OPERATIONAL SAFETY AT U.S. ARMY CORPS OF ENGINEERS DAM AND HYDROPOWER FACILITIES

Africa 2017 – Hydropower and Dams, 14-16 March, Marrakech.

Robert C. Patev
National Risk Advisor
Risk Management Center
Institute for Water Resources
US Army Corps of Engineers
Concord, MA USA

Adiel Komey
PhD Candidate
Dept. of Civil Engineering
University of Maryland
College Park, MD USA

Gregory B. Baecher
Glenn L. Martin Prof. of Eng.
Dept. of Civil Engineering
University of Maryland
College Park, MD USA

Introduction

The quantification of operational risks at US Army Corps of Engineers (USACE) dam and hydropower projects is a critical piece of the overall USACE risk assessment processes. Operational risks need to be considered for both the daily operations and maintenance of the dam and hydropower systems and for emergency operations required during flood events. Many USACE dam and hydropower projects are multi-purpose and the methodology developed needs to be considered holistically to all operational aspects of the projects. Dams, along with their spillways and other waterways, are built to retain and control the flow of water for purposes of power production, water supply, navigation, recreation, flood risk mitigation, and environmental restoration. A typical USACE flood risk management (FRM) and hydropower plant is shown in Figure 1.

Fig. 1. Typical FRM Project with Hydropower: John Day Dam, Columbia River.

Embankment dams are themselves complex structures or systems comprising geotechnical, structural, mechanical and electric subsystems, such as gates and control equipment. Current engineering approaches to dam and hydropower safety are mostly based on probabilistic risk analysis (PRA). PRA primarily addresses the capability of a dam to withstand loads, such as the demand caused by the design flood and the spillway's capacity to pass that flood, or the demand caused by the design earthquake and the dam's capacity to withstand resulting ground shaking. PRA has proven especially useful in appraising design and rehabilitation decisions and which design loads and corresponding factors of safety must be chosen.

In contrast, experience has shown that many dam failures and perhaps the majority of dam incidents do not result from extreme geophysical loads, but rather from operational events. These incidents and failures occur because an unusual combination of reasonably common events occurs, and this unusual combination has a malicious outcome (Baecher 2016). For example, a moderately high reservoir inflow occurs, but nowhere near an extreme event; the sensor and SCADA system fail to provide early warning for some unanticipated reason; one or more spillway gates

are unavailable due to maintenance, or an operator makes an error in not opening the gate to correct opening, or there is no operator on site and it takes a great while for one to arrive; and the pool was uncommonly high at the time. This chain of reasonable events, none by itself particularly dangerous, can in combination lead to an incident or even potential overtopping and failure of the dam.

The paper and presentation will define a system methodology that evaluates the performance of structural, mechanical, electrical controls and sensing equipment over a range of loading conditions that are in combination with human factors such as work environment and stress, internal communication, operator training, and management policies and practices. The result of this system modelling is to identify weaknesses and corrective actions in areas such as corrective maintenance activities, plant staff working environments and level of job training, horizontal and vertical communication with upper management, and operations and maintenance manuals for dam and hydropower projects. This paper and presentation briefly discusses an example of operational risk pilots at USACE dam and hydropower projects

1. Methodology for Operational Risk at Dam and Hydropower Facilities

Operational risks are presented here as the ability of equipment and humans to operate on demand under all loading scenarios (from daily operations to extreme floods) to which a plant is subjected. This requires knowing both the physical reliability and state of the plant equipment, and the reliability of project personnel to successfully operate the equipment on demand, including their response to a mal-operations. The consequences portion of the operational risk can be described over a wide range from little to no effect to catastrophic failure of the plant or spillway. These consequences should be quantified as part of the operational risk study to assist with the mitigation of the risks that are inherent to the operations of these facilities.

As part of the methodology development, the USACE has started to examine the operational risks at several USACE dam and hydropower facilities. These operational risk pilots include site visits and interviews with key project staff in management, operations and maintenance at each project. A comprehensive review of their existing component list and operational condition assessments is made and documented for the development of fault trees for each project. Discussions are conducted with project staff on how they currently operate their projects, using which components from normal daily operations to extreme flood events. The methodology under development by USACE is outlined in the following proposed steps:

Step 1. Plant Equipment Reliability and Importance - Development of fault trees for all components, subsystem and systems and quantify the mission areas for each component serves at the project (Pate 2005). This include both the redundancy and common cause failures of the components and subsystems at a project. Develop baseline Birnbaum importance measures for all components, critical failure paths and minimum cuts sets at the component, subsystems and systems level. Establish operating levels of functional utility or availability (Patev 2014) that need to be maintain by the project to maintain each mission.

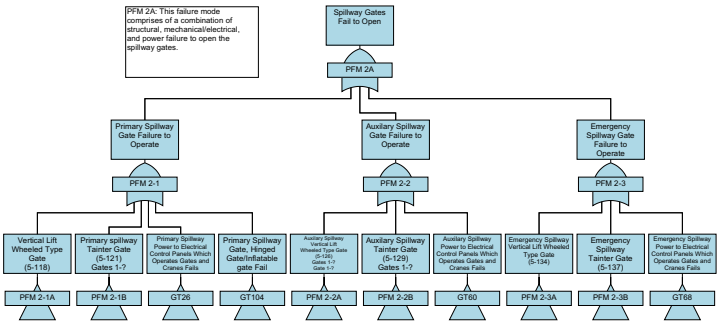

Fig 1. Fault Trees for Spillway Gates

Step 2. Operations of Plant Equipment – The understanding the operation of all components during all phases of dam and hydropower operation from normal daily operations out to extreme flood events. This is first established by examining the project operation and water control manuals and then conducting interviews with project management and staff on their understanding and operation of the plant. This is a critical step since often the

operation by manuals can be too prescriptive during normal to midrange operational levels. A frank discussion about mal-operations and backup systems or preventative actions that could be taken are important to capture when interviewing the plant operators.

Step 3. Maintenance Management of Plant Equipment – The understanding the maintenance practices for all components and establish the baseline operational condition assessment and availability of the plant including redundancy and available spares. Poor or unfunded maintenance practices result in a lower reliability and higher need of unforeseen maintenance and shutdowns to plant operations. This is critical to the operational modelling of the plant system. The understanding of both preventive and scheduled maintenance including inspections are important to mitigate future unforeseen risks which may lead to catastrophic events.

Step 4. Human Reliability of Plant Operations – NASA (Chandler 2006) defines human reliability as: 1) the probability that the human elements will function as intended over a specific period of time under specified environmental conditions, and 2) the probability that no extraneous human actions detrimental to the system reliability or availability will be performed. The key to these HR definitions is time, and specified environmental conditions. These are important since past human failure events in spillway systems have been directly correlated to many of the human performance shaping factors shown in Figure 2 (Chang 2007, Chandler 2006). Therefore, Human Reliability Analysis (HRA) is an important methodology that needs to be applied to spillway systems to account for the human errors that occur (Baecher 2016).

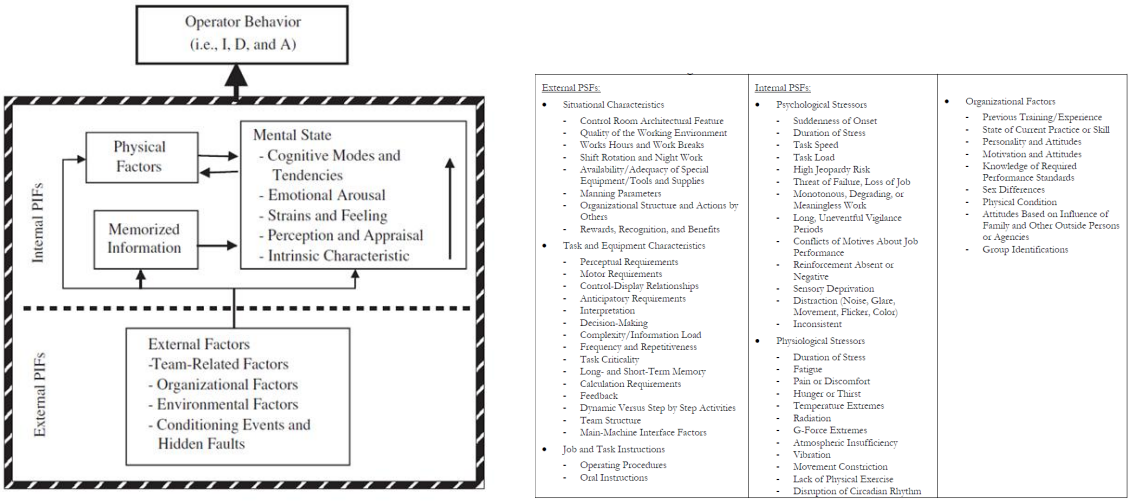

Fig. 2. Human Performance Shaping Factors (Chang 2007, Chandler 2006)

The HRA process needs to be tied into the system model being developed as part of this process. A human reliability assessment should be conducted for each level of operation based on current staffing and operation requirements at each project. The assessment needs to document the existing staffing at each plant for the internal performance factors such as years of experience, education background and training, operating room environment, stress levels and cognitive modes. A typical operator environment at a plant is shown in Figure 3. The external human factors should also include organizational performance factors such as management staff and corporate procedures or policies.

Fig. 3. Typical Plant Operators Environment

Step 5. Modelling of Operational System – As part of the USACE operational pilots, Steps 1 to 4 above are combined using simulation to examine the full range of the operational conditions (floods and external events) and the potential performance sequences (equipment and humans) that could lead to unfavourable events. While typical safety PRAs examines the likelihood of single events, this combination of unlikely events are captured in the outputs of the simulation and can then be examined more closely to assist with the mitigation of risks over various levels. The following example demonstrates the operational risks from one of the USACE pilots.

2. USACE Operational Risk Pilot

John Day Lock and Dam was built between 1958 and 1971 as one of the projects which is part of the Federal Columbia River Power System (FCRPS) in the Pacific Northwest of the United States. The project has a hydroelectric plant with 16 Francis turbines with total of 2,160MW generating capacity. The dam includes 1200-foot-long spillway with 20 Tainted gates that allow an annual flow capacity of over 2 million cubic feet per second, a 100-foot-high navigation lock (highest lift in the United States) and two adult and one juvenile fish ladders along both sides of the project. The layout of the John Day Project is shown in Figure 4.

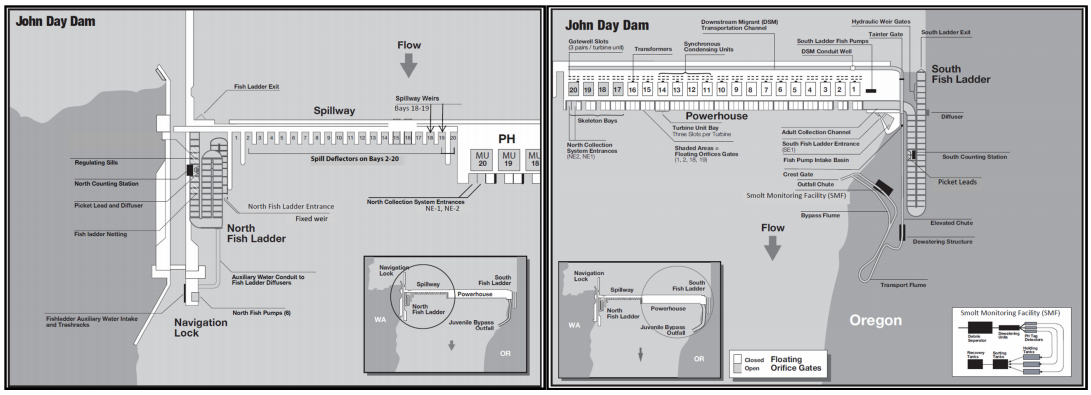

Fig. 4. Operational System at John Day Dam

As part of the USACE operational pilots, the GoldSim™ simulation platform is used to model the behaviour of the spillway and hydropower plant components during all phases of plant operations. The operational system model is shown in Figure 5 (main system model and gate control models) and reflects the inflow of water into the reservoir (on the left side of the inputs) to the output functions (gate operations on the right side). Many outputs can be represented by this simulation platform and some of these outputs for water control and gate reliability are shown in Figure 6.

The complexity of the operational model is represented by the inclusion of an element for each of the twenty spillway gates. Each gate is defined with fault tree structure and modelled using Weibull distributions to reflect the time dependent reliability of each gate and overall spillway system. The same level of complexity is used to model the other major systems (lock and hydropower plant) as well. Plant operations and human reliability will be included through the fault tree nodes to model the correct operation of each of the components.

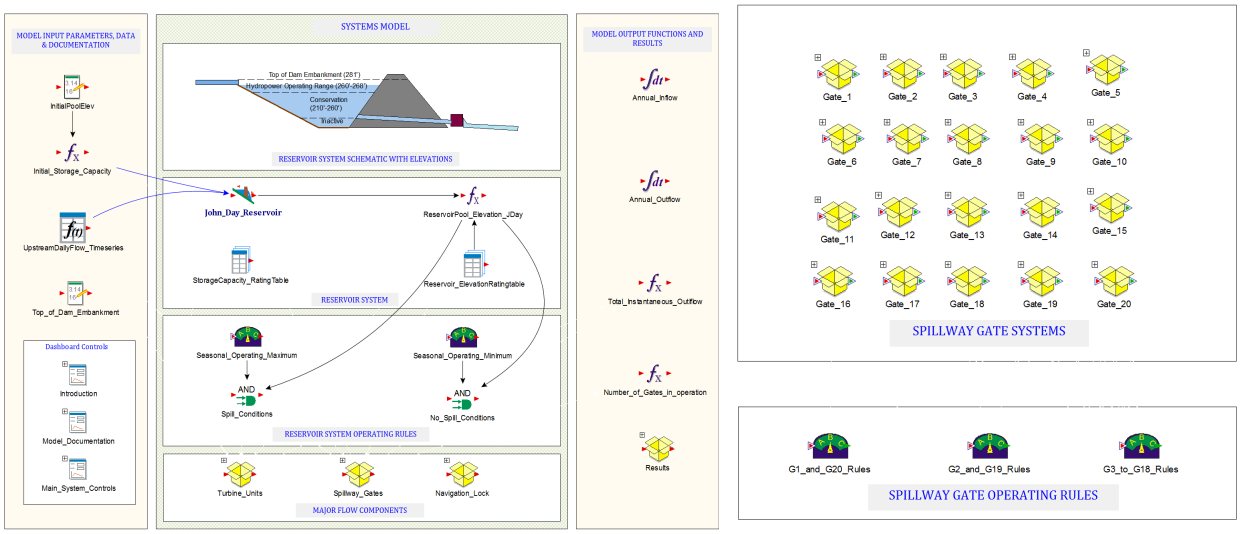

Fig. 5. Systems Model and Gate Model for John Day Lock and Dam

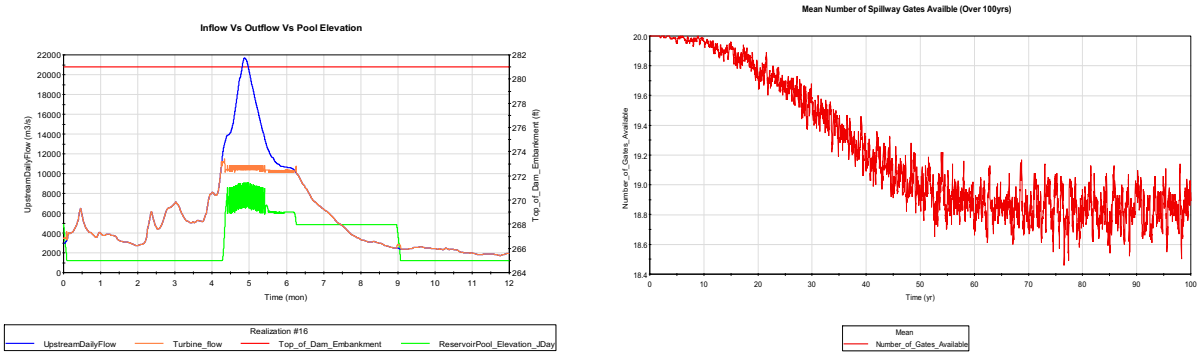

Fig. 6. Example Outputs (Inflows and Reservior Elevation (left) and Mean Number of Gates available (right)) from Systems Model for John Day Lock and Dam

3. Conclusions

Modelling of complex systems are important to understanding the operational risk associated dam and hydropower plants. The steps defined in the USACE pilot program are still being developed and tried over a full range of dam and hydropower plants to fully capture the risks that are present at USACE facilities. The inclusion of human reliability aspects is important to show that humans do make errors that can affect the potential performance of dam and hydropower facilities. These operational risk pilots using simulation can highlight areas in the system that will require a more focused assessment or direct mitigation of risk to lower the operational risks,

References

Becher, G., Hartford, D., Zielinski, A., Patev, R., Ascila, R., and Rytters, K. (2016). Operational Safety in Dams and Reservoirs – Understanding the reliability of flow control systems. Institution of Civil Engineers Publishing, London, UK.

Chandler, F., Chang, J., and Mosleh, A. (2006). Human Reliability Analysis Methods Selection Guidance for NASA. OSMA Technical Report, NASA, Washington DC.

Chang, Y. H. J., and Mosleh, A. (2007). "Cognitive Modelling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents – Part 1 Overview of IDAC Model." Reliability Engineering & System Safety, 92, 997–1013.

GoldSim™ User's Guide (2016). Golder and Associates, Seattle, Washington.

Patev, R. (2015). "Development of Utility Functions and Aspiration Levels for Multi-Purpose Inland Navigation Projects'. PIANC Smart Rivers 2015 Conference, Buenos Aires, Argentina.

Patev, R. C., and Putcha, C. S. (2005). "Development of Fault Trees for Risk Assessment of Dam Gates and Associated Operating Equipment." International Journal of Modelling and Simulation, 25(3).

The Authors

Robert C. Patev serves as the National Risk Advisor to the Director of the Risk Management Center, US Army Corps of Engineers (USACE). In his current capacity, he supports Headquarters USACE, Divisions, Districts and other federal agencies in the development of methodologies for risk and reliability assessment of Civil Works Infrastructure Projects. Mr. Patev currently consults on international risk projects with other governmental agencies all over the world including Canada, Sweden, Panama, Germany, Netherlands, France, UK and Belgium.

Adiel Komey is a doctoral candidate in civil engineering at the University of Maryland and holds a BSCE from Kwame Nkrumah University of Science and Technology, Ghana. He has consulted widely in the hydropower and dams industry, including to Ontario Power Generation, DC Water and Sewer Authority, the US Army Corps of Engineers, and the Volta River Authority.

Gregory B. Baecher is Glenn L Martin Institute Professor of Engineering at the University of Maryland. He holds a BSCE from UC Berkeley and a PhD in geotechnical engineering from MIT. He is the author of five books on risk, safety, and the protection of civil infrastructure, and is a member of the US National Academy of Engineering.