thesis Summated to Stanford University Civil Engineering. December 1985.

## **Chapter A-9 Governance and Guidelines**

Health & Safety Executive (HSE). 2001. [Reducing Risks, Protecting People: HSE's Decisionmaking Process](#). Risk Assessment Policy Unit. HSE Books, Her Majesty's Stationery Office, London, England.

HSE (see Health & Safety Executive).

LeGuen, J. 2008. Tolerability of Risk: UK Principles and Practices for Controlling Work Activities, Presentation at the Workshop on Tolerable Risk Evaluation, March 18, 2008, Alexandria, Virginia.

New South Wales Government Dams Safety Committee. 2006. Risk Management Policy Framework for Dam Safety. New South Wales, Australia, 22 August 2006.

Office of Management and Budget (OMB). 2007. Updated Principles for Risk Analysis, Memorandum for the Heads of Executive Departments and Agencies. September 19, 2007.

OMB (see Office of Management and Budget).

Planning NSW. 2008. Risk Criteria for Land Use Safety Planning, Hazardous Industry Planning, Advisory Paper No. 4, Consultation Draft. July 2008.

Reclamation (see Bureau of Reclamation).

United States Army Corps of Engineers (USACE). 2014. [Safety of Dams – Policy and Procedures](#), ER-1110-2-1156. March 31, 2014.

USACE (see United States Army Corps of Engineers).

Von Thun, J.L. 1985. Application of Statistical Data From Dam Failures and Accidents to Risk-Based Decision Analysis on Existing Dams, Internal Memorandum. Bureau of Reclamation, Engineering and Research Center. October 1985.