Spillway gate drive systems: how safe is safe?

Ken Grubb
Brent Imisson
Paul Jones
David Cave

Introduction
There is a great deal of interest currently in the probabilistic analysis of gated systems. This subject is crucial to the safe development of the spillway operating machinery but often takes civil engineers outside of their traditional comfort zone, as it requires a detailed knowledge of drive systems, their componentry and relative failure rates. It is recognised that some scepticism has been displayed by some engineers as to whether analysis leads to the illusion of accurate risk predictions due to the unavailability of valid statistics.

Where are we today in terms of best practice? And, what is the direction of travel? Can any driven gate be of adequate reliability? This paper reviews the philosophical thinking behind specifying dam protection gates and their related systems from a historical perspective. It also considers whether a "one size fits all" approach to dam protection gates can be applied to diverse geographic and technologically diverse societies.

The paper reviews typical spillway gate mechanical and hydraulic drive systems together with their associated control systems. It discusses their features in terms of their contribution towards overall reliability. In so doing, it examines what makes gate drives systems more or less reliable.
The paper also proposes a way forward in terms of the procurement of new and maintenance of existing equipment.

1. Background
Most engineers agree that one of the most significant risks to a dam arises if it is unable to pass a flood-flow that it is presented with. Where a dam includes a fixed level spillway, then security is only reliant upon the flood-flow being less than that for which the spillway was designed. However, many dams cannot incorporate a fixed spillway of sufficient dimensions and therefore incorporate spillway gates. The safety of the dam is then dependent on the adequate capacity of the gates and their reliability together with that of their associated machinery.

According to recently published papers, the hydro-world's safety record in terms of fatalities, does not compare well with other industries that clearly involve great risk such as the nuclear industry and aviation Leyland[1]. For instance, Leyland states that the hydro industry has a deaths/TW.h value of 1.4 compared with 0.04 deaths/TWh for nuclear and 60 for coal.

In a recent report on dam safety by the UK's Environment Agency[2] it was stated:

If asked to cite failures of British Dams, most engineers in the reservoirs industry would be able to quote Dale Dyke, Bilberry, together with recent serious incidents such as Ulley, but many would struggle to name more of the several hundred (near miss) *incidents that have occurred".*

This situation is potentially repeated throughout the world and leaves the uncomfortable feeling that the full nature of the risks associated with dams and reservoirs are not properly quantified and thus not understood.

As stated above, there is a recognition that the reliability of dam protection gates is crucial to the safety of the dam itself. There are also several incidents where the inadvertent operation of spillway gates has also led to fatalities, generally the drowning of members of the public who were accessing the associated river. This brings home the need to recognise that the subject of safety in relation to protection gates is not simplistic and requires careful, documented, thought.

Sadly, the evidence of history is that it often takes a major disaster causing loss of life for step changes in safety practice to take place, driven through legislation. Arguably these changes may be driven by insurance requirements in the modern world as, these days, people are more litigious and courts are less likely to attribute failure to "acts of god".

- It can also be argued that risk-based criteria have become the modern norm due to:
- Developments in statistical analysis which has led to greater understanding of the science
- Developments in computerisation which make the analysis of data relatively simple
- The availability of bigger data sets

2. Evolutionary History of Dam Safety

Dubler and Grigg[3] note that the use of spillways predates recorded history. They state that, historically, various empirical methods were used to estimate capacity.

It is interesting to note that the approach to risk and reliability in engineering has changed a lot over the last hundred years. It provides some useful background understanding to review this evolution. In the United Kingdom there are 14 recorded dam failures leading to 427 deaths, up to 1925 (Source: "Delivering benefits through evidence", Environment Agency[4]). Following which legislation was introduced in the form of the Reservoirs Act (Safety Provisions) Act of 1930. This has been replaced by the Reservoirs Act of 1975 and further initiatives were introduced in terms of responsibilities for enforcement in the form of the Flood and Water Management Act 2010.

The above legislation in the UK is intended to be firmly rooted in relation to risk, with more action being required the higher the perceived risk of the installation. There is also a requirement to report any incident which results, or could result, in the uncontrolled release of water from a large raised reservoir.

Elsewhere it is found that major safety initiatives tend to be driven by failure events in earlier years. Nowadays it could be argued that the stricter liabilities associated with asset owners and their insurance obligations are generally driving risk downwards.

In parallel with the specifics of the dam industry there has been the continual development of obligations under health and safety. Internationally, health and safety legislation requires that an engineer has a duty to consider the risks associated with his design in respect of safety. They are required to identify the hazards and carry out a risk analysis of the control system and the equipment

under its control for all reasonably foreseeable circumstances, including fault conditions and misuse, and:

- Avoid those risks that can be avoided
- Reduce those that cannot avoided so that they are as low as reasonably practicable (ALARP)
- Protect personnel and manage those remaining risks
- Record the results of their risk assessment so that all parties are aware of the residual risks that they own.

Potentially, fatalities arising from a failure to consider reliability needs and ensuring that they were satisfied, could leave a designer open to prosecution involving corporate manslaughter.
In terms of general machinery there have been a number of standards introduced that take a risk based look at machinery and/or their control systems. These include Harmonised European Standards and also ISO standards. Examples include:

- BS EN IS0 13849: Safety of Machinery – Safety Related parts of control systems
- BS EN 62061: Safety of Machinery: Functional safety of electrical, electronic and programmable electronic control systems.

The standards quoted above take a risk-based approach to their subject and have been harmonised in respect of the Machinery Directives enacted into UK law via the Supply of Machinery (Safety) Regulations.

Note that some of the above standards use the concept of a Safety Integrity Level (SIL). There are four such levels with SIL 1 being the lowest (probability of dangerous failure on demand $>=10^{-2}$ to $< 10^{-1}$) and SIL 4 being the highest (probability of dangerous failure on demand $>=10^{-5}$ to $< 10^{-4}$). BS EN ISO 13849 adopts a Performance Level (PL), though it is possible to cross-refer these criteria.

In the case of machinery used to protect a dam, reliability will usually be defined as “the Probability of Failure upon Demand”, rather than a rate of failure per 1,000 hours (say).

Note that whilst most general engineering assessments using the above codes tend to focus on the safety of the machinery in respect of the user. A machine that fails to perform its job regularly but shuts down safely will often be considered to be acceptable. This approach does not work for dam protection and it should be recognised that the codes include societal risk sections which can be used for dam protection machinery.

Overall, society has started from a position where individual engineers used their judgement, then moved to codified prescriptions and finally arrived at a position where design decisions are generally made on a documented, risk-based, approach. Given the ever changing nature of the world in which we live, this also leads to the conclusion that reliability is a journey and not a destination. A risk assessment therefore needs to be revisited on a regular basis.

One final point to make in terms of risk-based reliability assessment comes from the investigation into the Piper Alpha drilling rig disaster. The final report on the investigation into the causes of the loss of life through fire concluded that whilst a risk-based assessment had been completed on the rig’s systems, this had become an increasingly prescriptive task using paperwork based on previous studies. It was recommended that there should always be an original analysis for each rig with expert input.

2.1 Historic Civil Engineering Approach

There are a number of documented dam breaches which have led to loss of life. The civil engineering profession has a generally good story to tell in terms of the evolution of civils based analysis, construction methods and materials. It also has a proud history of cooperation through ICOLD. ICOLD was formed in 1928 and consists of around 90 member national committees which cooperate on learning from experience and sharing best practice.

In terms of legislation, the UK is not alone in introducing an obligation on reservoir owners to keep their assets in good repair and safe order. There is a recognition of the existence of small and large dams and reservoirs (a large reservoir is >25,000m³). Essentially there is then a requirement to appoint:

- An Inspecting Engineer to inspect the dam/reservoir "from time to time".
- A Supervising Engineer "At all times when the dam/reservoir is not under the supervision of a construction engineer" to advise the owner on its behaviour.

The modern civil engineering approach to sizing spillway capacity has been to equate the spillway flood discharge capacity (SFD) to the probable maximum flood (PMF) for significant dams. This has a number of advantages and disadvantages. As has been observed, this rating of the spillway is effectively a zero risk approach, provided the PMF is properly calculated and does not necessarily lead to the best allocation of public funds.

Historically there was then applied an "N+1" rule, where the number of discharge gates installed was one greater than that apparently needed. The legacy effect of the above is that:

- The larger the number of gates the smaller the level of spare capacity
- There is an inherent assumption that the gates will operate when called upon to do so, whereas the larger the number of gates, the more likely that one will fail to operate.

The above approach leads to a position where their safety in the face of extreme events is assumed, but may, or may not be delivered should the extreme event arrive. In addition, climate change has meant that there has been a general inflation in the estimated PMF over recent decades, which often means that spare capacity in the spillway gates does not exist. Hence the N+1 "rule" needs to be treated with much caution.

2.2 Traditional Mechanical and Electrical Engineering Approach Within the Hydro Industry

There are a number of international codes for water control gate design, but most stop short of specifying the reliability requirements of spillway flow control systems. Generally, operating machinery and associated control systems are only partially covered in such standards, where they tend to adopt a rules-based approach. For instance, that the capacity of a winch should be 120% of calculated frictional resistances irrespective of the perceived risk.

Traditionally the specifier (consultant) provides a list of functional requirements, but provides no analysis to the designer as to why these requirements were called for. It is very prevalent to find a general statement that the spillway gates "shall be reliable", however this has no definition and hence is unenforceable.

Review of typical contract specifications shows that resilience tends to be equated with redundancy and thus typically a specification requires:

- Duplicated drive motors
- Diesel engine back-up
- Ultimate manual means of operation

The above has been described as the "shopping list" approach, with the assumption that if such features are present, then the system must have resilience. The emphasis has been placed on "good engineering design" and demonstration of performance through factory and site testing. Due to commercial price pressure, there is a very large difference in the delivered product, from contractor to contractor. In fairness to the contractor/designer, they have no knowledge of the consequences of hazards on the specific site and are not in a position to know if the delivery of the specified equipment will, or will not, provide an appropriate design.

Within the UK, this reliance on testing as a means of establishing operational reliability is also established with an annual demonstration of machinery function to an inspecting engineer. Such demonstrations are valuable, but do not establish reliability as defined within this paper.

Upon detailed examination, it is often found that machinery incorporates common cause failures, so that the appearance of redundancy becomes an illusion. Also designers rely upon levels of maintenance which are unrealistic in some parts of the world, so that systems which are initially "safe", become not so as time marches on.
If further evidence is needed that there is a need to review custom and practice in terms of dam protection gate machinery, it should be noted that:

- There have been a number of dam failures where a failure of the spillway to work as intended was a contributory cause.
- There are numerous gate failures which have been classified as near misses around the world
- Reliability studies on protection gate systems regularly expose design, component, operational and maintenance weaknesses.

2.3 The Modern Hydro Industry Response
It is satisfying to record that much good work has been undertaken in the dam industry to adopt risk-based reliability techniques. The civil engineers in the fraternity have been using risk-based analysis for many years.

Early papers on machinery reliability were published by Lewin and Ballard[5] and are still valid when read today. Lewin, Ballard and Bowles[6] have also published excellent background papers on risk management.

ANCOLD embraced a unified approach to risk assessment in a "guidelines" document published in 2003 and there is a good overview of this in a paper by Barker[7].

Currently organisations such as BC Hydro in Canada, Scottish and Southern Energy in Scotland and many others have been embracing risk-based approached to protection gates. The work of Rick Schultz in the USA is excellent and further information on this can be gleaned from his papers.

Currently in ICOLD a Hydromechanical Committee has been established and it is working on a guideline document in respect of the safety of dam protection gates. Whilst it is not for this paper to predict what will become eventual ICOLD policy, it can be expected that a risk based approach will feature prominently.

3. The Lexicon of Risk and Reliability

3.1 Hazard Identification and Risk Analysis

Hazard Identification and Risk Analysis is a collective term that encompasses all activities involved in identifying hazards and evaluating risk at facilities, throughout their life cycle, to ensure that risks to employees, the public, and the environment are controlled to acceptable levels. These studies typically address three main risk questions:

- Hazard – What can go wrong?
- Consequences – How bad could it be?
- Likelihood – How often might it happen?

The hazard identification and analysis stage is a very important part of the risk management process, as no action can be made to avoid, or reduce, the effects of hazards that have not been identified. The hazard analysis stage also has the largest potential for error with little or no feedback of those errors.

When evaluating the risks arising from dangerous failures in the installation, it is important to consider both the risk to the individual and societal risk.

Individual risk is defined as the frequency at which an individual may be expected to sustain a specified level of harm from the realisation of specified hazards.

Societal risk is defined as the relationship between frequency and the number of people sustaining a specified level of harm in a given population from the realisation of specified hazards.

When considering what would be deemed an acceptable level of risk (the target risk) it is useful to know some typical background risks for people in the vicinity of the installation.

Some background risks for citizens in the UK (published by the Health and Safety Executive[8]) are shown in the table below:

Cause of death	Annual risk
Cancer	2.6×10^{-3} (1 in 387)
Injury and Poisoning	3.2×10^{-4} (1 in 3137)
All types of accidents	2.5×10^{-4} (1 in 4064)
Road accidents	6.0×10^{-5} (1 in 16,800)
Gas incident (inc. poisoning)	6.6×10^{-7} (1 in 1,510,000)
Lightning	5.3×10^{-8} (1 in 18,700,000)

The difference between the target risk and the risk arising from dangerous failures in the installation gives us the risk reduction required.

One way to achieve part, if not all, of the risk reduction is to incorporate safety related systems that meet a particular safety integrity level.

Safety Integrity is the probability of the safety-related system performing the specified safety functions under all stated conditions within a stated period of time.

Even when the target risk is achieved, legislation in the UK requires that all risks are reduced to a level that is as low as is reasonably practicable (abbreviated as ALARP). To carry out a duty so far as is reasonably practicable means that the degree of risk in a particular activity or environment can be balanced against the time, trouble, cost and physical difficulty of taking measures to avoid the risk.

In spillway gate installations reliable operation of the gates is often crucial to the overall safety of the installation and would form part of the safety function.

3.2 Reliability

Most people will have some concept of what reliability is from everyday life, for example, people may discuss how reliable their car has been over the length of time they have owned it.

Reliability therefore can be expressed as quality over time. If you purchase a new car and it breaks down on the way home from the dealer you would consider the car to be of poor quality. If, however, various parts of the car wear out before you would expect them to this would be termed poor reliability.

Reliability is associated with unexpected failures and understanding why these failures occur is key to improving reliability.

4. The Effect of Legal Systems in Driving Risk Management

In his paper on tolerable risk for dams, Bowles compares and contrasts the two leading legal systems, namely Napoleonic Civil Code and Common Law in terms of their effect on the obligations of a designer. The differences are far reaching and it is worth highlighting these so that their effects become apparent on an asset owner's obligations.

Many countries including the Netherlands operate under a civil law approach whereby the adherence to a regulatory code will be proof of meeting one's obligations towards liability. In the UK, USA, Australia and other territories, whilst targets are published, there is an obligation to make risks as low as reasonably practicable (ALARP). As Bowles[6] notes:

"The risk criteria adopted in the United Kingdom and the Netherlands look very similar. Both countries have upper limits of 'allowable' individual risk and both use criteria lines in the FN curves. Even their numerical values do not differ a great deal. However, the interpretation differs greatly. Whereas the criteria in the Netherlands are the end of the discussion, in the United Kingdom they are the starting point."

Thus there is an absolute need to assess risk and mitigate it in many countries of the world; as failure to do so will render themselves "naked" in defending themselves against an accusation of not meeting their obligations towards others. As can be seen, only the Courts can ultimately pronounce on whether these obligations have been met.

5. Skills and Data Needed for Risk Assessment
To undertake a good dam protection gate quantative risk assessment it is necessary to incorporate:

- Engineers who understand how machinery and structures are designed
- Engineers who understand how machinery and structures fail
- A clear understanding of the expected loading cycles (patterns of use) of the equipment under review
- A clear understanding of the competence of the asset owner's operating and maintenance organisation and their ability and commitment to maintaining what will be provided to them.
- Valid statistics about the reliability and life cycle of a wide range of components

The above is fairly wide ranging and is often used by some to undermine the benefits of quantative risk assessment. A few comments here may be illuminating.

The composition of the assessment team is very important and this needs a combination of a thorough grounding in the relevant technical disciplines and a good level of experience. After the Piper Alpha drilling rig fire there was an official enquiry which, in part, concluded that risk assessments had become too formulaic and that there was a need to bring original thinking when considering risks. This merely emphasises the point.

Engineers are taught to design things, but not necessarily how things fail. Anecdotally, the authors believe that a good background in asset surveys is extremely helpful in spotting future failure modes.

It is surprising how many statistics are available if you know where to look. Most have the disadvantage that they do not relate to the equipment under consideration, in the environment of the site and managed by the owner for the installation under deliberation. This is a draw-back but does not necessarily invalidate the benefit of statistics. However, it does emphasise the need for experience in the team.

More recently, Rick Schultz from the US Corps of Engineers has collected a range of statistics which apply to their portfolio of dams in the USA. This has also helped to highlight the relative failure rates of certain types of equipment.

6. Machinery Safety versus Machinery Availability
Over recent years there have been a number of risk-based European codes issued, which have been harmonised with ISO. An obvious example includes BS EN ISO 13849 'Functional Safety of Machinery'. These are very useful and a welcome contribution to the family of standards that apply to safety-related machinery in general.

It does need to be borne in mind that the above standards are generally written from the viewpoint of controlling a machine, whose normal fail-safe condition is to fail-stop. Whilst this is generally true from the viewpoint of protecting machine operators from personal injury, it is gate 'availability' that ultimately provides the public safety element for a dam. Hence, in the context of dam protection gates, there is no dam safety without gate availability.

This requires a risk-assessment approach (which is allowed within the codes) to ensure that operators are protected, but that the balance between operator and dam safety can be properly struck. In so doing there are some conundrums that are highlighted below.

7. Some Conundrums from the Risk Based Approach – How Safe is Safe?

7.1 Structural Drive Components

There are a number of mechanical components in a typical drive system, including shafts, hoist drums, etc. Traditionally standards such as FEM are used to calculate the acceptability of the structural capacity of such parts, using criteria relating to usage, average loading, etc. This works well for designing a crane, but the availability imperative is not reflected in the codes.

Logically it should be necessary to apply additional load factors to drive the structural "factor of safety" to a higher level for dam protection equipment. This would be similar in principle to the usual European approach to designing equipment to be used for lifting which has a higher level of proof required as opposed to say a conventional steel structure.

7.2 Drive Gearboxes and Gears

The modern gearbox is a wonder to behold. The evolution of computer analysis, materials science and production techniques have allowed producers to reduce the mass of metal to the point where its performance and life is very predictable. From a dam protection gate point of view, this has not all been a good thing and it is instructive to see that gearboxes sourced many decades ago, seem to have a longer working life than those of today.

Again the use of computational methods to predict performance against a precise FEM requirement does not sit well with the need for long run availability. This can be addressed by applying an additional load factor before selecting the equipment concerned.

Gearboxes often play a special role in hoist drives in that redundant drive motors are used but drive through a single gearbox.

Note that there are now gearboxes available which have been designed to give a high level of integrity and availability. This is achieved by the internal separation of two distinct drive trains within the unit that feed into a single output. This ensures that if one part of a drive fails, the alternative drive remains operational.
This approach can also be applied to open-mesh gears and ultimately to drive-couplings.

7.3 Oil Hydraulic Issues

In terms of oil hydraulic systems, the reliability of these elements of the gate operating equipment is obviously paramount.

Failure of individual components could potentially render the system unavailable, so careful design using redundancy wherever possible is crucial.

Something as simple as a ruptured oil reservoir, with the consequent loss of oil, could be enough to lose operability as could contaminants or water present in the oil itself.

There could potentially be issues with load holding valves that cannot be released – this can be overcome by careful circuit design and consideration of the operation of the equipment under all loading conditions – another important reason for carrying out a through hazard identification process at the start of the project.

Whilst it might seem that all valves are equal, there have been issues with the quality of some equipment and it is important to understand that the key is to ensure that the equipment quality is commensurate with the reliability target. Cylinders again will require careful selection to ensure that they are completely compatible with the duty required and the operating environment. This extends to the material of the rod, any coatings used on the rod and the quality of the sealing systems within the cylinder.

The fitment of quick release couplings directly on the cylinder manifold that enable the connection of a mobile diesel engine-driven Hydraulic Power Unit (HPU) in the event of loss of the main HPU will assist in improving the availability of the gate in question. NB: it is essential that these quick-release couplings are capable of connection and disconnection whilst the system is pressurised.

7.4 Electrical and Control Issues

Traditional "Fail-Safe" Circuits

Care should be taken when specifying and designing "fail safe" devices such as emergency stops, guard interlocks, over-travel switches, slack rope devices etc.

Fail safe devices may be fail-passive, fail-active or fail-operational:

- Fail-passive devices include circuit breakers, fuses etc. and could render the control system inoperable or de-energised until corrective action is taken.
- Fail-active devices tend to keep the system energised but inoperable until corrective action is taken.
- Fail-operational devices allow the system to function safely, even when a device fails.

Machine safety devices are traditionally fail-active and can introduce single point failures to the system. When availability of the machine is key to safety, as with spillway gates, safety circuits need careful design so that they can be both fail-active and fail-operational depending on the failure mode.

Power Supplies

Most gate control systems are reliant on electrical power. Often backup systems are provided to provide redundancy and/or diversity; however, it is difficult to design a system with no commonality and therefore Common Cause Failure problems need to be carefully considered, these can include auto transfer switches, and common distribution systems including bus sections and cabling.

8. What Affects Reliability?

The UK's Health and Safety Executive[9] undertook a study into the primary causes of control system failures. They concluded that the failures were caused in the following lifecycle phase:

- 44% Specification
- 20% Changes after commissioning
- 15% Design and implementation
- 15% Operation and maintenance
- 6% Installation and commissioning

This is interesting and instructive since it implies that (within the confines of this study) more than half of all failures had been built into an installation by the time of commissioning. This fits with anecdotal evidence from surveys of old equipment undertaken by the authors. Many of the long term detrimental issues displayed by equipment can be ascribed to a poor design, material selection, etc. The seeds of good or bad reliability of often there from the start.

Reliability is a journey not a destination but the evidence is that it is not possible to inspect or test out those faults which are already built in. Hence the key is to apply good risk mitigation practice from the very beginning of the project and to continually pass the results of this work on to those that come later in the process.

There have been several papers which have examined the experiences of geographic areas subject to major storms. It has often been found that there is then a high level of loss of primary electrical power from the grid. Where it is necessary to incorporate powered gates, the security of power supplies and their back-up systems becomes essential to the reliability of the machinery.

Systems with manual operating back-up have at least two major draw-backs:

- A normal person is only capable of delivering a relatively small power for an extended period of time (perhaps as low as 150 Watts) and it takes a long time to move large structures.
- If the one in ten-thousand-year flood is happening now, how many people turned up for work today?

Maintenance is too big an issue to be dealt with in this paper, but suffice to say that it is a crucial element to the reliability journey. It is also a potential source of common cause failures, hence the training and management of maintenance personnel is important.

The regular use and testing of equipment improves its statistical reliability. This is an accepted fact and matches with anecdotal experience.

The use of new technologies on reliability critical equipment should be avoided as there will, by definition be little or no experiential data on which to make judgements as to acceptability.

9. Implications for the Future

Ultimately, the points raised within this paper do not change the overall approach and there is still a need for somebody to take overall responsibility for dams. It is anticipated that this would normally reside with the civil engineer assigned to the particular dam.

However, as discussed previously, it is essential that the M&E hazard and reliability study is undertaken at an early stage by suitably qualified specialists and that this then becomes a reference tool for the dam engineer to assess future changes in operation or changes to the environs of the dam (including new habitations downstream of the dam for example).

Moving forward, it is crucial that the hazard and reliability study is therefore to be seen as continuous journey rather than a destination.

9.1 New Equipment Procurement

As has already been seen, the "shopping list" approach to specifications is no longer appropriate. With the increasing demand from society to reduce background risk it is predicted that the risk-centric approach to projects will relentlessly be required. This requires hazard and consequence identification at an early stage and the development and provision of this information needs to be fundamental to any design contract.

Perhaps in the future, there will be more stringent requirements for the risk / reliability issues to be signed off by an appointed person or third party organisation to ensure that they have been adequately considered.

9.2 Existing Equipment

Where existing dam protection equipment machinery is considered, it is necessary to establish the gap between what is owned and what you wished you owned. The requirements for a hazard identification and consequence review are virtually identical to that previously described.

Thereafter it is necessary to establish the reliability levels of the equipment installed and determine if these are adequate or need improvement.

The results of these studies are then held by the asset owner for future periodic review.

10. Final Thoughts and Conclusions

The hazard identification and consequence analysis for the gate and its associated drive system is the fundamental building block at the start of the assessment process.

Following the completion of this analysis, best practice in the design of modern spillway gate drive systems then relies heavily on the use of risk-based design codes to ensure that the appropriate level of equipment reliability has been achieved commensurate with the hazards previously identified.

The risk based approach has the added advantage that it can allow a common process, but still has the flexibility to take into account any specific issues relating to geographic location, existing maintenance regimes and other local/site factors.

References

1Leyland, B. (2014). *Gated spillways, are they safe enough?* British Dam Society Meeting 2014.

2 & 4 Environment Agency. (2011). *Delivering benefits through evidence, lessons learned from historical dam incidents.* Project SC080046/R, August 2011.

3 Dubler, J. & Grigg, N. (1996). *Dam safety policy for spillway design floods?* Journal of Professional Issues in Engineering Education and Practice, October 1996.

5 Lewin, J. & Ballard,G.M. (2004). *Reliability principles for spillway gates and bottom outlets* British Dam Society Biennial Conference Proceedings, Canterbury 2004.

6 Lewin,J., Ballard,G.M., & Bowles, D.S. (2003). *Spillway gate reliability in the context of overall dam failure risk* , USSD Annual Lecture, Charleston, South Carolina, April 2003.

7 Barker, M. (2011). *Australian Risk Approach for Assessment of Dams*. USSD, 2011

8 Health and Safety Executive (UK). (2001). *Reducing Risk, Protecting People*, HSE, 2001.

9 Health and Safety Executive (UK). (2001). *Out of Control*, HSG238, Second edition 2003.

The Authors

Ken Grubb has over 40 years of experience designing, constructing, installing and commissioning water control systems. Ken Grubb was the founder of KGAL Consulting Engineers. He is the former Technical Director of Biwater Hydropower and currently sits on the ICOLD hydro-mechanical committee as the UK's representative. In this forum he is aware of considerable unease at the current reliability of gate drive systems and the steps being taken to improve them. He hopes to use this speaking opportunity to promote this work.

Ken is currently the Hydro-mechanical Expert appointed to assist with rehabilitation works on the Kariba Dam.

Brent Imisson joined KGAL 10 years ago and is currently an Associate Director of the Company. He previously worked in the gate design department of Kvaerner Boving/GE Energy. He has over 30 years' experience of designing and detailing all types of gates for hydropower purposes, together with their associated drive systems.

Brent brings to bear an enormous wealth of experience of designing and implementing gate related installations from both the contractor and consultant view point. He is currently working on the design of the Xayaburi HEPP gates and those for the Hydro addition at Maris Dam in the Philippines.

Paul Jones is an electrical engineer with special expertise in safety related systems. He joined KGAL in 2007 and is currently an Associate Director. He has worked on a number of hydroelectric schemes for KGAL. For the last four years he has been working on spillway gate systems in Scotland developing and project managing safety related upgrades to the hydropower infrastructure owned by Scottish and Southern Energy, following specific reliability studies undertaken by KGAL over the last decade.

Paul brings to bear a great deal of practical experience analysing and implementing safety related improvements to gate machinery.

David Cave joined KGAL in 2014 as a Senior Engineer. He is a trained oil hydraulic specialist with over thirty years' experience. David provides specialist oil hydraulic expertise within KGAL and as such has a controlling involvement in all gates which have a significant hydraulic content.

David is responsible for designing, specifying and implementing the oil hydraulic operating systems on the 1283 MW Xayaburi hydroelectric project.

November 2017