RISK ANALYSIS IN DAM SAFETY: THE PAST, THE PRESENT AND THE FUTURE

DR. PRZEMYSLAW
Hydrosms, Ontario, Canada

*As knowledge advances, we are able to invent better and better models, which reproduce more and more features of the real world, more and more accurately. Nobody knows whether there is some natural end to this process, or whether it will go on indefinitely. …We expect that any model we are now able to construct will be replaced by more complete ones in the future, and we do not know whether there is any natural end to this process (*E.T. Jaynes,).

ABSTRACT

Until late 1980's the safety of dams had been assessed and controlled exclusively by a rules-based (often called standards-based) approach, which had been applied for both the design of new dams and the assessment of the safety of the existing dams. Increasing societal awareness of negative impacts resulting from failures together with the understanding that the trade-offs between to costs of increasing safety and the benefits from reducing the residual risk need to be determined before the best decisions can be made brought to the forefront new approaches that focus on explicit characterization of risks. This trend can be traced back to the late 1970's and despite the early scepticism about the feasibility of carrying out credible and defensible analysis of risk, it started gaining gradual acceptance in the dam safety field. The methods of risk analysis for dams have been constantly evolving over the past forty years and this paper provides a brief characterization of this process together with the lessons learned during this journey. Equally important as the analytic approaches were the developments in terms of risk evaluation and its use at different levels of decision-making but they are not discussed in the paper.

1. INTRODUCTION

Risk-informed analysis is steadily gaining acceptance as an appropriate approach to assessing dam safety. While in most countries, dam safety is regulated by governmental entities, and some of these are not in favour of utilizing information about risk in regulation, at the same time the dam engineering community is developing and implementing risk analytic techniques and various risk evaluation schemes for dam safety. While many of these address comparative risk and risk ranking within a collection of assets, the efforts continue in improving a risk-informed decision-making process for individual dams.

2. THE BEGGINNING

The beginnings can be tracked back to the early 1970's (Ellingwood and Ang, 1972) and (Yucemen et al, 1973). In their report Ellingwood and Ang stated that the concept of an acceptable risk of failure is central to a rational approach to safety. They postulated that the classical reliability theory which assumes that loads (S) and resistances (R) are random variables can provide the foundation for risk analysis for dams. The approach would ensure safety by assigning a sufficiently small probability to the event that the resistance will be less than the applied load effect or, in other words, the probability of failure, $P_f = P(R < S)$, would be specified to be acceptably small. The report's focus was strictly on the analytic approach to characterization of the probabilistic component of risk and did not discuss the complex and difficult aspects of risk evaluation and of what could constitute the acceptably small probability of failure.

One year later Yucemen et al published a report on probabilistic study of earth structures. They noted that soil and foundation engineering were characterized by extensive uncertainty, caused by insufficient information and inadequate knowledge of the subsoil conditions and the fact that properties of soil generally varied both in space and in time. Therefore, the report proposed a probabilistic method of addressing all sources of uncertainty when analysing slope stability problems. The proposed format was based on the approximate first-order probability theory and was illustrated by examples of short and long-term stability of slopes.

There were some further developments in the following years, (Rouselle and F. Hindié, 1975) and (Alonso, 1976). However, it was the publication of three papers [(Bowles et al, 1978), (McCuen, 1979) and (Prendergast, 1979)] which explicitly and in more formal way introduced the concept of dam safety risk assessment.

Bowles and his co-workers proposed the framework of a phased process of risk analysis for dams based on (Rowe, 1977). The framework was built on a four-element sequence of event-outcome-exposure-consequence paths which allowed the analysis to link the occurrence probabilities of each event. The work was later expanded (Howell, 1980) to a format comprised the following five major elements: event-system response-outcome-exposure-consequences.

McCuen observed that at the end of 1970's safety factors were still predominantly, if not exclusively, used to account for uncertainty in design and construction[1] of dams and although such practice resulted in excellent safety record the fact that the failures had been occurring should have caused the engineering profession to re-examine the approach. He then postulated that what was needed was a design system that permitted the formal assessment of risk for all design aspects affected by uncertainty. As a solution he proposed a framework based on the Bayesian decision theory.

Prendergast' report was even more succinct in outlining the need for a new approach. He pointed out that the design process for dams involved numerous uncertainties associated with the external and internal forces and factors. Although the engineers were fully aware of this fact, no meaningful attempts had been made to quantify the uncertainty and the designers always relied on subjective choice of design parameters and conservative safety factors based on experience and judgment. As a result, there was no consistent basis for comparing safety of different designs and there was no systematic and credible way of assessing the impacts of uncertainty on the safety of a design. He further stated that *"In a realistic sense, the safety of a dam is a matter of acceptable risk, and within this premise, the logical and quantitative basis for evaluating dam safety requires the concepts and methods of probability"*. The conclusion of the report was that "*the concepts and methods of probability, i.e., extended reliability theory, provide the proper basis for evaluating of the safety of dams*". The proposed approach was illustrated in the report by describing in detail the process of probabilistic stability analysis of concrete gravity dams at normal or extreme operating conditions.

A different approach to the similar problem begun to be developed in the Netherlands (Bakker and Vrijling, 1980) and (Mulder and Vrijling, 1980). The papers provided an outline of a probabilistic method for protective sea defenses (dunes and dikes) design. The approach utilized the fault tree techniques for the development of all possible failure scenarios of the sea defenses system and the concept of the ultimate limit-state of a failure mechanism. The approach included derivation and complex probabilistic calculus that begun with the probability density functions (pdf) of the boundary conditions and ultimately led to the derivation of the pdf's of 'potential threat' and 'resistance'. The approach relied heavily on theoretical mathematical models.

The concept of using information about risk in assessing dam safety has been further explored in the early 1980's. (Cheng et al, 1982) developed a risk model based on fault tree and a load model that included random process modeling of the flood, wind, and other geophysical forces. (Kreuzer and Bury, 1984) outlined a complete procedure based on classical reliability approach for the evaluation of dam safety and risk, comprising (i) identification of primary failure causes and hazardous conditions, (ii) selection of load scenarios, (iii) cause-failure analysis providing failure probability value, (iv) failure-consequence evaluation, and (v) estimation of total risk. All uncertainties pertaining to data were expressed by probability functions or partial coefficients. (Bury and Kreuzer, 1986) illustrated how event trees can be utilized to develop cause-to-failure-to-consequence scenarios.

Important developments occurred in the second half of 1980's. First, (McCann et all, 1985) issued a report dealing with safety evaluations of existing dams. The report proposed a methodology for conducting dam safety risk analysis comprising four steps, namely (i) identification of events that can cause dam failure, (ii) determination of frequency of occurrence of loading conditions caused by events identified above, (iii) determination of conditional probabilities of dam failure caused by each loading condition, (iv) assessment of consequences caused by each failure mode.

One year later US Bureau of Reclamation issued a report (USBR, 1986) providing guidelines on dam safety related decision analysis when using the information about risk. The purpose of the guidelines was "*to outline a decision analysis framework incorporating the concepts of adverse consequences and the risk of occurrence by which alternative solutions to a given problem may be evaluated"*. The guidelines stated out that although engineering judgment is an important factor in problem solving under uncertainty, a formal decision analysis provides a means for displaying the uncertainty in a manner that allows an informed decision.

The proposed analytic framework included five steps: (i) problem definition, (ii) site condition characterization, (iii) identification of loading conditions, (iv) determination of system response[2], and (v) hazard assessment. The guidelines were followed by a detailed risk assessment procedure (USBR, 1989) with the focus on seismic and hydrologic events as causes of failure,

Both reports influenced in a significant way the developments in risk assessment for dams in North America and Australia for the next several decades. The most important decision taken in developing both of these documents was the separation of the analysis of loading conditions from the analysis of system response. The separation made the organization of the analytic process simple and easy to understand. It also led the practical development and applications toward analytic tools dealing with the sequences or chains of events and event tree technique. The (USBR, 1986)

1. For a long time, dam safety risk assessment efforts concentrated on design and construction aspects. Risk issues caused by operation appeared later.

2. System response was defined as reaction or performance of the dam and appurtenant structures under specified loading conditions with possible outcomes that may include no failure, partial failure, or complete failure.

remains a benchmark in the field of dam safety as it provided the general framework following the line of reasoning as depicted in Figure 1. The principal concepts of this framework included separation of the analytic process of failure initiation and development into three steps:

- Analysis of loadings or conditions initiating the failure mechanism;
- Analysis of failure mechanism development and progression;
- Forecast of consequences should failure occur.

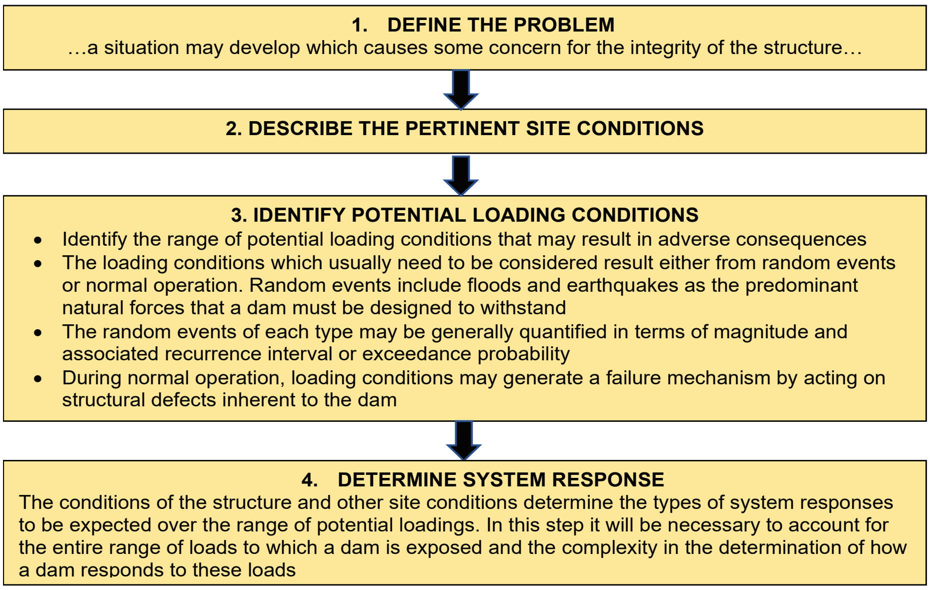

Figure 1 : (USBR, 1986) top portion of decision analysis framework

This conceptual model of the set of conditions preceding the dam failure has been universally accepted and for the past two decades served as a basis for the vast majority of risk models aimed at risk-informed support for decision making in dam safety (ANCOLD 1994 and 2003), (Defra, 2013 a,b), (FEMA, 2014), (ISPANCOLD, 2013), (USBR/USACE, 2012), (USBR/USACE, 2015)).

3. THE PRESENT

Within a relatively short time period risk models utilizing event tree technique became the most widely used tool in dam and levee safety risk analysis. The first comprehensive application of the risk assessment for dams based on even tree risk model appeared in the same year as the USBR Guidelines. Tongue River Dam Risk Assessment (DNRC, 1986) was initiated after the traditional dam safety assessment concluded that since the dam was unable to pass the Probable Maximum Flood without failing, a risk assessment was needed in order to evaluate alternative actions proposed to mitigate the risk. The risk assessment was carried out using the framework outlined in 1986 USBR Guidelines (event-system response-outcome-exposure-consequence framework). The risk identification stage included:

- Initiating events (flood, earthquake, slope instability, piping at outlet works or embankment, landslide into reservoir, foundation failure)
- System response or failure mode (overtopping, deformation, liquefaction, rupture)
- Outcome (breach)
- Exposure (time of day, season, warning time)
- Consequence (Loss of life, economic damage).

Risk model utilized an event tree that included the sequence of events starting out from each initiating loading event to an ultimate fail/no fail outcome. Key probabilities for all loading events, for the system response[3] and for the outcome were estimated using the mix of probabilistic frequency analyses, subjective/judgmental approaches and pro-rating of historical failure rates.

Important guiding documents began appearing in the 1990's and they included first ANCOLD Risk Assessment Guidelines (ANCOLD, 1994), Reclamation Guidelines for Achieving Public Protection in Dam Safety Decision-making (USBR 1997, 2003), second ANCOLD Risk Assessment Guidelines (ANCOLD, 2003) as well as an important book (Hartford and Baecher, 2004) and ICOLD Bulletin on Risk Assessment for Dam Safety (ICOLD, 2005).

3. System response included three possible outcomes: no failure, failure and partial failure. While the interpretation for the first two is obvious, the third one has not been defined.

Extensive effort by US Federal agencies brought several versions of Best Practices in Dam and Levee Safety Risk Analysis (USACE and USBR, 2012, 2015 and 2018) and FERC Interim Guidance on Risk-Informed Decision Making (RIDM) - Risk Guidelines for Dam Safety (FERC, 2016). Original developments in the US and Australia influenced development of SPANCOLD Guidelines on Risk Analysis Applied to Management of Dam Safety (SPANCOLD, 2013).

The common element of these different approaches to analysis of dam safety risks originated from the fundamental assumption that the analysis of hazards creating loadings on the dam and the analysis of responses to these loadings can be separated, analyzed independently and then combined utilizing chain-of-events (with the event tree as a preferred analytic technique) approaches in order to arrive at the probability of dam failure.

The further evolution of the approach included important changes to the definition and the understanding of what is the system response to loadings. The current definitions are:

System response – how a dam responds, expressed as a conditional probability of failure, to a given scenario of applied loads and concurrent conditions (FERC, 2016).

System response (or probability of failure) describes the relationship between the demand (i.e. driving forces or loads) that a system is subjected to and the capacity (i.e. resisting forces or strength) of the system to withstand the demand (USBR, 2015).

It should be noted the above definition of system response excludes modifications of loadings, both in terms of probability of occurrence and the magnitude. Such changes can occur with relatively high frequency in hydrologic loadings and may be caused by a variety of disturbances causing disruptions in the flow of water through the system. In terms of system-thinking approach such exclusion is equivalent to the removal of feedback links from the system model.

In dam safety risk assessment applications there are frequently used arguments that even if a dam is decomposed into its primary sub-systems (for example, earth embankment, sluiceway, gates, powerhouse, headworks, etc.) and components (rip-rap, shell, filter, core, etc.), there is little or no interaction or feedbacks among the components and sub-systems. Thus, all components can be considered separately and the safety of the entire dam systems can be derived from the information about the reliability of individual components. This position was very clearly expressed recently by (Galic,2017) who stated that "…*Regardless of whether they are constructed of concrete or earth, large dams are, to some extent, passive structures, with limited control over a significant percentage of the stored volume. While there are usually electromechanical components present, the failure of such a component (e.g., of a spillway or penstock gate) generally has the potential to harm fewer people than the failure of the dam itself. With some exceptions (e.g., a pumped storage facility built without a spillway), most large dams, with respect to the potential for a major failure, would not be properly characterized as complex systems. Thus, while an intricate dynamic model may be required for a complete understanding of the 1979 incident at Three Mile Island, the only thing needed for a working understanding of how Teton Dam failed three years earlier is a good grasp of fundamental soil mechanics concepts*".

While such interpretations can be applied to most of the structural (hard) components of a composite dam it disregards the functioning of the non-structural (soft) components of a dam system. In particular,

- Failure of flow control equipment may lead to overtopping and ultimately dam failure.
- More often than not, there are multiple dams within a single watershed and the operation of any single dam may affect the safety of other structures. For that reason, hydrology and water management engineers have always thought in terms of *river systems*, where interactions between individual reservoirs (system components) are of the utmost importance.
- Dams in multiple dam systems cannot be operated independently because the water is flowing through the system all the time and it has to be either stored or passed to the next reservoir. Any failure of flow control equipment at any dam may impact the operating strategy of the entire system or its part and any disruption in the individual reservoirs or the entire system operation may change both the magnitude and/or the exceedance probability of hydrologic loadings.
- The term *dam system* refers to more than just physical components and technical aspects. It has to include social, managerial, organizational, human and political factors, which together create a complex dynamic system with complicated interrelations and feedbacks.

To some extent the concept of dam systems has been explicitly recognized in (Defra, 2013a, b) where the elements described in Table 1 are included in the definition of a reservoir system.

While the concept of a *dam system* has been adopted as a general principle in Defra guidelines it has not been extended to all elements of a broader system comprising all dams and reservoirs (interrelated through physical, operational and human agency-based links) within the watershed under consideration. Thus, many important dynamic interactions and feedbacks are either not accounted for or are only partially included in the analysis during the development of loading scenarios.

Table 1 – Dam as a system

Aspect	Definition
Physical features	The reservoir system including surrounding hillsides, the dam(s) and their abutments and foundations and other reservoirs in cascade
	All appurtenant structures
	Electromechanical equipment
	All instrumentation and communication systems
	Any other natural or man-made physical features relevant to the safe operation of the reservoir
Operational features	Maintenance, monitoring, surveillance and inspection procedures
	Any manuals and software needed to operate automated or remote-control systems for reservoir operations upon which safe reservoir operation depends including inflows and discharges, information such as inflow flood forecasts, management systems, communications and decision protocols
Human factors	Includes maintenance, monitoring and surveillance, supervision and inspection
	All management aspects of the owner/undertaker or operating organisation on which safe reservoir operation depends

Following the conceptual model of dam failure requires analytic procedures capable of systematic and logical characterization of sequences of events beginning with initiating events and ending in the uncontrolled release of storage. The early applications of risk analysis for dams experimented with the use of Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects and Criticality Analysis (FMECA) but at the present the field is dominated by events trees (and fault trees for some specific applications). The common feature of all these techniques is that they view accidents and failures as something which results from a chain of events that can be organized in chronological order.

As pointed out before, event trees as the analytic technique appropriate for these purposes were recommended as early as early 90's and have become the preferred technique. There is no doubt that the application of event tree as the logic engine of risk analysis significantly advanced dam failure analyses. As (FEMA, 2014) indicated this analytic technique provided additional insight into dam safety (as compared to the traditional safety assessments based on "standards" and design values) since event trees are:

- Capable of displaying the chronological order of events;
- Intuitive because the events from left to right are the sequence of events that occur given the previous event or condition to the left;
- Well suited for displaying dependencies between events and the order in which they occur;
- Capable of better communicating and understanding about assumptions in developing the model;
- Easily understood by people with non-technical background;
- Well suited to display details of the problem; and
- Drawn on standard computer spreadsheets or specialty software.

At the same time when these important developments were taking place in the dam engineering field, a new philosophy begun emerging across many hazardous industries - a philosophy for assessing the safety of built facilities based on an underlying principle of *system safety*. The philosophy was based on the recognition of the fact that engineered systems are not just a collection of technological (hard) components but they also must include these (soft) elements of the system that reflect the structure, management, institutional arrangements, procedures, plans and the culture of the dam owning organization.

The growing recognition of importance of treating dams as systems is now challenging the general perception that chain-of-event analytic techniques are sufficient for risk analysis of dams, as the events that are ending as failures may be complex combinations of many factors. These may include components failures, inadequate maintenance, problems arising from instrumentation and control, human actions, design errors, errors in the operating plans and procedures, errors in implementing the operating decisions and problems arising from multiple dam ownership and conflicting interests in system operation.

Chain-of-events models that work well for simple systems are not always appropriate for complex systems. Chain-of-events models are based on the assumption that the behaviour of analyzed system can be explained by a series of linearly related events over time. As a result, they simplify the process leading to failure and may exclude important systemic factors and indirect and non-linear interrelations between individual events (Leveson, 2011). Leveson also pointed out that traditional chain-of-events models have particularly poor performance when dealing with human errors and with all issues related to decision making. Human behavior can be included in an event tree through the binary decision of human actions (success or failure). While adequate for certain situations, this may mask the range of behaviours possible at any given moment and system state. It can also obscure the underlying reasons for the behavior, including many important causal factors that are difficult or impossible to model in any failure-based method such as: correct human behaviour that is not defined for certain situations, specified human behaviour that is known by operators but thought to be incorrect, procedures that conflict with each other, or it is not obvious which procedure applies, information necessary to carry out a procedure is not available or is incorrect, the person has multiple responsibilities or goals that may conflict, past experiences and current knowledge conflict with a procedure, procedures are not clear or misunderstood, procedures are known but responsibility for the procedures is unclear or misunderstood, procedures are known and followed, but they are unsafe.

It should be noted that design errors and requirements flaws are not amenable to analysis using chain-of-event techniques and are easily overlooked. In addition, higher-level systemic causes such as organizational and managerial issues cannot be included in a chain-of-event based analytic approaches. Such issues can be numerous and may include poor or inadequate management, ineffective communication, misplaced regulatory priorities, and complacent staff attitudes.

The modern understanding of system safety entails an approach in which all elements (physical sub-systems and components, operating plans and procedures, organizational, managerial and human factors) are modelled in a fully combined and integrated frame. This and only this ensure that all dynamic interactions and interdependencies between the elements are accounted for thus providing all relevant information to analysis of system risks. It is intuitively clear that such objective can be achieved by embedding the models of systems processes dynamics and human behaviour into stochastic simulation framework allowing it to reproduce the occurrences of failures along any required time frame. The general concept of such approach can be found in (Hartford et al, 2016).

4. THE FUTURE

The progress in developing and implementing various risk analysis techniques for dam safety assessment purposes has been steady in the past two decades and the credit for that belongs predominantly to the US federal agencies and dam owners and regulators in Australia. The work done in these countries was instrumental in getting the world-wide attention of dam owners, regulators of dam safety and dam engineering consulting community that the information generated through dam safety risk assessment is invaluable in making the right decisions with respect to various aspects of dam safety.

Notwithstanding the progress made and the current state of developments in this field, it is becoming clear that the improvements in the analytic methods can be and need to be made. Some precursors of alternative approaches have been proposed in the past few years and they include stochastic simulation and Bayesian Networks as two possible analytic techniques capable of addressing 'dams as systems' aspects of risk analysis for dam safety. It is expected that with the growing importance of risk-informed decision making in dam safety, other analytic approaches will continue to be explored.

4.1 Stochastic simulation

Stochastic event simulation approach (Micovic et al, 2015) was applied to probabilistic characterization of hydrologic hazard through the probabilistic characterization of reservoir water levels and releases in the Campbell River System, BC, Canada. The basic concept employed in the approach was the computer simulation of multi-thousand years of flood annual maxima and their progression through the river system. Stochastic flood modelling was conducted using the Stochastic Event Flood Model in combination with a deterministic watershed (precipitation-runoff) model which utilized the conversion of the precipitation input into runoff, with hydrometeorological input parameters treated as variables instead as fixed values. Monte Carlo sampling procedures were used to allow the climatic and storm-related input parameters to vary in accordance with those observed in nature. There were three distinct aspects of stochastic flood simulation in a complex river system, namely:

- the simulation of natural inflows in each of the reservoirs within the river system;
- the simulation of reservoir operating rules, i.e. flood routing for the individual reservoirs as well as the whole system;
- the stochastic simulation of on-demand availability of various discharge facilities within the system, i.e. failure of individual spillway gates, low level outlets, powerhouse outlets, or some combination of those

All three aspects were combined within the stochastic simulation framework and multi-thousand years of extreme storm and flood annual maxima were generated by computer simulation. The simulation for each year applied a set of climatic and storm parameters selected through Monte Carlo procedures based on the historical record and collectively preserved dependencies between the hydrometeorological input parameters. Execution of the watershed model with reservoir routing of the inflow floods through the system and stochastically modelled failure/availability of various discharge gates, provided corresponding multi-thousand-year series of annual maxima flood characteristics. Characteristics of the simulated floods such as peak inflow, maximum reservoir release, runoff volume, and maximum reservoir level were the flood parameters of interest. Annual maxima series were then created for each of these flood parameters and the values were ranked in descending order of magnitude and a non-parametric plotting position formula and probability-plots were used to describe the magnitude-frequency relationships. Simulation with the help of watershed model produced one maximum for flood peak discharge, maximum reservoir release, runoff volume, and maximum reservoir level at each of the dams in the river system. These maxima were then used in assembling annual maxima series representing multi- thousand years of flood events.

Continuous stochastic simulation approach (Zielinski et al, 2017) based on the principles of system safety (Hartford et al, 2016) was applied to the Madawaska River System in Ontario, Canada. A comprehensive risk assessment study seeking to determine whether risk exposure due to inability to safely pass IDF is sufficiently high to justify discharge capacity upgrades was carried out. The Madawaska River watershed is a complex system comprised of numerous inter-related, interdependent and interactive components which can be influenced by random events. The operation of the system is mainly governed by the actual water levels in reservoirs, actual inflow and the inflow flood forecast of Madawaska watershed to achieve target reservoir water levels based on historic safe operation. However, the system can be greatly influenced by other random events such as failure of transmission system, failures of flow control equipment, and inability to gain access to sites. Other operational challenges that further contribute to the complexity of the system and its operation include numerous contributing watersheds that are managed by other entities, many facilities requiring sluiceway equipment to be manually operated on site, fairly remote sites of these facilities, limited resources available to manage all sites, inaccuracy of the inflow flood forecasts, and environmental and other stakeholder's requirements for water levels flow releases to maintain ecological and/or biological healthy system. Simulation of such a complex system is not practical using analytical solutions. Therefore, a dynamic system simulation (a systems approach) was used to analyze and predict how all components comprising the system interact and behave as a whole.

Analytic approach was based on the philosophy of system modeling through stochastic simulation. Inflows to the sites simulated as random functions of time were routed through the system thus creating dynamic demand on flow discharge equipment. Recorded frequencies of overtopping occurrences provided good approximation of probabilities of failures due to overtopping. The diagram illustrating the general conceptual modeling framework is depicted in Figure 2.

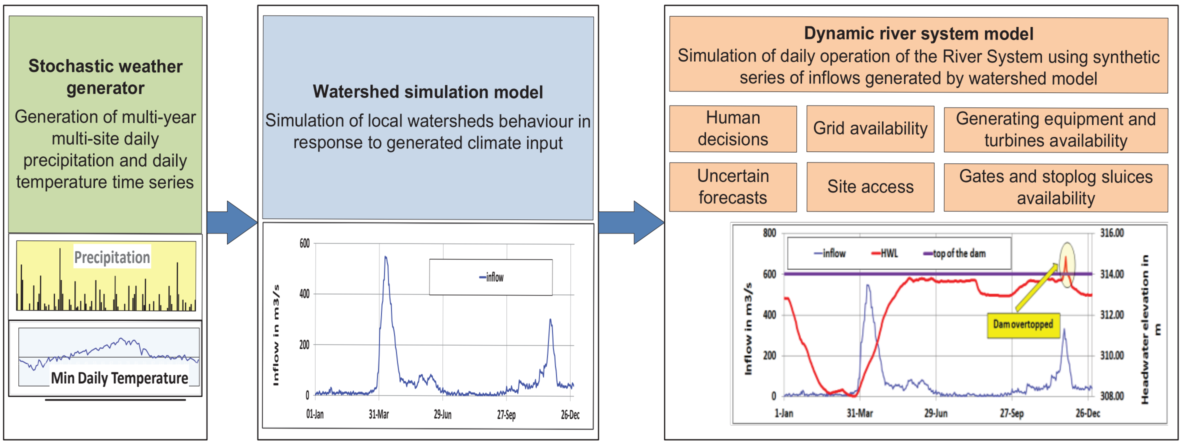

Figure 2 : Modelling approach

The first element of the framework was the climate module responsible for generation of the long (up to 100,000 years) stochastic time series of daily synthetic climate data. The climate data provided the input to the second module which comprised hydrologic watershed models of local sub-basins in the Madawaska River System. The models used the synthetic climate data and converted it into runoff in the sub-basins and the streamflow at the outlets from the sub-basins. The outflows provided the necessary data in form of daily inflows enabling carrying out the simulation of the operation of the entire system. The routing of the flows through the system created the demand on flow control equipment. Each piece of flow control equipment (system component) responds to the demand according to its availability characterized by individual reliability metric. Demand was created dynamically in response to various stochastic disturbances impacting the operation. The simulation was carried out and all instances when the headwater level exceeded the level of potential overtopping failure mode initiation were recorded at each site.

4.2 Bayesian Networks

Bayesian networks (BNs) have been one of the most successful analytic methods used to deal with systems operating under uncertainty conditions. Recent applications in the field of dam safety include (Li and Liang, 2016), (Ponnambalam et al, 2019) and (El-Awady et al, 2019).

In the first paper a method based on a Bayesian network combined with stochastic Monte Carlo simulation is used in this research to calculate the probability and analyze the risk of a single reservoir dam overtopping and two reservoirs collapsing under the combined action of flood and landslide surge. Two adjacent cascade reservoirs on the Dadu River in China are selected for risk calculation and analysis. The authors concluded that combining Bayesian network theory with stochastic Monte Carlo simulation was an effective method for calculating probabilities and analyzing the risk associated with a single reservoir dam overtopping and for investigating whether multiple cascade reservoirs will collapse under the combined action of various risks and working conditions. This study may constitute a firm basis for providing useful technical support with respect to risk prevention and control in reservoirs in the future.

Ponnambalam et al paper pointed out that determining failure probabilities of a complex system using exhaustive simulation methods is efficient only when the number of components is small. It proposes a BN approach to solve the same problem in an efficient manner supported by simulations, where they are appropriate, calling this method the simulation supported BN (SSBN). SSBN decomposes the network into smaller sub-networks; each simulated separately to provide failure probability information. The BN allows for combining this information to calculate failure probability of the entire system. SSBN makes the complex system easy to deal with by reducing the time and effort to solve.

In El-Awady et al paper Mountain Chute Dam system, which is a part of the Madawaska River System in Ontario, is used as a case study. Bayesian Network (BN) is used to represent various components of dams with associated probabilistic information such as marginal and conditional probabilities to estimate system failure probabilities. Expert judgement, logic inference, and models of reservoir systems, may also be used to aid BN. The network representation of Mountain Chute dam and generating station is relatively complex. While limited data are available for this network, logic inference or eliciting expert judgement may be used to quantify the network probabilistically. This revealed a significant difference in the failure probabilities when the BN is quantified using expert judgement than the case that uses logic inference. Adding expert engineering judgement helped in reducing the uncertainty in the network, and gave better estimates for the operation of the dam. The two cases of using logic inference and using expert judgement can be considered two different scenarios that the decision maker can rely on. The worst-case scenario may be the one that uses logic inference, and the safe operating scenario is the one that uses expert judgment. If more data is available, simulation models may support BNs in estimating the steady state probabilities for such systems.

5. CONCLUSIONS

The progress made in the several past decades in the area of risk assessment for dams makes the formal risk assessment an important part of dam safety decision making. Development of specific, detailed methodologies of risk analyses in the US and Australia reached the level of maturity which allowed successful implementation of explicit risk assessment results into dam safety decision making. This, in turn, increased the interest in analytic aspects of risk-informed dam safety decision-making around the World, and encouraged research efforts aimed at improving analytic capabilities.

There is no doubt that with time, new, better and more complete methods of characterizing all probabilistic aspects of dam failures will be developed, tested and implemented. Dam safety field is no different than any other area of engineering where the progress is constant and new methods and approaches appear and replace the old ones. This process will continue and as quoted out in the motto to this article *we expect that any model we are now able to construct will be replaced by more complete ones in the future.*

REFERENCES

1. Alonso EE (1976). Risk analysis of slopes and its application to slopes in Canadian sensitive clays. Géotechnique, 26(3), ISSN 0016-8505 | E-ISSN 1751-7656.
2. ANCOLD (1994). Guidelines on Risk Assessment. Australian National Committee on Large Dams, January.
3. ANCOLD (2003). Guidelines on Risk Assessment. Australian National Committee on Large Dams. October.
4. Bowles DS, Anderson LR and Canfield Bakker WT and Vrijling JK (1980). Probabilistic Design of Sea Defences. Report nr. 13780501. Dept. of Civil Engineering, Delft University of Technology.
5. RV (1978) A systems approach to risk analysis for an earth dam, Proceedings of the International Symposium on Risk and Reliability in Water Resources, Waterloo, Ontario, Canada.
6. Bowles DS and Ko HY (1984) Probabilistic characterization of soil properties, American Society of Civil Engineers.
7. Bowles DS and James LD (1984). Risk-Based Design and Evaluation of Dam Safety: An Overview. Presented at the 1984 Fall Meeting of the American Geophysical Union, San Francisco. December.
8. Bowles DS (1987) A comparison of methods for risk assessment of dams, in Engineering Reliability and Risk in Water Resources. L. Duckstein and E. Plate (eds). Springer, NATO ASI Series Book, Vol. 124.
9. Bury KV and Kreuzer H. (1986) The assessment of risk for a gravity dam. International Water Power & Dam Construction. 38(12).
10. Cheng S-T, Yen BC and Tang WH (1982). Overtopping Risk for an Existing Dam. Hydraulic Engineering Series No. 37, UILU-ENG-82-2017. University of Illinois, Urbana, Illinois.
11. DEFRA (2013a). Guide to risk assessment for reservoir safety management. Volume 1: Guide. Report – SC090001/R1, Environment Agency.
12. DEFRA (2013b). Guide to risk assessment for reservoir safety management. Volume 2: Methodology and supporting information. Report – SC090001/R2, Environment Agency.

13. DNRC (1986) Tongue River Dam Risk Assessment Report. State of Montana Department of Natural Resources and Conservation. December.
14. El-Awady A, Ponnambalam K, Bennett T, Zielinski PA, Verzobio, A (2019) Bayesian network approach for failure prediction of Mountain Chute dam and generating station. Sustainable and Safe Dams Around the World - Tournier, Bennett and Bibeau (Eds). Canadian Dam Association, ISBN 978-0-367-33422-2.
15. Ellingwood BR, and A. H-S. Ang AH-S. (1972) A Probabilistic Study of Safety Criteria for Design. Structural Research Series No. 387, UILU-ENG-72-2008. University of Illinois, Urbana, Illinois, June 1972.
16. FEMA (2014). Selecting Analytic Tools for Concrete Dams to Address Key Events along Potential Failure Mode Paths P-1016. U.S. Federal Emergency Management Agency.
17. FERC (2016). Risk-Informed Decision-Making Guidelines. Chapter 1 - Introduction to Risk-Informed Decision Making. Version 4.1 March.
18. Galic D (2017). On the Physical Meaning of Dam Safety Risk Estimates. Proceedings of Geo-Risk 2017 Geotechnical Risk Assessment and Management. June 4-7, Denver, Colorado, ASCE Publication.t
19. Hartford DND, Baecher GB, Zielinski PA, Patev RC, Ascila r and Rytters K. (2016) Operational Safety of Dams and Reservoirs: Understanding the Reliability of Flow-Control Systems. ICE Publishing, London.
20. Howell JC, Anderson LR, Bowles DS and Canfield RV (1980). A Framework for Risk Analysis of Earth Dams. Utah State University Reports Paper 405.
21. Kreuzer H and Bury KV. (1984) A probability-based evaluation of the safety and risk of existing dams. Proceedings of the International Conference on Safety of Dams. Coimbra, Portugal. 23-28 April.
22. Leveson NG (2011). Engineering a Safer World: System Thinking Applied to Safety. The MIT Press, Cambridge, MA.
23. Li P and Liang C (2016). Risk Analysis for Cascade Reservoirs Collapse based on Bayesian Networks under the Combined Action of Flood and Landslide Surge. Mathematical Problems in Engineering, Hindawi Publishing Corporation, Volume 2016, Article ID 2903935.
24. McCann MW, Franzini JB, Kavazanjian E and Shah HC (1985). Preliminary safety evaluation of existing dams. Report prepared for the Federal Emergency Management Agency, Stanford University, Stanford, California.
25. McCuen RH (1979). Risk Assessment in Dam Safety Analysis. J. Washington Academy of Science, 69(4).
26. Micovic Z, Hartford DND, Schaefer MG and Barker BL (2015). Flood hazard for dam safety – where the focus should be? Q.97-R.38 Proc. of the XXV ICOLD Congress, Stavanger, Norway.
27. Mulder T and Vrijling JK (1980) Probabilistic load determination in Hydraulic Aspects of Coastal Structures. Paape A, Stuip J and Venis WA (Eds).
28. Ponnambalam K, El-Awady A, Mousavi SJ, Seifi A (2019) Simulation supported Bayesian network for estimating failure probabilities of dams. Sustainable and Safe Dams Around the World - Tournier, Bennett and Bibeau (Eds). Canadian Dam Association, ISBN 978-0-367-33422-2.
29. Prendergast JD (1979) Probabilistic Concept for Gravity Dam Analysis. Special Report M-265. US Army Corps of Engineers Construction Engineering Research Laboratory.
30. Rouselle J and Hindié F (1975) Evaluation des débites de crues, 2, Evaluation du risque
31. Rowe (1977). An Anatomy of Risk, Wiley, N. York.
32. SPANCOLD (2013). Technical Guide on Operation of Dams and Reservoirs Vol. 1 Risk Analysis Applied to Management of Dam Safety. Spanish National Committee on Large Dams (SPANCOLD) and Spanish Professional Association of Civil Engineers (CICCP).
33. USBR (1986) ACER Technical Memorandum No. 7 - Guidelines to Decision Analysis. United States Department of the Interior, Bureau of Reclamation, March.
34. USBR (1989). Policy and Procedures for Dam Safety Modification Decision Making. U.S. Department of the Interior, Bureau of Reclamation. Denver, CO.
35. USBR/USACE (2012). Best Practices in Dam and Levee Safety Risk Analysis. U.S. Department of the Interior Bureau of Reclamation and U.S. Army Corps of Engineers.
36. USBR/USACE (2015). Best Practices in Dam and Levee Safety Risk Analysis. U.S. Department of the Interior Bureau of Reclamation and U.S. Army Corps of Engineers.
37. USBR/USACE (2018). Best Practices in Dam and Levee Safety Risk Analysis. U.S. Department of the Interior Bureau of Reclamation and U.S. Army Corps of Engineers.
38. Yucemen MS, Tang WH and Ang. A H-S. (1973) Probabilistic Study of Safety and Design of Earth Slopes. Structural Research Series No. 402, UILU-ENG-73-2015. University of Illinois, Urbana, Illinois.
39. Zielinski PA, Perdikaris J, Zhou r, Salloum T and Sakamoto D. (2017) System approach and simulation in risk assessment of dams. Proc. of the 85th Annual Meeting of ICOLD Symposium "Knowledge Based Dam Engineering". July 5, Prague, Czech Republic.