ICOLD Bulletin on Dam Safety Management

David S. Bowles[1], Francisco L. Giuliani[2], Desmond N.D. Hartford[3], J.P.F.M. (Hans) Janssen[4], Shane McGrath[5], Michel Poupart[6], David Stewart[5], Przemyslaw A. Zielinski[7]

[1] *Institute for Dam Safety Risk Management, Utah State University, Logan, Utah, USA and RAC Engineers & Economists, Providence, Utah, USA*
[2] *Organismo Regulador de Seguridad de Presas (ORSEP), Cipolletti, Argentina*
[3] *BC Hydro, Vancouver, British Columbia, Canada*
[4] *Rijkswaterstaat, Utrecht, The Netherlands*
[5] *Goulburn-Murray Water, Tatura, Victoria, Australia*
[6] *Electricite de France, Grenoble, France*
[7] *Ontario Power Generation, Toronto, Ontario, Canada*

The ICOLD Committee on Dam Safety (CODS) "was established as a coordinating body to assure an integrated approach of all Technical Committees to safety issues, to guide toward action where shortcomings or gaps may be perceived, to define a common safety philosophy and to prepare general guidelines on dam safety outlined along this philosophy." As part of this mandate the CODS has initiated the preparation of a new bulletin aimed at development and documentation of the general structure of a system approach to the safety management of dams. The approach intends to address the interdependencies and wide range of arrangements that are necessary to ensure that the safety of dams is properly managed. The document will build on principles established by ICOLD Bulletins 59 (Dam Safety) and 130 (Risk Assessment), with the goal of assisting those responsible for dam safety to develop, review and improve dam safety management systems. The document is being developed with significant opportunity for consultation with all ICOLD Technical Committees.

Key concepts in developing the Bulletin are centred on the following issues:

- *Dam safety management has to be developed as part of an integrated management system of the dam owning organization.*
- *Safety fundamentals should include the key principles of Prevention-Control-Mitigation*
- *A balance between social equity and economic efficiency can form the basis for establishing target levels of safety in a general way for all ICOLD member countries and in a way that does not explicitly rely on quantitative risk assessment.*
- *Clearly-defined roles are needed for the Responsible Entity (owner or operator) and the Government/ Regulator.*
- *An effective dam safety management program must address interrelationships amongst technical and management aspects of program activities in all life cycle stages.*
- *In addition to individual dam issues, portfolio issues must be addressed from the owner's and regulator's perspectives.*

Keywords: *dams, dam safety, dam safety management*

Introduction

In 2004 the ICOLD Executive Meeting decided that all ICOLD Bulletins published before 1987 should undergo a review by their respective Technical Committee and should be updated if necessary. The ICOLD Committee on Dam Safety (CODS) has been charged with the review and an update of Bulletin 59 (Dam Safety Guidelines), which was published in 1987. When the CODS was first established in 1982, its terms of reference stated that it:

> *"was established as a coordinating body to assure an integrated approach of all Technical Committees to safety issues, to guide toward action where shortcomings or gaps may be perceived, to define a common safety philosophy and to prepare general guidelines on dam safety outlined along this philosophy."*

The result of this charge was ICOLD Bulletin 59, establishing general guidance on dam safety assessment and management. In 2005 ICOLD issued Bulletin 130 (*Risk Assessment in Dam Safety Management - A Reconnaissance of Benefits, Methods and Current Applications*), which was prepared by the CODS. The current effort of the CODS is focused on developing and documenting the general structure of a systems approach to the safety management of dams. The approach is intended to address all interdependencies and will encompass all arrangements that are necessary to ensure that the safety of dams is properly managed. The Bulletin will build on the principles and general philosophy established by both Bulletins 59 and 130, with the expectations that it will assist those responsible for dam safety, at all organizational levels, to develop, review and improve dam safety management systems.

Key concepts in developing the Bulletin are centred on the following issues:

- Dam safety management has to be developed as part of an integrated management system of the Responsible Entity (Owner or operator).
- Safety fundamentals should include the key principles of Prevention-Control-Mitigation.
- A balance between social equity and economic efficiency can form the basis for establishing target levels of safety in a general way in any ICOLD member country and in a way that does not explicitly rely on quantitative risk assessment.
- Clearly-defined roles are needed for the Responsible Entity and the Government Authority/Regulator.
- An effective dam safety management program must address the interrelationships amongst technical and management aspects of program activities in all life cycle stages.

Dam safety and management of risks

Historically, the underlying philosophy for dam safety has been that

> *"the safety of a dam manifests itself in being free of any conditions and developments that could lead to its deterioration or destruction. The margins which separate the actual condition of a dam, or the conditions it is designed for, from those leading to its damage or destruction is a measure of its safety"* (ICOLD Bulletin 59).

Bulletin 59 clearly recognised that the safety of dams depends on more than engineered factors, and that the failure of a dam is a complex process that can include human error in design, construction, operation, maintenance and surveillance. Since the publication of Bulletin 59, the understanding of the causes of failures of complex engineered systems, such as dams, and indeed complex systems in general, has advanced considerably. Accordingly, the underlying philosophy of this proposed Bulletin is that a systematic approach and a comprehensive management systems framework, which account for the complexities of the operation of dams in a modern society, are fundamental for achieving and assuring dam safety.

ICOLD Bulletin 130 brought forward another aspect of a properly designed dam safety management program. It pointed out that at the high level of any safety-related decision making "*there are two fundamental competing principles:*

- *Equity – the right of individuals and society to be protected*
- *Efficiency – the need that society has to distribute and use its available resources in such a way as to gain maximum benefit."*

The matter of striking an appropriate balance between these two principles is of fundamental importance. There should be no doubt that all stakeholders that could be adversely affected by a dam failure have an inalienable right to safety. This unconditional right to a certain level of protection has lead to the development of standards, which in practical terms were means of defining a limit or maximum level of risk above which no individual should be exposed. However, rights often conflict and in the real world there are no rights that are absolute. The current dam safety practice often does not adequately and sufficiently address the need to maintain a balance between the conflicting social principles of equity and efficiency.

It can be stated that typically, the level of safety for any activity in a society varies in some proportion to the societal consequences of the activity going wrong. The hazard classification systems used in dam safety are an example of this in practice. This said, and not withstanding the fact that absolute safety cannot be achieved, there is a general societal desire to do more to improve safety and to protect the environment. However, at least conceptually, and actually in many endeavours, the notion of the level of safety varying in some proportion to the consequences of the activity going wrong provides a framework for consideration of the whole matter of levels of safety or safety standards.

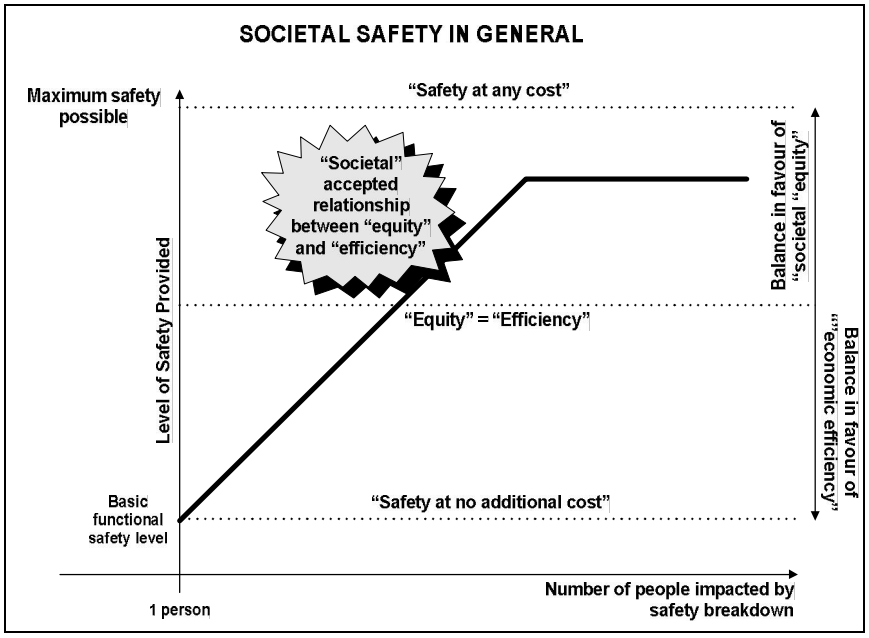
The recognition by governments that risk is an inevitable part of the human condition, and that government intervention in societal activities that generate risk is necessary, are central to determining levels of safety in a society. The recognition of this fact by Governments has resulted in laws and regulations pertaining to the safety of hazardous activities. In any country, the body of laws is usually complex, largely because the process of government is political and not pre-determined by scientific principles. However, science, in the sense of reliable knowledge, can play a vital role in informing political choices. Even where the law is clear with respect to the level of safety to be achieved, political considerations can override the existing law and deliver a different result.

The extent to which government will be involved in assuring the safety of dams covers the entire spectrum from no involvement whatsoever, to extensive prescriptive regulations administered by government through a "Regulator". In cases where there is no government involvement, the safety of the dam is entirely a matter for the owner ("Responsible Entity"); whereas with extensive prescriptive regulation, the government takes a large degree of the responsibility for dam safety, with the owner simply implementing directives. Between these two extremes, responsibility for dam safety is shared by the dam owner and the "regulator", with the "regulator" setting standards or performance goals, and the owner establishing means to interpret and meet them. In some cases, government will establish a regime whereby an independent engineer, acceptable to government and the owner, will be engaged to interpret the intent of the prevailing dam safety standard or performance goal. Under such circumstances, the independent engineer will carry a significant responsibility for the safety of the dam.

From the perspective of dam engineering, the level of safety can be considered as bounded by the following two extremes:—the maximum level of safety that is physically achievable at any cost, and a minimum level below which

the dam cannot withstand normal operating conditions, referred to as a "basic functional safety level". Between these bounds, safety decision-making involves striking a balance between the risks and the benefits and between social equity and economic efficiency as outlined in Bulletin 130 and as illustrated in Figure 1.

Figure 1. Conceptual definition of the level of safety



Overarching framework and philosophy

The proposed Bulletin is to be developed through a regular consultative process within the Committee on Dam Safety and periodic consultations with other Technical Committees.

The Bulletin will embody modern concepts of managing the safety of dams in the context of protecting the public, property and the environment from the failure of the dam to perform all of its functions. In this respect, dam safety is not simply restricted to preventing dam collapse; rather dam safety includes the operational aspects of the dam and reservoir. Dams, reservoirs and river systems will be considered as systems and the safety of dams will be analysed using the methods of systems analysis. The safety of dams, in the general sense outlined above, will be considered in the context of other industrial hazards that can be characterized in terms of risks. However, the broad framework of the proposed Bulletin will be applicable whether or not quantitative risk assessment is explicitly used. Figure 2 illustrates the overall structure of the proposed Bulletin.

Safety fundamentals

The Bulletin will set out basic objectives, concepts and fundamental principles, which, if applied will ensure that the desired level of dam safety is being achieved through the on-going application of the managed safety system. In the application of these fundamentals, differences between the legal systems in ICOLD member countries, their societal and cultural preferences, and their traditional dam safety practices will lead to differences in how a particular safety management system is designed and implemented. The proposed Bulletin will provide the guidance on the application of these concepts and principles.

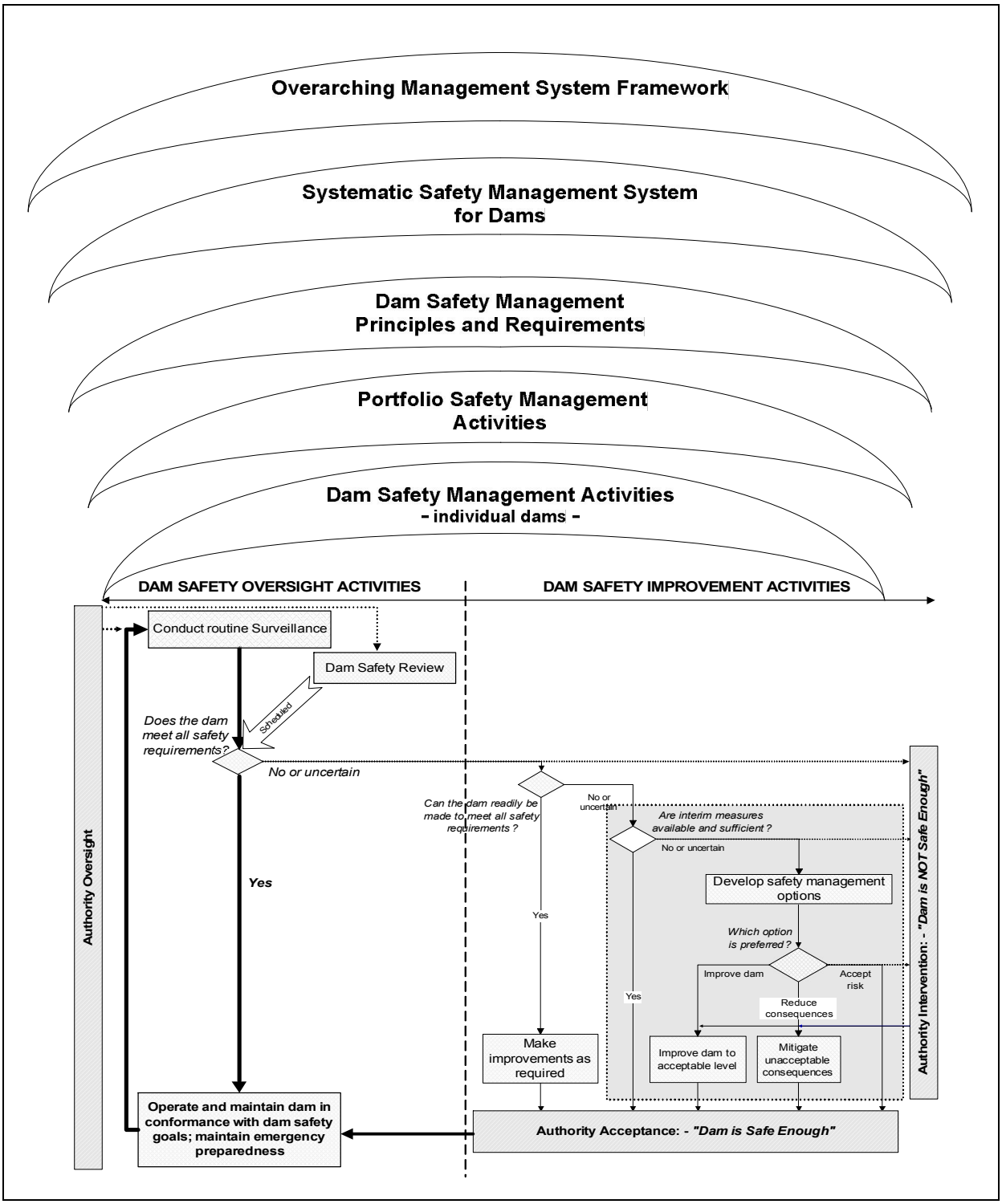
Dam safety objective

The overarching dam safety objective is to protect people, property and the environment from the harmful effects of misoperation or failure of dams and reservoirs

This overarching objective can be achieved by controlling the stored volume of water and controlling all flows through and around the dam within specified limits. It has to be achieved without unduly limiting the operation of dams and reservoirs or the conduct of operations that create the benefits of taking the dam safety risks. To ensure that dams and reservoirs are operated and that activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following three fundamental safety objectives:

- To control the release of damaging discharges downstream of the dam,
- To restrict the likelihood of events that might lead to a loss of control over the stored volume and the spillway and other discharges,
- To mitigate through on-site accident management and/or emergency planning the consequences of such events if they were to occur.

Figure 2. Proposed Bulletin structure



These fundamental safety objectives apply to all facilities and activities and to all stages over the lifetime of a facility, including planning, design, manufacturing, construction, commissioning and operation, as well as decommissioning and closure.

Dam safety principles

A unified set of nine principles representing a common safety philosophy have been modeled on the application of universal safety standards for hazardous installations (Management of Operational Safety in Nuclear Power Plants, 1999 and Fundamental Safety Principles, 2006). These nine principles form the basis from which safety requirements for dams can be developed and safety measures implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances.

Principle 1: Responsibility for dam safety

The prime responsibility for dam safety should rest with the entity responsible for the dam and the activities that give rise to the risks

Responsibility for dam safety should be clearly defined. Government is ultimately responsible for assuring the safety of the public, property and the environment, around and downstream of dams.

The entity that has the prime and direct responsibility for achieving dam safety and for the activities that give rise to the risks is referred to in the proposed Bulletin as the "Responsible Entity". A government institution may be the Responsible Entity that is directly responsible for the safety of the public, such as in cases where dams are owned and operated by government. In other cases, government institutions might only have oversight of the safety management activities of non-governmental bodies that own or operate a dam.

The safety arrangements established by the Responsible Entity must conform to the requirements and expectations of Government and the prevailing laws, regardless of how they are established and implemented. Therefore, the Responsible Entity's values and principles reside within the overarching legislative and regulatory values system.

In order for the Responsible Entity to meet its obligations in relation to the safety of its dams, it is necessary to ensure that its dam safety management activities are approached in a systematic way. The aim should be to achieve and enhance safety by formulating and documenting the planned and systematic actions necessary to provide adequate confidence that all safety requirements are satisfied and by embedding them in the organization and its workforce.

Some Responsible Entities (owners or operators) for dams may have significant dam engineering and safety management capability and be capable of implementing all aspects of dam safety management over the entire life-cycle of the project. A self-regulating government dam owning agency can be an example of such an entity. At the other extreme, the Responsible Entity might be the legislative and judicial arms of Government, where the safety of dams is implied by existing legislation and precedents, with all responsibility for meeting the intent of the law resting with the dam owner/operator.

Principle 2: Role of government

The legal and governmental framework for safety provides the overarching structures for dam safety assurance

A properly established legal and governmental framework provides for the regulation of dams and reservoirs, and related operational activities that can give rise to a dam breach and other inundation risks, and for the clear assignment of responsibilities. The government is responsible for the adoption within its national legal system of such legislation, regulations, and other standards and measures as may be necessary to effectively fulfil all of its national responsibilities and, where relevant, its international obligations. A modern view of safety governance includes the establishment of an independent regulatory body to assure the safety of dams.

Government authorities should ensure that arrangements are made for preparing programmes of actions to reduce risks from dams, including actions in emergencies, for monitoring high discharges to the environment, and for disposing of reservoir silt waste. This does not require that Government establishes and maintains these arrangements, but Governments may choose to do so. In addition, Government authorities have to address the safety of dams for which no other organization has responsibility.

Principle 3: Leadership and management for safety

Effective leadership and management for safety should be established and sustained in organizations responsible for dam risks

In general, leadership in safety matters should be demonstrated at the highest levels in all organizations with responsibility for dam safety risks. Safety has to be achieved and maintained by means of an effective management system that integrates all elements of management. Thus, the requirements for safety should be established and applied coherently with other requirements, including those for human performance, quality and security, and so that safety is not compromised by other requirements or demands. The management system also has to ensure the promotion of a safety culture, the regular assessment of safety performance, and the application of lessons learned from experience.

An important factor in a management system is the recognition of the entire range of interactions of individuals at all levels with technology and with organizations. To prevent human and organizational failures, human factors have to be taken into account and good performance and good practices have to be supported.

Safety has to be assessed for all dams and reservoirs and for all operational activities, consistent with a graded

approach. Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to control the hazards, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them. Where control measures or operator actions are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the arrangements made are robust and that they can be relied on. A dam may only be constructed and commissioned once it has been demonstrated, to the satisfaction of the regulatory body if one exists, that the proposed safety measures are adequate.

The process of safety assessment of dams is repeated in whole, or in part, as necessary, in the conduct of operations in order to account for changed circumstances (such as the application of new standards or scientific and technological developments), the feedback of operating experience, modifications, and the effects of ageing. For operations that continue over long periods of time, assessments should be reviewed and repeated periodically as necessary.

Despite all measures that are taken, accidents may occur. The accepted view is that lessons should be learned from accidents and measures should be implemented to prevent recurrence of the accident. Accordingly, the precursors to accidents must be identified and analysed, and measures taken to prevent the recurrence of accidents. The feedback of operating experience of dams everywhere is a key means of enhancing safety. Processes should be put in place for the feedback and analysis of operating experience, including initiating events, accident precursors, near misses, accidents and unauthorized acts, so that lessons may be learned, shared and acted upon.

Principle 4: Justification for dams and reservoirs

Dams, reservoirs and activities that give rise to dam safety risks should yield an overall benefit to society

The construction of a dam imposes risks on society, and typically these risks are unevenly distributed, such that those who benefit from the dam are not necessarily those on whom the risk is imposed. For dam and reservoir activities to be considered justified, the benefits that they provide to society as a whole should outweigh their costs and the risks that they create. For the purposes of assessing benefits and risks, all significant positive and negative consequences of the operation of dams and reservoirs have to be taken into account.

In many cases, decisions relating to benefits and risks are taken at the highest levels of government, such as a decision by a State to embark on a dam building programme. In other cases, the regulatory body may determine whether a dam proposed by a private entity is justified.

Principle 5: Optimisation of protection

It is recommended that protection should be optimized to provide the highest level of safety that can reasonably be achieved

The safety measures that are applied to dams, which give rise to societal risks, are considered to be optimized if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the dam, without placing an unreasonable burden on society and without unduly limiting its utilization. Optimization of protection should be considered in terms of risks to individuals, to society and to future generations as described in Principles 6 and 7 below. The optimisation process necessarily involves making comparisons and trade-offs between competing interests that cannot be compared directly. Risk acceptability is a complex issue, which is, in principle, a political issue. Therefore, the optimization process needs to include political factors that are, more often than not, non-measurable.

To determine whether dam safety risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, should be assessed a priori and periodically reassessed throughout the lifetime of facilities and activities.

Where there are interdependencies between related actions or between their associated risks (e.g., for different stages of the lifetime of dams and reservoirs, or for risks to different groups), these should also be considered. Account also has to be taken of uncertainties in knowledge.

The optimization of protection also means using good practices and common sense to avoid dam safety risks as far as is practical in day-to-day activities. The resources devoted to safety by the Responsible Entity, and the scope and stringency of regulations and their application, have to be commensurate with the magnitude of the dam safety risks and their amenability to control. Regulatory control may not be needed where this is not warranted by the magnitude of the dam safety risks.

Principle 6: Limitation of risk to individuals

Measures for controlling dam safety risks should ensure that no individual bears an unacceptable risk of harm

Justification and optimization of protection do not in themselves guarantee that no individual, including employees and operators, bears an unacceptable risk of harm. Risk limits, where defined, typically represent a legal upper bound of acceptability, they are insufficient in themselves to ensure the best achievable protection under the circumstances, and they therefore have to be supplemented by the optimization of protection. Thus, both the optimization of protection and the limitation of risks to individuals are necessary to achieve the desired level of safety.

Principle 7: Protection of present and future generations

People, property and the environment, present and future, should be protected against the effects of dam failures and other reservoir risks

Due account must be taken of the fact that dam safety management decisions made in the present will affect future generations, and therefore have impacts that span many human generations. Similarly, dams are not benign with respect to the environment and the long-term risks to the environment must also be considered.

Dam breach inundation may transcend national borders and may persist for a period of time (in some cases, one month or more). The possible consequences, now and in the future, of current actions have to be taken into account in judging the adequacy of measures to control risks of dam failure and reservoir release. Whereas the effects of exposure to flood waters on human safety and health are relatively well understood, albeit with some uncertainties, the effects of severe flood waters on the environment have been less thoroughly investigated. The general intent of the measures taken for the purposes of environmental protection has been to protect ecosystems against dam breach floods and damaging inundation that would have adverse consequences for populations of a species (as distinct from individual organisms).

Principle 8: Prevention of accidents

All reasonably practicable efforts should be made to prevent and mitigate dam failures and accidental releases

To ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken to achieve the following:

- To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to uncontrolled release of all or part of the stored volume*;*
- To prevent the escalation of any such incidents or abnormal conditions that do occur.

The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. This principle is implemented mainly through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people, property or the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

The CODS recognises that there are some practical difficulties in achieving 'defence in depth' for all critical elements of dams, largely because it is not possible to ensure redundancy of the physical protection systems. Therefore, conservative criteria and non-physical measures, as outlined below, should be provided to compensate for the lack of physical redundancy. Defence in depth is provided by an appropriate combination of an effective management system and the incorporation of good design and engineering features providing safety margins, diversity and redundancy.

Accident and incident management procedures should be developed in advance to provide the means for regaining control of the reservoir or a spill in the event of a loss of control of the reservoir, and for mitigating any destructive consequences.

Principle 9: Emergency preparedness and response

Appropriate arrangements should be made for emergency preparedness and response for dam failures and accidental releases

The primary goals of preparedness and response for a dam breach emergency are as follows:

- To ensure that arrangements are in place for an effective response at the scene and, as appropriate, at the local, regional, national and international levels, to a dam breach emergency*;*
- To ensure that, for reasonably foreseeable incidents, inundation consequences would be minor;
- For any incidents or failures that do occur, to take practical measures to mitigate any consequences for human life and health, property and infrastructure, and the environment.

The dam owner/Responsible Entity, the employer, the regulatory body and appropriate branches of government have to establish, in advance, the arrangements for emergency preparedness and response for a dam breach emergency at the scene, at local, regional and national levels and, where so agreed, between countries at the international level.

The scope and extent of arrangements for emergency preparedness and response have to reflect the following:

- The likelihood and the possible consequences of a dam breach emergency;
- The characteristics of the dam breach flood;
- The nature and location of the dam and reservoir and operational activities and their proximity to habitations and dam safety infrastructure;
- Criteria set in advance for use in determining when to take different protective actions;
- The capability to take actions to protect and inform personnel at the scene, and if necessary the public, during an emergency.

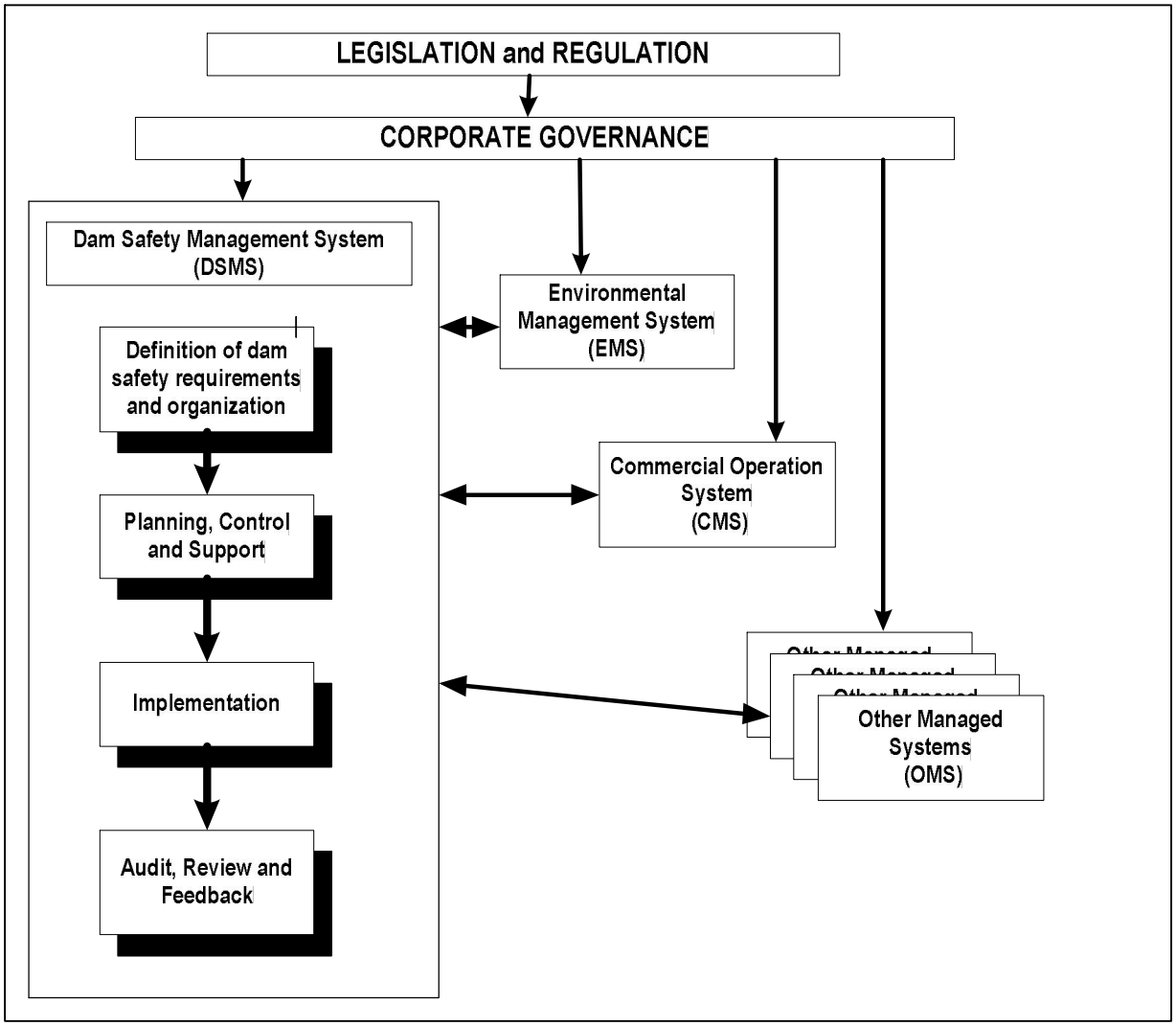
In developing the emergency response arrangements, consideration has to be given to all reasonably foreseeable events. Emergency plans should be exercised periodically to ensure the preparedness of the organizations having responsibilities in emergency response, but such exercises do not replace the requirement to adequately prepare emergency plans.

Dam safety management system (DSMS)

Safety fundamentals, as outlined above, can be most efficiently implemented through a Dam Safety Management System (DSMS) that is illustrated in Figure 3. A DSMS can be perceived as an administrative framework that allows the organization to achieve and ensure good safety performance. It does not mean that safety is managed separately from other activities; on the contrary, if it is to succeed, it not only will comprise those arrangements that are primarily safety-oriented, but it must be well integrated with those arrangements that contribute to the organization's other objectives. Although a DSMS can be developed as a stand-alone managed system it is preferable that it be a part of an integrated management system. The integrated system approach not only focuses on satisfying all operational requirements, but also maintains and improves safety performance. An integrated system provides a framework allowing for consistent and efficient consideration of all organizational objectives, goals and plans. It is capable of addressing the impacts of their interdependencies, establishing proper prioritization, and ensuring that these priorities are included in the decision-making process.

Figure 3 illustrates the general concept of the Dam Safety Management System. It also shows the links between the DSMS and other managed systems in the organization. The systems should be linked together into a single integrated management system.

Figure 3. Dam Safety Management System



Conclusions

The Bulletin is still a work in-progress. Because of its importance for not only the CODS, but also for all other ICOLD Technical Committees, the consultative approach adopted at the initiation stage will be continued. The ultimate goal of the proposed Bulletin is the development of a comprehensive and consistent management system that is able to identify and demonstrate that the dam is safe and which does not pose unacceptable risks to public safety, property and the environment. This goal can be achieved only with the cooperation of all parties involved

during the lifecycle of a dam. Dams that meet this test would further require some mechanism for managing residual risks and the proposed Bulletin will also address this task.

The authors would welcome feedback and comments from ICOLD Members on the framework and issues presented in this paper to assist in the development of the Bulletin.

Acknowledgements

The kind permission of the ICOLD Executive Director to republish this paper, which was first published in the 2007 St Petersburg ICOLD Symposium Proceedings, is gratefully acknowledged.

References

ICOLD (International Commission on Large Dams). 1987. Dam Safety Guidelines. ICOLD Bulletin 59.

ICOLD 2005. Risk Assessment in Dam Safety Management - A Reconnaissance of Benefits, Methods and Current Applications. ICOLD Bulletin 130.

IAEA (International Atomic Energy Agency) 1999. Management of Operational Safety in Nuclear Power Plants, INSAG-13.

IAEA (International Atomic Energy Agency) 2006. Fundamental Safety Principles. Safety Fundamentals SF-1.