Would bowties and critical controls contribute to the prevention of high consequence / low frequency dam failures?

Learnings from the global mining industry on catastrophic event management

Russell Mills PhD, Principal Risk Consultant
Rebecca Freeman, Senior Risk Consultant
Malcolm Barker, Principal Dams Engineer
GHD Pty Ltd
145 Ann Street, Brisbane, Qld 4000

The global mining industry lives with the risk of catastrophic events such as water storage or tailings dam failures as part of its daily operations, and has developed a number of approaches to enable mine management to understand the nature of the risks and the ways in which they are being managed. One such approach involves the use of bowties for the understanding of the hazards and risks. Building from bowties, the second approach involves the selection and management of controls critical to the prevention or mitigation of the catastrophic event. The Australian mining industry is a world leader in this regard and the purpose of this paper is to illustrate how bowties are constructed, how risks can be semi-quantitatively estimated, how critical controls are selected and managed, and how, if all this is done well, risks can be demonstrated to be as low as reasonably practicable (ALARP).

This paper sets out key themes and presents an example for a tailings dam failure to illustrate the role of bowties and critical controls in management of catastrophic events. It will also highlight the role of bowties in the anticipated introduction of a Safety Case approach to dam risk management. Bowties provide a useful tool for the transfer of risk management knowledge from the designer, to allow dam owner / operators to better understand their risks and to recognise the link between design and operational controls and how they are used to manage those risks to ALARP.

Keywords: bowtie, risk assessment, critical control, tailings dam, dam safety, ALARP, safety case.

Introduction

The retention of water is a normal part of the day to day operations of many mining operations. Water from minerals processing operations such as washing, dewatering, floatation, filtration processes, plant washdown, rainwater collection in processing areas etc is a substantial source of the heavily contaminated water stored in tailings dams. Embankment dams are used for the collection of water from aquifers, surface water runoff or water wetdown of faces and benches etc. Hence the mining industry needs a good understanding of the factors affecting safety in dam design, construction and operation.

There have been a considerable number of incidents involving tailings dam failures, the more severe of which have led to loss of life, environmental damage and community disruption. International Committee on Large Dams (ICOLD) Bulletin 121 (ICOLD, 2001) has collected information on and analysed 221 tailings dam incidents to determine the causes of these incidents. They attributed the reported cases to:

- Lack of control of the water balance
- Lack of control of construction
- Lack of understanding of the features that control safe operations.

Only one or two of the cases involved unpredictable events and other cases were caused by unexpected climatic events including earthquakes.

Serious and very serious failures of tailings dams are regarded as high consequence events (HCEs) with the potential to cause loss of life, community dislocation, environmental impact and substantial clean-up costs in both direct and indirect damages. The most recent tailings dam failure occurred at the Germano Mine, Bento Rodrigues, Brazil (operated by Samarco SA) on November 5th 2015. Figure 1 below illustrates the devastation that can be caused by such a failure, but according to the ICOLD Report incidents are occurring with a frequency of about two per year. This trend is confirmed by inspection of the chronology of tailings dam failures published by the World Information Service on Energy Uranium Project (WISE, 2016). Bowker and Chambers (2015) have analysed a large number of tailings dam failures using historical failure rates and concluded that the risk of serious and very serious failures is increasing.

Image Source: Wall Street Journal

Figure 1: Aftermath of the tailings dam failure at Germano Mine, Bento Rodrigues, Brazil (operated by Samarco SA) on November 5th 2015

The need for any type of large dam to not pose a threat to downstream communities and environments has been recognised in the ANCOLD Guidelines on Risk Assessment (2003). These guidelines provide a common approach to managing dam safety risks using a risk assessment process aligned with ISO31000:2009, the International Standard for Risk Management (Standards Australia, 2009). The mining industry has also adopted ISO31000 and developed a sophisticated understanding of mine operations risk management through three fundamental steps:

1. Hazard identification using bowties
2. Risk assessment using more quantitative techniques as the level of consequence increases
3. Critical controls that meet specific functional requirements matched to the significance of the risks involved, which are monitored and maintained to pre-defined performance standards.

Core to the mining industry approach is the development and use of bowties, which aids the understanding of complex events with the potential for loss of life in mining operations. In this paper each of these steps will be examined for their application to dam safety, based on what has been learned in the global mining industry about catastrophic event management, and with the aim to address one the most fundamental questions about dam safety – when is it safe enough? This will conclude with a discussion about risk mitigation to the point where the residual risks are as low as reasonably practicable (ALARP), and set the scene for a future Safety Case regime in the design, construction and operation of large water storage dams.

Bowties for high consequence events

History

Bowties first appeared in the 1990's in the oil and gas industry and were adopted by operators of major hazard facilities in Australia to demonstrate through Safety Cases that they were operating their facilities safely. The bowtie concept for

Dams, a Lasting Legacy

the visualisation of hazards > events > consequences and some of the pitfalls in their use has been described by Pitblado and Weijand (2014). The Australian mining industry adopted bowties in the early 2000's to describe their mining operational risks in an effort to reduce their fatality rates in mining and processing operations. The most significant users of bowties were the coal, iron ore and aluminium industries. Today bowties are the most widely used method for describing what causes catastrophic loss of life events and what controls are in place to try and prevent the event or mitigate the catastrophic outcome.

Bowtie Architecture

Bowties for high consequence events (HCEs) (Mills, 2016) have an architecture that makes them useful for characterising the dynamics of the chain-of-event progression from causes > top events > outcomes along pathways, noting the controls for prevention and mitigation. The top event is chosen as the failure event leading to the surrounding public safety, environmental and community impacts. They identify the critical controls along the pathways amongst the string of pathway controls. An example of a HCE bowtie is shown in Figure 2 below.
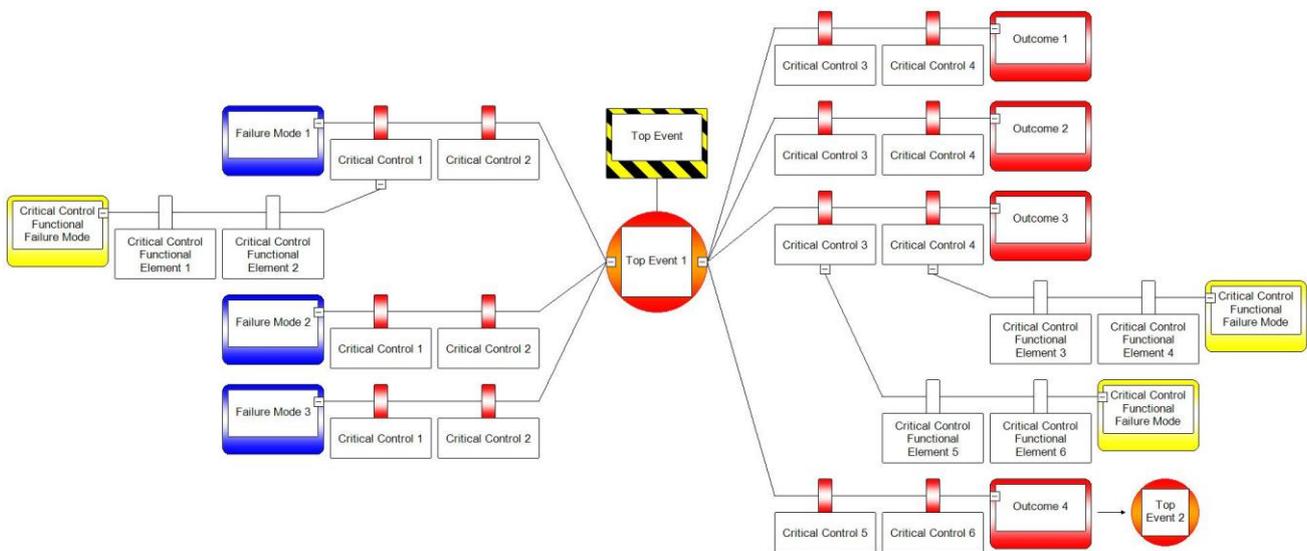

Figure 2: Example of a high consequence event bowtie

The left hand side of the bowtie shows the failure modes for the top event, and the right hand side shows all of the high consequence outcomes of the top event including; safety, environmental, community, financial and reputational impacts of the event on the organisation in which they occur.

Bowtie Critical Controls

The bowties also show the critical controls to preventing such events from occurring, or mitigating their consequences if they do occur, along each of the failure mode pathways. Critical controls are the physical and/or nonphysical means planned to prevent, control, or mitigate undesired events or accidents. (Sklet, 2006). These critical controls are fundamental to risk management, without them the events would likely occur and/or the consequences would be realised most of the time.

Each of the critical controls should be designed to block the event development. The critical controls form the lines of defence and were first described in the literature by James Reason (1995) by the analogy to the cheese slices in the "Swiss Cheese" model of accident causation. The effectiveness of these critical controls is to a large extent determined by the number of "holes" in the Swiss Cheese. A high integrity critical control has smaller and/or no holes, poorer critical controls have larger and/or many holes. What this means, is that the constituent elements of the critical controls, called critical control functional elements, all must combine to produce the desirable performance of the critical control under conditions where there is a demand on the critical control. The critical control functional elements are not random selections; they derive from a taxonomy which classifies them by type as:

- Design –the control is designed to the right standard or specification to meet its functional requirement

- Implementation – the control is implemented sufficiently to meet its functional requirement
- Operation / Maintenance – the control is operable and maintainable to meet its functional requirement
- Competence – the control is managed by people who are trained and competent in its functional requirement
- Monitoring – the control is monitored to verify its actual performance meets the functional requirement

Failure modes for the critical control functional elements are the "holes", they are plugged by the above characteristics being recognised and adhered to. This requires operations management to establish the performance requirements and implement programs to maintain the performance of the critical controls.

Based on examples of the bowties GHD has prepared for mining operations including; a manganese mine in NT Australia, a copper mine in South Africa, and multiple coal mines in Central Queensland and NSW, we have developed a representative bowtie for a high consequence event involving a tailings dam failure as a case study. This type of dam failure is a reasonable candidate to analyse. Since 2010 there have been at least 13 tailings dam failures globally. Three high consequence events have occurred during this period; (1) at Germano Mine, Bento Rodrigues, Brazil (operated by Samarco SA) on November 5th 2015, (2) Mt. Polley Mine, Likely, British Columbia, Canada (operated by Imperial Metals Corporation) on August 4th 2014, and (3) Ajka, Veszprém County, Hungary, operated by MAL Magyar Aluminium) on October 4th 2010. Two of these events resulted in a major loss of life and all three had significant environmental and downstream community impacts (WISE, 2016). The tailings dam failure at Mt Polley has been the subject of an expert panel review (Morgenstern et al, 2015) and has received significant public exposure.

GHD's dams engineers reviewed the existing bowties and identified example failure modes using the ANCOLD Risk Assessment Guidelines (2003) and Tailings Dams Planning, Design, Construction, Operation and Closure Guidelines (2012). The example failure modes anticipated for a tailings dam failure appearing on the bowtie are:

- A failure of the ground support system
- Overtopping
- Piping / internal erosion

They then identified the critical controls for each failure mode and the critical control functional elements. For ease of presentation, the resulting bowtie has been separated into its left hand side (prevention of the top event – a tailings dam failure). This is shown in Figure 3.
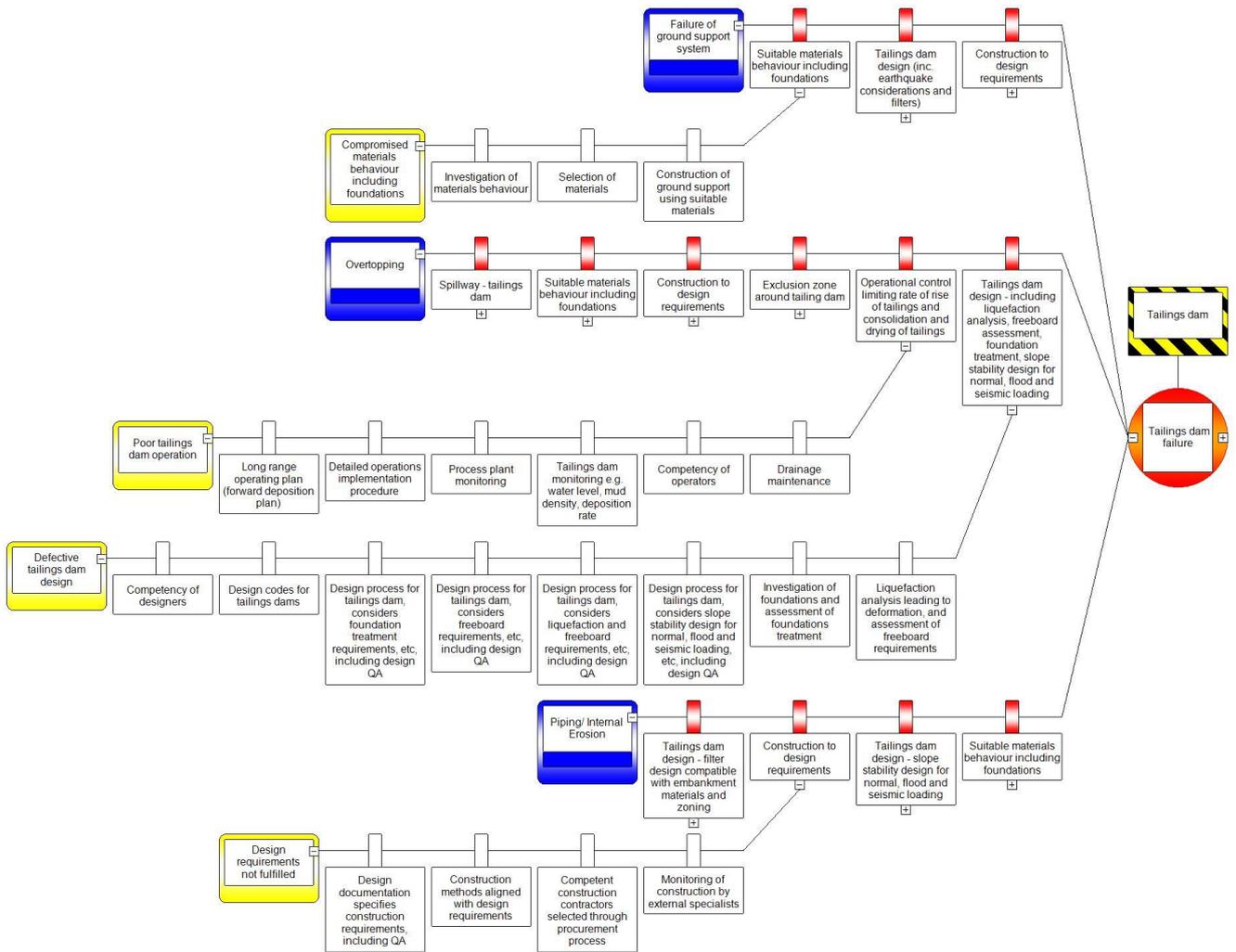
Dams, a Lasting Legacy

Figure 3: Failure modes and critical controls for preventing a tailings dam failure, with examples of critical control functional elements (bowtie left hand side)

The right hand side (mitigation of the outcome after the top event has occurred) is shown in Figure 4.
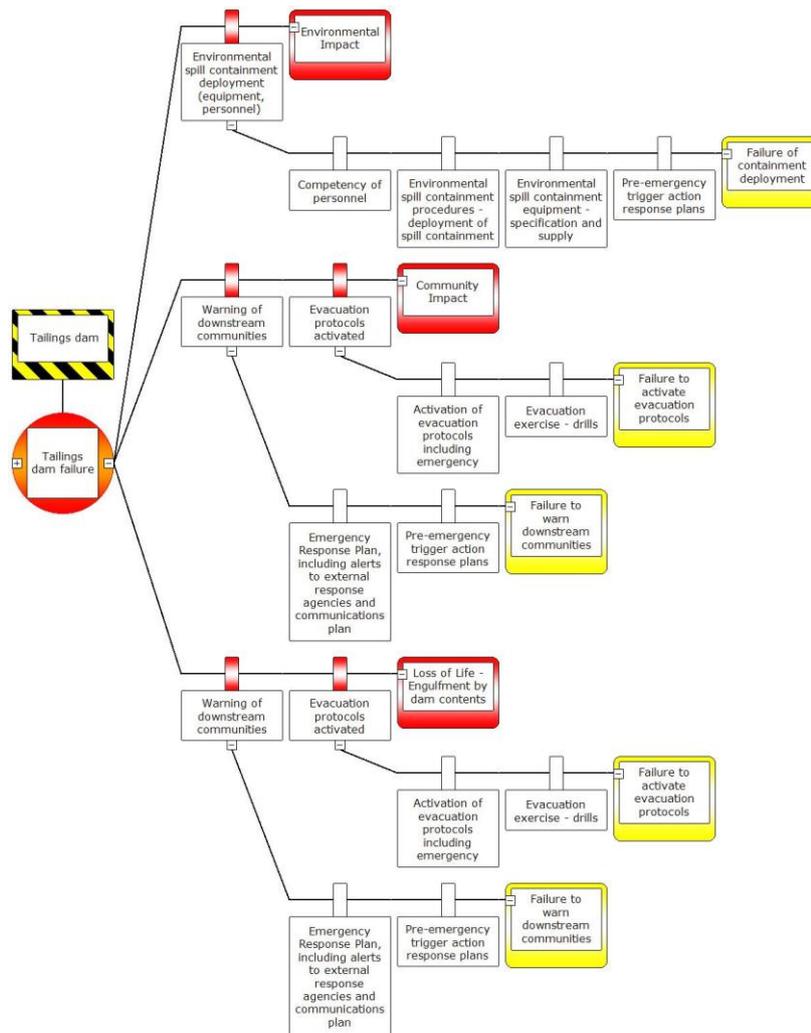
Figure 4: Outcomes and critical controls for mitigating a tailings dam failure, with examples of critical control functional elements (bowtie right hand side)

The critical controls shown in Figure 3 and Figure 4 are the lines of defence to the prevention or mitigation of tailings dams failures. The critical control functional elements are the design, implementation, operation / maintenance, competency and monitoring processes that must be put in place to maintain the performance of these critical controls. Figure 4 illustrates that the critical control functional elements may appear on multiple pathways, Hence, a weakness in any one functional element can have multiplier effects across many failure mode pathways.

For example, an ineffective training and competency program may compromise multiple implementation controls involving procedures, introducing a systemic weakness throughout the implementation of management system procedures. A failure to monitor and verify activities may cause an inability to detect design flaws and implementation weaknesses in the control.

Estimation of Risk

History

Traditional risk assessment options have either been qualitative or quantitative. Qualitative techniques (such as matrix based assessments) are easy to understand and have a higher level of workforce ownership. By comparison, quantitative risk assessments (QRA) utilise failure data and are typically performed by consultants with limited workforce involvement or ownership.

Following the Longford gas explosion in 1998, and the subsequent Royal Commission into the causes (Dawson, 1999), the Victorian Government introduced Major Hazard Facility (MHF) legislation. As part of MHF legislation, facilities handling or storing designated hazardous materials above certain threshold quantities were required to develop and

submit a Safety Case which demonstrates that the risks associated with the facility were understood and managed. Traditionally, Safety Cases utilised QRA techniques to assess the risk, however the new legislation had a strong emphasis on site ownership and assessing the effectiveness of controls compared with other legislative requirements within Australia at the time. This led to the development of an alternate risk assessment technique, semi-quantitative risk assessment (SQRA) which incorporates workforce involvement and provides a semi quantitative measure of risk as an output. This technique has proved useful for mining operations where failure statistics are insufficient for QRA.

The SQRA technique was adopted by a number of mining companies in the early 2000's as a means to provide a more in-depth analysis of the sources of mining risks and also to provide a foundation for selecting the best risk controls, based on a better understanding of the contribution these controls are making to risk reduction. It also provided a metric for monitoring performance improvement or decline. The profile of mining risks is generated within facilitated team workshops to estimate the risk of a fatality (or some other predetermined consequence) from each of the hazards and be able to rank the potential risks relative to each other. The profile enables prioritisation of risks for subsequent assessment and risk management.

The steps involved in the application of SQRA requires the estimation of three factors:

1. Frequency of the top event

    a.   The overall frequency of the top event considers the contribution of each of the failure mode pathways
    b.   Use fault tree analysis (FTA) to estimate the failure frequency for each pathway
    c.   The effect of the critical controls in modifying the failure frequencies is included.

2. Probability of the top event escalating to the consequence outcomes

    a.   Potential for escalation considers the outcome (social, economic, environmental)
    b.   Probability is based on a stepwise approach to escalating the top event, using event tree analysis (ETA)
    c.   The effect of the critical controls in modifying the probability factors associated with each step is included.

3. Consequence analysis for each outcome

    a.   Loss of life onsite / offsite population at risk
    b.   Direct and indirect damage costs
    c.   Environmental and amenity impacts, measured as indirect damage costs.

These factors are combined into the risk equation:

Risk = Top Event Frequency (p.a.) x Probability of Escalation x Consequence Outcomes (outcomes p.a.) – Equation (1)

The mining industry has implemented the use of SQRA as a preferred method of analysis for high consequence events such as single and multiple fatalities. The approach they have taken is to undertake the risk assessment with the involvement of operations personnel and subject matter experts, including designers and external specialists. This team is responsible for the selection of the critical controls based on their knowledge and experience. The benefits observed using this approach include:

•   A high level of workforce involvement and increased understanding and awareness of the risks, and controls that manage those risks
•   The risk profile, using Equation (1) to assess a wide range of mining risks, allows for prioritisation and improved management of valuable implementation resources.

The detailed risk assessments undertaken by GHD involving tailings dam failures cannot be provided due to the confidential nature of this work. However, tailings dam failures are known to be a significant risk to the global mining industry. Bowker and Chambers (2015) have analysed a large number of tailings dam failures using historical failure rates to estimate that in the decade 2010 to 2019 there will be approximately twelve serious failures[1] and eleven very serious failures[2] of tailings dams across the world. They estimated that the average clean-up cost for these catastrophic events would be around US$543M. This is, indeed, a significant risk to the industry, as the size of tailings dams grow, costs are constrained in a globally restrained market, and societies through their government legislatures place increasing burdens on the operators to meet higher performance standards.

---

[1] A serious failure is defined by the authors as having a release of greater than 100,000 cubic metres, and / or loss of life.
[2] A very serious failure is defined by the authors as having a release of at least 1 million cubic metres, and / or a release that travels 20 km or more and / or multiple deaths (generally $\geq$ 20).

Critical Control Performance

There are two aspects to consider when determining the performance of a critical control; (1) the control is an effective means of reducing the risk and (2) the critical control is performing adequately to meet a defined performance standard. Both aspects are important to the overall question of whether the risks are ALARP. It is the premise of this approach that the effectiveness of the critical controls is determined by their ability to reduce the risk; removing them would have a significant detrimental impact on preventing incidents or mitigating the consequences.

In the SQRA process, critical controls are selected and then a detailed assessment is performed on each by operations personnel and subject matter experts to determine how adequately the control is performing. The outcomes from this assessment are used to define actions (risk reduction measures) to improve the performance of the controls.

Subsequent to the SQRA, critical control verification programs are implemented to monitor the ongoing performance of the critical controls. The in-field verification of the adequacy and effectiveness of the controls allows targeted actions to be identified to address any weaknesses. The overall aim of the performance assessment and in-field verification activities is to establish that the risks are reduced to ALARP.

The mining industry has developed this technique, and the approach they are taking is described in the International Council on Mining & Metals (ICMM) Good Practice Guide on Critical Control Management (ICMM, 2015). The approach is called critical control management (CCM) and consists of the following core steps:

- Selecting the critical controls
- Assessing their adequacy
- Assigning accountability for their implementation
- Verifying their effectiveness in practice

The implementation of CCM, by mining companies has led them to prepare critical control performance standards, which set the objectives, performance requirements, monitoring and verification activities to be undertaken by operations to ensure the ongoing effectiveness of the critical controls. This is vital step in the demonstration of ALARP, as it provides the demonstration that all of the significant risk reduction controls put in place to manage the risk are working to a defined level of performance.

As an example, the bowtie segments shown in Figure 3 and Figure 4 contain examples of the critical control selections and functional elements made by GHD's dams engineers. The two controls shown in Figure 3 are undoubtedly critical controls in the prevention of a tailings dam failure by overtopping, and as their functional elements reveal, there are many components to ensuring that the design and operation of the tailings dam are effective.

As shown in Figure 4, there are also critical mitigation controls that if implemented effectively would reduce the risk of loss of life in downstream communities. The performance standards for each of the critical controls shown on the bowtie would include an assessment of all of their functional elements and in-field verification that these functional elements are performing effectively.

Dam Safety – Are Risks ALARP?

Armed with bowties, a semi-quantitative risk assessment and critical controls implemented and assessed for the performance in managing the risk it is now possible to address the fundamental issue for dam safety – is it safe enough? The mining industry approach is to rigorously evaluate and constantly monitor the performance of the critical controls. Any weakness in a critical control functional element is taken as a sign of weakness in the critical control and becomes a reportable event for follow up through successively higher management levels of the organisation until it is resolved. ALARP is demonstrated when all critical controls are performing to their functional requirements, meeting defined performance criteria.

But is this enough?

A recent publication on the implications for designers of the Engineers Australia Safety Case Guideline (3rd Edition) (Francis 2013) discusses the Safety Case risk reduction approach based on so far as is reasonably practicable (SFAIRP) and states that it is different to ALARP. The SFAIRP approach, now a feature of Australian workplace health and safety legislation, focusses on showing that all foreseeable critical hazards have been identified, all practicable precautions have been taken, the reasonableness of the precautions has been determined and the reasonably practicable precautions have been implemented.

An outcome of this interpretation of the Statutes in most Australian States is that designers and operators of large dams must ensure that the processes they use are capable of identifying all foreseeable critical hazards, their criticality has been established and the precautions have been designed, implemented, operated and maintained to reduce the risk so far as is reasonably practicable. Hence, there will be no generic one-size-fits-all Safety Case for all types of dam structures; each structure will require its own evaluation and will need to demonstrate in its own right that its risk to the community is reduced to SFAIRP.

Conclusions

Over the past decade the global mining industry has developed a sophisticated risk based approach to the understanding and management of catastrophic events within its mining and minerals processing operations. The role of bowties has been highlighted as a useful tool for the transfer of risk management knowledge from the designer, to allow dam owner / operators to better understand their risks and to recognise the link between design, construction and operational controls and how they are used to manage those risks to ALARP.

In this paper we have illustrated how bowties are constructed, how risks can be semi-quantitatively estimated, and how critical controls are selected and managed. If all this is done well, throughout all stages of the dam lifecycle, risks can be demonstrated to be as low as reasonably practicable (ALARP). The approach has been demonstrated for a tailings dam failure, but the findings are more generally applicable to large dam safety. This approach sets the scene for a future Safety Case regime in the design, construction and operation of large water storage dams.

Acknowledgements

List of References

Australian National Committee on Large Dams (ANCOLD). 2003. Guidelines on Risk Assessment

Australian National Committee on Large Dams (ANCOLD). 2012. Consequence Guidelines

Australian National Committee on Large Dams (ANCOLD). 2012. Guidelines on Tailings Dams. Planning, Design, Construction, Operation and Closure

Bowker, L.N.; Chambers, D.N. 2015. The risk, public liability, & economics of tailings storage facility failures. Accessed on 29/06/2016 from:
https://www.earthworksaction.org/files/pubs-others/BowkerChambers-RiskPublicLiability_EconomicsOfTailingsStorageFacility%20Failures-23Jul15.pdf

Dawson, Sir D. M. (1999). The Esso Longford Gas Plant Accident Report of the Longford Royal Commission. *Parliament of Victoria Government Printer*. Accessed on 7/07/2016 from:
http://www.parliament.vic.gov.au/papers/govpub/VPARL1998-99No61.pdf

Francis, G; Richardson, R. 2013. Implications for Designers of the Engineers Australia Safety Case Guideline (3rd Edition), accessed on 11/02/2016 from:
http://www.iceweb.com.au/icenews/Nov13/Implications%20Australian%20Safety%20Case%20Guideline.pdf

ICMM Good Practice Guide on Critical Control Management. 2015. *International Council on Mining & Metals, London, UK.*

ISO31000:2009 International Standard for Risk Management. *Standards Australia*.

Jonker, M.; Barker, M.; Harper, G. 2006. Failure modes analysis as applied at Rocklands Dam. *ANCOLD 2006 Conference.*

Mills, R.; Andrew, M.; Reynolds, H. 2016. Can we stop a black swan breeding? Advances in bowties and critical control management. *International Mine Management Conference, Brisbane, Qld, 22-24 August 2016, AusIMM, Carlton, Australia.*

Morgenstern, N. R., Vick, S. G. and Van Zyl, D., 2015. Report on Mount Polley tailings storage facility breach. Report of Independent Expert Engineering Investigation and Review Panel to Province of British Columbia, January 30th.

Reason, J. 1995. A system approach to organisational error. *Ergonomics, Volume 38: 1708-1721.*

Sklet, S. 2006. Safety barriers: Definition, classification, and performance. *J Loss Prevention Process Industries, Volume 19*: 494–506.

UNEP/ICOLD Bulletin 121. 2001. Tailings dams risk of dangerous occurrences, lessons learned from practical experience. *ICOLD Committee on Tailings Dams and Waste Lagoons.* Accessed on 7/07/2016 from: http://www.icold-cigb.org/GB/Publications/moteur_bulletin.asp

World Information Service on Energy Uranium Project. 2016. Accessed on 12/07/16 from: http://www.wise-uranium.org/mdaf.html