Operational Safety of Dams and Reservoirs

Understanding the reliability of flow-control systems

Operational Safety of Dams and Reservoirs

**Understanding the reliability of flow-control
systems**

**Desmond ND Hartford
Gregory B Baecher
P Andy Zielinski
Robert C Patev
Romanas Ascila
and
Karl Rytters**

Published by ICE Publishing, One Great George Street, Westminster, London SW1P 3AA

Full details of ICE Publishing sales representatives and distributors can be found at:
www.icebookshop.com/bookshop_contact.asp

Other titles by ICE Publishing:

Risk and Uncertainty in Dam Safety.

Desmond ND Hartford, Gregory Baecher. ISBN 978-0-7277-3639-0

Hydraulic Gates and Valves in Free Surface Flow and Submerged Outlets.

Jack Lewin. ISBN 978-0-7277-2990-3

Floods and Reservoir Safety, Fourth edition.

Institution of Civil Engineers. ISBN 978-0 7277-6006-8

A Guide to the Reservoirs Act 1975, Second edition.

Institution of Civil Engineers. ISBN 978-0-7277-5769-2

www.icebookshop.com

A catalogue record for this book is available from the British Library

ISBN 978-0-7277-6121-7

© Thomas Telford Limited 2016

ICE Publishing is a division of Thomas Telford Ltd, a wholly-owned subsidiary of the Institution of Civil Engineers (ICE).

All rights, including translation, reserved. Except as permitted by the Copyright, Designs and Patents Act 1988, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise, without the prior written permission of the Publisher, ICE Publishing, One Great George Street, Westminster, London SW1P 3AA.

This book is published on the understanding that the author is solely responsible for the statements made and opinions expressed in it and that its publication does not necessarily imply that such statements and/or opinions are or reflect the views or opinions of the publishers. Whilst every effort has been made to ensure that the statements made and the opinions expressed in this publication provide a safe and accurate guide, no liability or responsibility can be accepted in this respect by the author or publishers.

Whilst every reasonable effort has been undertaken by the author and the publisher to acknowledge copyright on material reproduced, if there has been an oversight please contact the publisher and we will endeavour to correct this upon a reprint.

The views and opinions expressed in this this book do not reflect the positions of the US Department of the Army or US Department of Defense.

Cover image: Lady Evelyn Dam owned by Ontario Power Generation, Toronto, Canada.

Commissioning Editor: Laura Balchin

Production Editor: Rebecca Norris

Market Development Executive: Elizabeth Hobson

Typeset by Academic + Technical, Bristol

Index created by James Helling

Printed and bound in Great Britain by TJ International Ltd, Padstow

This volume is dedicated to the memory of Dr Michael J Casey PE – friend and colleague.

Contents

Acknowledgements	ix
About the authors	xi
Foreword	xiii
Preface	xvii

Part I. Dam systems and modelling 1

01	Flow control failures in dam safety	3
	1.1. Operational safety	3
	1.2. Operational incidents and failures	4
	1.3. Contemporary dam safety risk analysis	13
	1.4. Flow control	17
	1.5. Dams as engineered systems	21
	1.6. The need for a new approach	21
	1.7. The organisation of this book	24
	References	24

02	Management, control and operation	27
	2.1. System operation	27
	2.2. Operational objectives	32
	2.3. Operational strategies	36
	2.4. Qualitative modelling of dam safety management activities	40
	2.5. Stable and unstable system states	42
	References	46

03	Systems and systems engineering	47
	3.1. Objectives of the systems approach	47
	3.2. Dam safety from a systems perspective	49
	3.3. Systems models	51
	3.4. General systems engineering process	61
	3.5. Example of system operational arrangements	62
	3.6. Operational arrangements and instructions under fault conditions	69
	3.7. Dam safety in relation to systems	71
	3.8. Summary	73
	References	73

04	Modelling dam and reservoir systems	75
	4.1. Performance and reliability of dam systems	75
	4.2. Beyond current risk analysis	79
	4.3. Modelling approach	83
	4.4. Modelling framework	84
	4.5. Functional considerations	96
	4.6. Tracking system states	97
	4.7. Component reliability	99
	4.8. Interpreting the results of simulation models	102
	References	103

Part II. Inputs and constraints 105

05	Hydrological modelling and river flow routing	107
	5.1. River systems modelling	107
	5.2. Hydrological modelling	113
	5.3. Example of the Madawaska River watershed	124
	5.4. Time-series modelling of reservoir inflow	130
	5.5. Streamflow routing model	138
	5.6. Uncertainty in watershed and streamflow modelling	143
	References	154

06	Reservoir and outflow control	161
	6.1. Operating concepts	161
	6.2. Role of simulation and optimisation in system operation	168
	6.3. Decision-support systems in operation	169
	References	171

07	Disturbances	173
	7.1. Disturbances defined	173
	7.2. Probabilistic model of disturbances	176
	7.3. Seismic hazard	183
	7.4. Floating debris	187
	7.5. Ice and icing effects on flow control	195
	7.6. Interference with discharge function	203
	7.7. Landslides	207
	7.8. Forest fires	210
	7.9. Tornadoes	211
	7.10. Miscellaneous disturbances	212
	References	215
	Part III. Engineered systems of flow control	221
08	Release function and human factors	223
	8.1. Gate systems	223
	8.2. Spillway accidents	224
	8.3. Gated spillways	231
	8.4. Fault-tree analysis	235
	8.5. Human reliability analysis for spillway systems	241
	References	249
09	Discharge conveyance function	251
	9.1. The conveyance process	253
	9.2. Conveyance failure process	255
	9.3. Hydraulic analysis	263
	9.4. Flow in closed conduits	278
	9.5. Energy dissipation	284
	9.6. Hydraulic system simulation	289
	References	299
	Part IV. Modelling dam and reservoir systems	303
10	Simulating flow control operations	305
	10.1. System simulation of hydropower operations	305
	10.2. Stochastic simulation	308
	10.3. Systems model of the Mattagami River	314
	10.4. Systems dynamics	338
	10.5. Systems model of the Göta River	341
	10.6. Verification, validation and accreditation	351
	References	355
11	Postscript	357
	11.1. Development of risk analysis in dam safety	357
	11.2. Effectiveness of current risk-analysis approaches to dam safety	358
	11.3. The next generation of risk analysis for dam safety	359
	11.4. The goal of this book	359
	11.5. Summary	360
	References	360
Appendix	Weibull data for gate components	361
	References	366
	Index	367

Acknowledgements

Sponsors and sponsors' representatives

BC Hydro, Stephen Rigbey
Elforsk – Swedish Electrical Utilities R&D Company, Cristian Andersson
Ontario Power Generation, Tony Bennett
Vattenfall, Lars Hammar, Urban Norstedt (ret.)
US Army Corps of Engineers, Robert C. Patev, Andy Harkness

Core working group and project manager

Romanas Ascila, Vattenfall
Gregory Baecher, University of Maryland
Mona Bechai, MOBEC Engineering
Desmond Hartford, BC Hydro
Robert Patev, US Army Corps of Engineers
Karl Rytters, Sekond AB
P. Andy Zielinski, Ontario Power Generation

Analysis team

Tyler Atkinson, Ontario Power Generation
Michael Casey, George Mason University
Qianli (Shally) Deng, University of Maryland
Mikael Mathiesen, SWECO
Niklas Mattsson, Uppsala University
Rebecca McAfoos, University of Maryland
Andrew Sander, US Army Corps of Engineers
David Strajt, BC Hydro
Yibing Zhang, Ontario Power Generation

Reviewers

John T Christian
Peter Mason
Slobodan Simonovic

About the authors

Desmond ND Hartford is Principal Engineering Scientist at BC Hydro reporting to the Director of Dam Safety. His responsibilities at BC Hydro span the development of risk management policy, risk-informed decision processes, and risk-informed management systems for BC Hydro's Hydropower and Dams risk profile. Dr Hartford is also responsible for introducing systems engineering techniques into the analysis of functionality of river systems and associated hydropower sub-systems; guiding the application of engineering principles-based assessment of spillway gate reliability comparable to those of the nuclear safety case regime; and leading BC Hydro's research and development activities for dam safety. He presently holds the position of Adjunct Professor in Civil Engineering at the University of Western Ontario providing industry guidance on a new research project to develop a prototype systems engineering model suitable for application in BC Hydro's natural and operating environment. Dr Hartford has received several national and international awards and honours, is an overseas member of the Royal Swedish Academy of Engineering Sciences, and in 2011 was recognised as one of the 20 most influential engineers in the world of Hydropower and Dam Engineering.

Gregory B Baecher is Glenn L Martin Institute Professor of Engineering at the University of Maryland. He is a geotechnical engineer with 40 years' experience specialising in asset and risk management for water resource development projects, dam and levee safety, hydropower and navigation. He is the author of five books on risk, safety and management of civil infrastructure, and over 200 technical publications. He is a member of the US National Academy of Engineering, recipient of the USACE Commander's Award for Public Service for his contributions to the levee system risk analysis of New Orleans following Hurricane Katrina, and recipient of the Panamanian National Award for Science and Technology Innovation for his contributions to enterprise risk management at the Panama Canal. Dr Baecher has worked extensively with US federal agencies on dam and levee safety and coastal protection works.

Przemyslaw A Zielinski, is Manager, Technology and Dam Safety at Ontario Power Generation (OPG) in Canada. Since the late 1980s Dr. Zielinski has been involved in numerous studies and assessments of safety of OPG dams. At OPG Dr Zielinski is responsible for developing risk management programmes for OPG portfolio of 240 dams. He was instrumental in drafting the regulatory framework for risk-informed dam safety assessment and decision-making in the province of Ontario. He is currently serving on the Dam Owners Advisory Committee for the Ministry of Natural Resources and Forests – regulator of dam safety in Ontario and on the Tennessee Valley Authority (TVA) Dam Safety Independent Review Board (IRB) which acts in an advisory role to the TVA's Dam Safety Officer. In 2010 he was elected as the Fellow of the Engineering Institute of Canada. Since the early 2000s, Dr Zielinski has been actively involved in the works of International Commission on Large Dams (ICOLD) and he is one of the principal authors of ICOLD Bulletin on Dam Safety Management. In 2013 he was elected as Vice Present of ICOLD and he is the current chair of the ICOLD Committee on Dam Safety. Dr Zielinski is also an active member of Canadian Dam Association where he co-chairs the Dam Safety Committee. In addition to his research in field of risk assessment and risk-informed decision-making in dam safety, he currently holds the position of Adjunct Professor at the System Design Engineering Department of the University of Waterloo.

Robert C Patev is National Risk Advisor at the Risk Management Center, Institute for Water Resources, U.S. Army Corps of Engineers. His duties have included serving as the National Risk Advisor for the US Army Corps of Engineers and he currently provides technical oversight and direction to the USACE Dam and Levee Safety Program, Asset Management Program and Major Rehabilitation Program. During his career with the USACE, Mr Patev has worked primarily on the development of state-of-the-art methodologies for risk and reliability assessments of USACE Civil Works Infrastructure. He has also developed USACE guidance documents and software to support state-of-the practice in Event Tree Analysis, Fault Tree Analysis, Bayesian Weibull Analysis, Expert-Opinion Elicitations, Uncertainty Analysis and Human

Reliability Analysis. Mr Patev also served as the USACE technical lead for the Operational Risk and Reliability Assessments for the Hurricane Katrina Interagency Performance Evaluation Team (IPET). He has also has worked on many international infrastructure projects, including risk and reliability assessments for Autoridad del Canal de Panama.

Romanas Ascila has worked in hydropower development and dam engineering in Sweden and several overseas locations since 2000. After his graduation, he worked for 10 years as a consultant and the head of department where he has been involved in many aspects of hydropower planning and dam construction projects. His major activities consisted of hydraulic design of spillways, dam safety evaluations, risk assessments for embankment and concrete dams, design of dams and spillways, hydrological and hydraulic modelling, power calculations, optimisation and GIS-analysis. Mr Ascila was deeply engaged in the development of the Swedish National Program for coordinated emergency preparedness planning where he was responsible for the hydraulic modelling, dam failure simulations, and inundation mapping. He was a member of several domestic and international research projects with responsibility of dam-break studies, development of the flood mapping methods, and computational aspects. For the last six years he has been working as a dam engineering specialist and systems engineering manager at Vattenfall, the biggest Swedish hydropower utility. Mr Ascila is responsible for safety management at several high hazard dams and the development of the reliability program of the spillway function for the whole Vattenfall's dam portfolio. He is also responsible for the development of the Master Plan for the Lake Vänern and Göta River valley where the dam safety and river basin sustainability goals must be addressed in the context of the changing climate and rapid social growth in the area. Mr Ascila has a particular interest in systems engineering, systems dynamics, CFD, numerical modelling, and, especially, simulation.

Karl Rytters is a consultant for hydropower development, dam safety, water resources, hydrology and hydraulic engineering. Since the early 1970s he has performed feasibility studies, design or implementation in more than 25 countries of schemes up to 3600 MW capacity and 800 m in head, with dam heights up to 170 m, spillways up to 50 000 m³/s capacity with a special interest in hydraulic structures and sediment engineering. Mr Rytters has performed research and development for dam safety and numerous dam safety assessments of existing dams nationally and internationally including peer reviews and panel work. He has been responsible for layout design of waterways, including main spillways of 5800 m³/s at 90 m head, fuse plug spillway 3500 m³/s, bottom outlet 275 m³/s at 60 m head, emergency spillways for 4500 m³/s, desilting facilities and surge chambers for 480 MW. He has been responsible for hydrological studies in more than 10 countries, including flood, sediment and river hydraulics studies.

Foreword

This book arose out of a concern to better understand the reliability of discharge facilities at dams, particularly spillway systems which are so critical to dam safety. The authors brought a range of perspectives, training and experience to their task. The resulting book represents a landmark in the evolution of risk assessment for dams by providing a platform for wider adoption of a systems-based approach to the analysis of risks. The approaches described in this book could represent a step-change improvement for dam safety risk analysis, allowing owners and operators to better recognise and understand the risks posed by the complex interaction of natural and man-made systems.

The authors' thesis is that the unwanted consequences of dam operations are generally the result of unusual combinations of usual events rather than of extreme events, which are the focus of traditional design methods. Examples of actual incidents at dams and other complex facilities are cited in support of that view.

Through the two decades up to the mid-1970s a series of alarming dam failures and incidents, such as with Vega de Tera Dam (Spain), Malpasset Dam (France), Vajont Dam (Italy), Baldwin Hills, Lower Van Norman, and Buffalo Creek Dams, along with the newly constructed Teton Dam (all in the United States) caused growing concern. The result was a renewed focus on dam safety, beginning around the late 1970s with systematic inspection programs in a number of countries to assess the safety of existing dams.

Through the early 1980s it became evident that many dams were in need of improvement, especially in their capacity to safely pass floods. Among other influences, the high cost of retrofitting dams, along with increasing demands by lay managers for justification of large capital expenditures with no new productive use of water, resulted in growing dissatisfaction with the initial three class categorisation of dam failure consequences as the main determinant of a need for safety improvement. The search for a more compelling justification motivated a number of countries to explore the benefits of risk analysis, long practiced in other hazardous industries.

Initially dam engineers struggled to adapt the techniques of risk analysis to dam safety. Criteria for the tolerability of public safety risks, a main driver for improvement, were a particular challenge. Over time and with experience the needed elements came together and the risk-based approach gained acceptance. In June 1997 the first international meeting on risk assessment for dams was held in Trondheim, Norway in conjunction with the HYDROPOWER 97 conference. The International Commission on Large Dams (ICOLD) published *Risk Assessment in Dam Safety Management A Reconnaissance of Benefits, Methods and Current Applications* in 2005. In New South Wales, Australia, the regulator of dam safety developed a risk-based *Risk Management Policy Framework for Dam Safety*, which was endorsed by the state Government in August 2006, establishing a tolerability framework for public safety risks as a basis for determination of safety levels for dams.

In retrospect we see that a risk-based approach has considerably deepened the understanding of dam safety. For example, the need for comprehensive hazard analysis extended the focus beyond flood capacity, prompting research into failure modes less amenable to analysis, such as internal erosion and piping. Human factors and automated controls became better recognised as hazards. Also the need to account for the total sample space in comparing risks with tolerability criteria revealed that the major risks posed by dams do not arise from the extreme events traditionally used for design but from more moderate events. Many other insights became evident.

Despite much progress, difficulties remain. Though human factors have been recognised as a significant hazard for well over a decade, they are still not usually integrated into dam safety risk analyses. The same observation can be made for

monitoring and data transmission systems. The complex interactions between the various influencing factors have generally not been modelled. Whilst uncertainty is the very essence of risk-based approaches, its analysis has largely been confined to sensitivity testing of key input parameters.

In this book on the reliability of flow-control systems, the authors have provided a means for overcoming these problems.

The flood discharge reliability of gated spillways in current risk analyses has mainly been assessed as the probability of gates operating as intended on demand. The authors demonstrate that the problem is more complex. They have concluded that the risk analysis techniques currently available are not up to the task of properly identifying and estimating the risks of discharge facilities. This realisation is not a repudiation of the risk-based approach but points to the need to extend its techniques.

The recognition by the authors that combinations of events are critically important sources of incidents and failures means that interactions must be captured in analyses. Moreover the need to model time effects is well demonstrated in the book. The authors propose that the way to incorporate these aspects is by taking a systems-based approach as developed in other fields such as nuclear power, aviation and space exploration. Thus the authors propose extending the current approach to analysis by estimating the need for discharge, and then analysing the reliability of the release function, of the conveyance function and of the energy dissipation function, with operation of other dams on the watershed, with external disturbances, with human factors and with data acquisition and control systems all possibly affecting reliability. Once the system has been defined and the influences on performance are identified, simulation using techniques such as Monte Carlo analysis can reveal the risks and the uncertainties.

The authors acknowledge that the book points the way forward and is a platform for further development, rather than a treatise on established practice. Systems-based analysis is not yet widely applied for dams and no doubt much remains to be learned. Arguably dam safety analysts have reached the threshold of systems-based analysis through the practice of risk analysis over recent decades. When we look back it is evident analysts were initially ill-equipped to embark on risk analysis for dams but those involved have progressively learned by experience. It is reasonable to expect a similar outcome with systems-based analysis.

Owners and operators need to properly understand the risks posed by dams and related facilities. As the authors have observed, that task is becoming progressively more difficult with more complex organisation structures, greater reliance on automated data capture and control, aging dams and ever-changing understanding of natural events. Much is at stake, including people's lives and property, the owner's business viability and its corporate reputation. In the contemporary context, a well-educated populace is increasingly likely to call to account those who cause harm through an insufficient level of care. Owners need to do what can reasonably be done to minimise risks and can ill afford to miss risks. Simulations of the Lower Mattagami Project and of the Göta River System are presented in the book to show how systems-based analysis can identify risks of both mal-operation and failure and is able to reveal risks which would not otherwise have been recognized. A systems-based approach seems to us to be a defensible way of meeting the public and corporate duties of owners.

The book is well written and clear. In making the case for a systems-based approach real examples are drawn on wherever possible. A large number of relevant and useful sources have been cited, including many which set out the understanding of systems-based analysis as developed in other industries. Whilst the focus of the work remained

the reliability of discharge facilities, it is our belief that the concepts set out in the book could have application in other facets of dam safety in greater or lesser degree.

We strongly recommend the book to dam owners, their professional advisers, safety regulators and other interested parties.

*Leonard McDonald
Past Chairman
NSW Dams Safety Committee
Australia*

*Kaare Høeg
Past President of ICOLD
Norway*

September 2016

Preface

The emphasis on spillway gate reliability improvements that followed the Folsom Dam gate failures led to increasing use of fault tree analysis (FTA) in the safety assessment and remediation of spillway gate systems. A quantitative statement of the probability of gate failure was one of the useful features of these fault tree analyses. Discussions between Mr Urban Norstedt, the former Dam Safety Controller at Vattenfall AB and Dr Desmond Hartford of BC Hydro which centred on how best to maximise the benefit and value of these fault tree analyses, raised two additional questions as follows:

What is the probability of demand for the spillway gates to be brought into service?

What is the probability of operational failure of the spillway?

Elforsk – Swedish Electrical Utilities R&D Company – commissioned a feasibility study (pre-study) aimed at identifying a means of addressing the above questions. Two issues became immediately obvious during the feasibility study:

The probability of demand for the spillway to be brought into service is higher than the probability of flood events requiring discharge, and,

The probability of operational failure of the spillway is dependent on a great deal more than flood discharge.

The feasibility study was carried out in the context of the gearing up by the dam owning industries to address the technical and financial challenges of their aging portfolios of dams and changing operational conditions. These changes are occurring both in upstream and downstream development, increasing expectations for safety and cost efficiencies and ever more stringent global environmental performance.

This feasibility study was timely as the dams industry was beginning to focus on the fact that a major fraction of large modern dams – especially hydropower dams – were constructed in the middle decades of the 20th Century. These are now aging with many of the key functional components reaching the end of their operational life. Many have suffered deferred maintenance, and many require remedial attention even if their maintenance has been adequate. This deferred maintenance is especially true of spillways, conduits, and other flow-control systems. At the same time, there have been gradual – and on occasions, not so gradual – changes in hydrology, land use, and other environmental conditions. These changes are felt most strongly on the same spillways and flow-control systems. Many dam owners face dramatically higher costs of maintaining discharge functionality with attendant impacts on the safety of their dams.

Dam owners must prioritise spillway system repair and upgrading in view of the large costs involved. Some analytical means is needed through which the most critical dams and system components in a portfolio can be identified, and cost-effective plans can be developed for their remediation. For the most part, however, such analytical tools are not available. This situation is unsurprising even given the maturity of water resource engineering. Other safety-driven industries such as chemical processing, aerospace engineering, and even other sectors of electrical power generation, face a similar situation: traditional engineering analysis tools have evolved in response to design needs, not operational needs. Traditional engineering analysis tools focus on the capacity necessary to meet specified demands and on compliance with codes or regulations. They mostly ignore operational and systems effects, including the interplay of human operators, modern sensor and control systems, and randomness.

The approach to the analysis and understanding of operational safety of dams and reservoirs developed in this volume starts from the observation that the dominant risks to be managed in dam safety derive not from unique events but from adverse combinations of more usual events. One might think of these as *unusual combinations of usual conditions*. The timing of such events and their magnitudes can create conditions to which the dam had not been designed and which were not accounted for in preparing

operational plans and strategies. These include the systems interactions among management policy, procedural factors, instrumentation and SCADA systems, operational and maintenance practices, design flaws, construction compromises, deterioration, outside disturbances, and many other things that are often overlooked at the time of design. The result is that many systems failures do not fit within a traditional engineering-analytic framework and a new systems framework is needed.

How does the present approach differ from and complement earlier approaches to reliability and dam safety? Fundamentally this approach goes beyond the traditional approach which considers ultimate structural and ultimate hydraulic capacities treated separately, to one that considers all ways that the dam can fail in its containment and conveyance functions, including those conditions where structural and/or hydraulic capacity can be exceeded. Traditionally, for example, analysing spillway capacity and flow control has meant sizing spillways for design conditions: What is the reservoir inflow that a spillway must accommodate; can gates and chutes withstand the pressures and flow velocities to which they will be exposed; can the kinetic energy of flows be dissipated before re-entering the downstream channel? In conventional practice, answering these questions has focused on independent and unique loads: What is the largest flow to be accommodated, what is the worst ground shaking an earthquake might impose, or what is the largest debris or ice load that might accumulate on a gate structure? Even contemporary risk analysis approaches, such as failure modes and effects analysis and probabilistic risk assessment, are of the same character. They concentrate on pre-determined chains of events leading to an accident or failure, and are usually just probabilistic interpretations of existing practice.

This approach is reflected in ICOLD Bulletin 61, *Dam Design Criteria* (ICOLD 1988), which says that,

[The] engineer attempts to create a structural form which together with the foundation and environment will, (i) perform satisfactorily its function without appreciable deterioration during the conditions expected normally to occur in the life of the structure, and (ii) will not fail catastrophically during the most unlikely but possible conditions which may be imposed.

The first condition pertains to operation and maintenance, not safety. Only the second condition considers risk and uncertainty of failure. However, failures or significantly adverse performances do occur in other than extreme conditions. The traditional approach is not necessarily wrong; it just focuses on things other than the systems behaviour and how most incidents and failures actually occur. The evolving notion of risk analysis, and the thinking about how risks arise, motivates a new perspective.

In this volume, we make a clear distinction between *practicable* in the sense of physically feasible and *practical* in the sense of achievable under given circumstances. The term *practicable* is an adjective meaning, feasible, 'can be done'. The term *practical* is also an adjective but it pertains more to implementation (doing) than to the feasibility of an idea.

An approach may be *practicable*, but under certain circumstances may not be *practical*. For example, an approach that is *practicable* for, and has been implemented by, a large dam owner may not be a *practical* option for a small dam owner. In this regard, the term *practicable* does not have limitations associated with capacity and capability whereas the term *practical* does. This limitation is important as it applies to both organisations and to personnel, with the result that what is eminently *practical* to one organisation or individual may not be *practical* to another.

The 'new approach' we outline in this volume may not strike the journeyman engineer as immediately *practical*, just as computational fluid dynamics or critical path scheduling did not strike him or her as immediately *practical* in the last generation. But both of those methods are today valued and routinely applied in practice, and we

anticipate that the ‘new approach’ laid out here, and the extensions by others that grow out of it, will enjoy a similar fate.

The book is organised in four sections. The first section lays out the problem and provides an overview of the proposed analytical approach using stochastic simulation of dam and reservoir operations. It explains why a need exists, and outlines a solution for *next-generation risk analysis*. The second section addresses the inputs to and constraints on reservoir operations. It considers hydrologic inflows, downstream outflow requirements, and external disturbances that may affect operations. The third section examines the engineered components of flow control. It considers spillways, SCADA and control, outflow conveyance and energy dissipation, and the importance of humans in the loop. The last section lays out a future analytical approach based on stochastic simulation of operations. It introduces the concept of a next-generation of safety analysis tools for dam safety based on understanding of operational factors.

This next-generation of safety analysis is not a replacement for our existing probabilistic tools predicated on failure-modes analysis, event and fault-tree models, and the characterisation of unique events. Those tools have proven themselves to be important and valuable, and have profoundly changed the practice of management of the safety of dams over the past two decades. These advancements are reviewed in many guidance documents, for example in ICOLD *Bulletin 130, Risk Assessment in Dam Safety Management*; in the more recent (US) *Federal Guidelines for Dam Safety Risk Management*, or in the predecessor volume to this one, *Risk and Uncertainty in Dam Safety* (ICOLD 2005; FEMA 2015; Hartford & Baecher 2004). The causes of many dam and reservoir failures in recent history can be traced to floods, earthquakes, or internal erosion in earth embankments. These are important failure modes.

The next-generation risk analysis tools for dam safety proposed in the present volume address operational risk. While unique events are important considerations in dam safety, it is also an empirical fact that a large number of accidents and failures – possibly even most – do not arise from such events but from routine operations. Even those accidents and failures that might be attributed to unique loads often might have been avoided were it not for operational factors: a sensor system reported a misleading measurement, an operator overlooked an important precursor, or a spillway gate was unavailable due to routine maintenance. Our existing Probabilistic Risk Analysis tools are valuable but they provide little or no help to the dam safety engineer trying to understand operational failures.

The original motivation for the five years of research leading to the current volume arose from a simple but revealing observation. The simple expression for the probability of failure in dam safety risk analysis is usually expressed as a product of the marginal probability of a demand on the system and the conditional probability of system response given the demand: $P(\text{failure}) = P(\text{demand})P(\text{failure} | \text{demand})$. The *demand*, for example, might be a reservoir elevation (pool level) caused by flooding.

What is this $P(\text{demand})$? Is it a static probability that can be associated with an external natural process like floods or earthquakes? Yes, in some cases it is. But more often, the probability of demand is generated dynamically by the functioning of the system itself. The pool level (and thus, load) on a spillway gate depends dynamically on how the dam and reservoir as a system has been operated up to that time, and on how the dam and reservoir as a system responds. Time is essential, as is the possibly complex interaction of many operational factors. The critical chains of events leading to an accident or failure may have an emergent character, meaning that they are not obvious or easily identified *a priori* but arise from the interactions of the system itself. An analyst creating an event tree would likely never conceive of them, and if he or she did, the important element of time might be impossible to account for.

$P(\text{demand})$ is dynamic not static. In this regard, safety is not a function of a static comparison of demand and response, but a function of system controls. This led to the

realisation that new analytical tools were needed for us to understand operating risk in hydropower and dam safety, and thus the present volume.

The authors.

References

- FEMA (2015) *Federal Guidelines for Dam Safety Risk Management*. Washington DC: Federal Emergency Management Agency.
- Hartford DND and Baecher GB (2004) *Risk and uncertainty in dam safety*. London: Thomas Telford.
- ICOLD (1988) *Dam Design Criteria: The Philosophy of their Selection*. Paris: International Commission on Large Dams.
- ICOLD (2005) *Risk Assessment in Dam Safety Management*. Paris: International Commission on Large Dams.