THE TAUM SAUK DAM FAILURE WAS PREVENTABLE — HOW DO WE PREVENT THE NEXT OPERATIONAL DAM FAILURE?

David W. Lord, P.E.¹

ABSTRACT

Taum Sauk Dam in Missouri overtopped and failed in December 2005. A number of factors contributed to the failure, including the lack of a spillway, changes to the project that decreased the already minimal freeboard, a lack of understanding of the original and current design basis of the project, inadequate electrical/mechanical equipment and controls, and an inadequate owner’s dam safety program (ODSP). Potential failure modes (PFMs) related to these factors are best described as operational failure modes. The risk of these types of failures is increasing because of operational changes at dams, caused by deregulation of utilities, environmentally required changes, and the increasing numbers of remotely operated dams. This paper discusses how the lessons learned from the failure of Taum Sauk Dam can be used to evaluate and protect all dams from overtopping failures.

Completing rigorous risk analysis procedures for operational PFMs often requires a very personnel and time-intensive process. Even with these rigorous procedures, many of the interactions of these complex systems will be missed because linear risk analyses cannot consider every interaction. Systems engineering does consider these interactions, but does not yet provide a fully developed framework for evaluating overtopping PFMs of dams like the risk procedures do. Dam owners need a simplified framework to begin to evaluate and manage operational failure modes without missing the complexity inherent in these systems. The framework should be broad enough to include very simple to very complex evaluations depending on the vulnerability of the dam to an overtopping failure. This paper proposes such a framework.

This overtopping protection framework (developed from the Pumped Storage Hydro-Electric Project Technical Guidance, October 5, 2007 and new FERC ODSP procedures) can be used to assess the vulnerability of projects to operational PFMs. The framework includes general procedures for analyzing the specific vulnerabilities of each dam and for reducing the likelihood of these types of failures. Using a combination of monitoring and rigorous management policies, the framework could prevent dam failures without needing to know the specific failure path or set of interactions that might cause a failure. Combined with guided use of risk analysis procedures, this could significantly reduce the risk of these failures.

¹ Senior Civil Engineer, FERC, Division of Dam Safety and Inspections, Portland Regional Office, 503-552-2728, david.lord@ferc.gov

Preventing Operational Dam Failures
INTRODUCTION

The Taum Sauk project (FERC No. 2277) is located in Reynolds County, Missouri on the East Fork of the Black River. It is a reversible pumped storage facility consisting of an upper man-made reservoir and a lower storage reservoir. Built in 1963, the Upper Dam was an 84-foot high, hilltop ring-dike forming a kidney shape with a total crest length of 6,562-feet. A 10-foot high reinforced concrete parapet wall ran along the crest, raising the crest altitude to El. 1,599 feet. The dike was a concrete-faced rock-fill dike until a geo-membrane liner was added in 2004.

The Upper Dam is connected to the 450 MW Powerhouse by a 26.2-foot diameter vertical shaft which flows into one-mile long tunnels. The Lower Dam, a concrete gravity dam, is a maximum of 60 feet high by 390 feet long. The Powerhouse is located at the upstream end of the Lower Reservoir, which provides storage for the pump-back operations. The Powerhouse was used as a peaking plant.

In December 2005, the Upper Dam (herein referred to as Taum Sauk Dam) was overpumped and the embankment failed. Although no one died, several people were in the dam failure inundation zone and were very lucky to survive. Figures 1 and 2 show the Project Location and Layout. Photo 1 shows an aerial view of the dam prior to the failure. Photo 2 shows the dam after failure.

Figure 1. Project Location Map
Cross section from original design drawings

Figure 2. Embankment Cross Section from Original Design Drawings

Photo 1. Taum Sauk Upper Reservoir Prior to 2005 Failure
Photo 2. 2005 Failure of Taum Sauk Dam

Photo 3. Overall view of Taum Sauk Development

2 Photos 1 through 3 taken from Lessons Learned at the Taum Sauk Rebuild, Paul Rizzo, Carl Rizzo, and John Bowen, USSD 31st Annual Conference, April 2011.
CAUSES OF TAUM SAUK FAILURE

Failure Investigation Reports – Technical Causes

Three failure investigation reports have been issued which thoroughly discuss the technical failure modes. For full discussion of failure modes refer to these reports. They are available on the FERC website under the Dam Safety and Inspections Division section and listed as references at the end of this paper. “In summary, these reports listed the following failure modes:”

Failure occurred because the 10-foot high parapet wall overtopped causing erosion of the downstream face of the dam (The toe wedge and the infinite slope stability were susceptible to saturation). One to two parapet sections failed first (the lowest one(s)), with the breach width reaching 656 feet wide.

The technical factors contributing to the failure included:

1. The reservoir was operated to within 1 foot of the lowest point along the dam crest and may have been routinely filled to within 0.25 feet of the lowest point.
2. The reservoir level control instruments were failing because of changes to the design during construction of the liner. The licensee attempted to fix this with a virtual fix by reprogramming alarm sensors.
3. The alarm (safety) sensors were physically located above the lowest point on the parapet wall.
4. Control programming was changed reducing the redundancy and increasing the time until the automatic shutdown would occur.
5. There were poor original construction practices leading to a dirty (erodible) rockfill.
6. There was no visual monitoring.
7. There was no overflow spillway.

Non-Technical Factors

The technical factors listed in the reports, while providing useful information, do not provide much insight into how a failure of Taum Sauk Dam could have been prevented or how to prevent similar future failures.

Organizational issues were included as a secondary contributing cause in one of the Failure Investigation Reports. Ameren signed a Settlement Agreement with the FERC on October 6, 2006 in which it agreed to add a new Owner’s Dam Safety Program (ODSP) in recognition that the existing program had been inadequate at the time of the failure.

Organizational factors that appear to contribute to the failure include changes to the project physical control systems and operating procedures that decreased the already minimal freeboard, an incomplete understanding of the original and current design basis of the project by personnel charged with implementing those changes, inadequate control of
contractors making changes to the project, and an inadequate ODSP, as mentioned above.

Another way of listing the factors related to the failure are as follows:

1. Instrumentation not designed, installed, or maintained adequately.
2. No visual backup or ground truthing of the monitoring.
3. Controls not designed, installed, or maintained adequately.
4. Changes to the design basis made without regulatory oversight.
5. Inadequate recognition of design flaws in dam, i.e., susceptibility to overtopping failure for a pumped storage dam without a spillway.
6. Inadequate freeboard.
7. Licensee’s dam safety program was not set up to recognize these problems.
8. Regulatory oversight was not set up to require an ODSP which required reviews of all safety and control systems whenever operational and organizational changes are made.

Following the failure a group of pumped storage owners was convened by the FERC to determine how to respond to the failure. Their first task was to conduct a fault tree analysis of the overtopping protection control schemes (OPCS) for each project. The results were presented at a conference held near the FERC Washington D.C. offices on November 1, 2006.

During that meeting, each owner pointed out any single source of failure of the OPCS that had been discovered at their projects in response to reviews conducted subsequent to the Taum Sauk failure. These single source failure modes had been addressed by changing the projects to include alternative sources of controls, instrumentation, power, or communications, etc. In addition, all projects had been revised to include cameras to visually monitor the pumping at the projects. At that meeting it was decided to continue the review process at a second meeting and to develop guidelines for pumped storage owners because of the understanding that there had been other similar failures, such as the failure of Upriver Dam in Washington State in 1985.

The second meeting was held on February 28, 2007. The result of this meeting, chaired by Mr. Warren Witt of Ameren, was to complete a document titled, PUMPED STORAGE HYDRO-ELECTRIC PROJECT TECHNICAL GUIDANCE (PSTG), Revision 0, March 7, 2007. This document will be discussed later in this paper.

**COULD THE TAUM SAUK FAILURE HAVE BEEN PREVENTED?**

Dam safety inspectors, looking at Taum Sauk Dam prior to 2005 would have seen a rockfill dam, thought to be relatively impervious to overtopping erosion, with a 10-foot-high parapet wall, 2 feet of freeboard and two sets of instruments to warn of a high reservoir level. One of these sets of instruments should automatically shut off the pumps.

---

The project had been operated for more than 40 years without apparent problems. The dam did not have a spillway, so reliable operation was counted on to avoid overtopping. How could someone, particularly someone untrained in hydro plant controls or operating systems, be able to detect problems at Taum Sauk?

The following is a set of procedures that a dam inspector might have developed and implemented based on knowledge of other similar failures:

1. Request the owner to provide an analysis of the lowest point on the dam parapet wall at the peak of the normal maximum water level. This should include visual observations and photographs of the location(s) of minimum freeboard at the maximum water level.

2. Request the owner to provide documentation of the historic maximum water levels. (Note that given the flaws in the pressure transducer system, this might not have shown much).

3. Actually be present during the end of the pumping cycles at the locations found in Item 1 to witness the actual freeboard present. Comparing this event to recorded values of the reservoir level would have been revealing.

4. Request the owner to conduct a physical test of the overtopping protection control scheme to determine whether it was in working order. This would have revealed that the OPCS was not working and raised questions about many issues.

5. Request the owner to provide an analysis of how long it would take to overtop the parapet wall, if the OPCS fails. Is it minutes, hours, or days?

6. Any freeboard under 3 -5 feet is questionable. For a dam without a spillway, the freeboard was not adequate. The owner could have been asked to provide a justification for why this freeboard was adequate.

7. When these issues are not satisfactorily answered, continue to ask questions until the problems are fully understood.

The above procedures if implemented may have prevented the failure. However, given the general lack of knowledge about overtopping failures during operation, it is understandable that the dam failure was not prevented. The Taum Sauk failure and the development of the PSTG have led to an understanding of these types of failures that should create awareness in the dam safety community of practices to be used to prevent similar future failures.

**PREVENTING FUTURE OPERATIONAL TYPE FAILURES**

A FERC mandated Potential Failure Mode Analysis (PFMA) was to be completed at the project, and may have revealed the problems that led to the failure. However, unless
someone who was familiar with operational failures, these issues may not have been discovered.

In the future, the FERC plans to begin completing risk analyses for many of its dams. This will create a framework that will make it more likely that operational type failure modes will be addressed to the extent possible by linear analyses. Good judgment by knowledgeable teams will be required to identify and describe the failure modes.

Even if the PFM is recognized, completing rigorous risk analysis procedures for operational PFMs often requires a very personnel and time-intensive process. Even with these rigorous procedures, many of the interactions of these complex systems might be missed because linear risk analyses cannot consider every interaction. At Taum Sauk, it is unlikely that anyone could have described each step of the actual failure mode that overtopped the dam prior to the failure. The control and instrumentation issues are too interrelated and complex. In addition, the organizational issues are rarely considered in risk analyses in the manner possible using systems engineering procedures.

Wikipedia defines systems engineering as an interdisciplinary field of engineering focusing on how complex engineering projects should be designed and managed over their life cycles. Issues such as logistics, the coordination of different teams, and automatic control of machinery become more difficult when dealing with large, complex projects. Systems engineering deals with work-processes and tools to manage risks on such projects, and it overlaps with both technical and human-centered disciplines such as control engineering, industrial engineering, organizational studies, and project management.

As discussed in a book by Professor Nancy Leveson in Engineering A Safer World, systems engineering does consider issues of interrelationships between instrumentation, and electrical and organizational control systems. However systems engineering does not yet provide a fully developed framework for evaluating overtopping PFMs of dams like the risk procedures do.

Accordingly, dam owners need a simplified framework to begin to evaluate and manage operational failure modes without missing the complexity inherent in these systems. The framework should be broad enough to include very simple to very complex evaluations depending on the vulnerability of the dam to an overtopping failure. This paper proposes such a framework.

**OPERATIONAL OVERTOPPING PROTECTION FRAMEWORK**

This overtopping protection framework (Framework) was developed from the PSTG and new ODSP procedures. The Framework can be used to assess the vulnerability of projects to operational PFMs. The framework includes general procedures for analyzing
the specific vulnerabilities of each dam and for reducing the likelihood of these types of failures. Using a combination of monitoring and rigorous management policies, the framework could prevent dam failures without needing to know the specific failure path or set of interactions that might cause a failure. Combined with guided use of risk analysis procedures, this could significantly reduce the risk of these failures.

**Framework**

The Framework includes the following steps:

**Overtopping Vulnerability Analysis.** Each hydroelectric project should complete a simple analysis to understand how long it would take for typical flows at the project to overtop the dam and cause a failure.

For instance, a canal flow could overtop an embankment dam within a short period of time if flow through the turbines abruptly stopped and the spillway gates were not opened as happened at the Upriver Project in 1985. Or, overpumping of the embankment could take a few minutes if the overtopping protection controls failed as happened at Taum Sauk.

On the opposite end, an arch dam that would take days for typical flows to overtop it would be invulnerable to overtopping erosion unless the abutments or toe were erodible.

More complex analyses would be needed for flood flows that might cause debris buildup in the spillways.

A chart should be developed showing the time to overtopping the embankment for any reasonable set of circumstances. This chart should be used to determine how vulnerable the dam is to overtopping and how much time is available to correct problems. If any problem that is reasonably foreseeable can be corrected prior to overtopping, the dam is relatively invulnerable to overtopping from an operational problem. For instance, power or mechanical issues at spillway gates can usually be fixed within a few days unless other issues prevent access, such as a large earthquake or flood. Another type of invulnerable dam is a one with a very large uncontrolled spillway that can handle all reasonable flows.

**Vulnerable Dams.** The chart should be used to highlight vulnerable dams. Dams with embankments that would overtop within a few minutes or hours are considered vulnerable to operational failure modes. Also vulnerable dams would include embankments with limited access to fix problems or a single source flaw, such as a failed gate hoist as the only source of operation that might take weeks to fix.

Even for larger floods, operational issues in handling debris or opening the gates could cause overtopping of the embankment. These issues would include redundancy of power and communications, potential for mechanical and electrical problems, access to the dam by operators, and owner’s organizational challenges or changes that result in not recognizing the problem in time.
For vulnerable dams, further analyses may be required. The more vulnerable the dam is, the greater the need for further analysis.

The PSTG document provides a useful guide for completing these analyses. The document is divided into three major sections, Design Basis, Organizational Processes, and Instrumentation and Monitoring Equipment.

**Design Basis.** The following section is taken from the PSTG:

“The design basis for a project should be clearly defined and understood by everyone involved in the project operation, maintenance, and modification. Because each project can address the below factors differently, the design basis for that project should be clearly documented in concise design basis documents or an operating design basis document (OBD). The design basis documents should discuss the hydrologic, hydraulic, and civil design basis issues that might relate to overtopping protection. Based on these hydraulic and civil design bases, the documents should then define the controls and control logic, timing of overtopping, operating cycle, and staffing levels.

The design basis documentation should discuss the overall fault tolerance or intolerance of the overtopping protection. A fault tolerant system would be one where the upper reservoir was very large compared to pumping capacity and the dam had an overflow spillway large enough to handle the Inflow Design Flood (IDF). Another fault tolerant system would be one with a dam and foundation that could handle extended periods of overtopping without failure. A fault intolerant system would be an embankment dam without a spillway with a small upper reservoir compared to pump capacity.”

The design basis section of the PSTG includes a general prescription to provide a “fail-to-a-safe-condition” design of the control system. If a part fails, it should fail in a way that provides a predicable safe outcome. An example would be to have the failure of a communication system provide an alarm showing that it has failed, so that other action can be taken.

Other factors under design basis ease of testing and calibration of controls, and the timing issues discussed above in the section on overtopping vulnerability analysis.

Redundancy of controls was also recommended by the PSTG, but systems engineering teaches that the more complex the system, the more potential for unforeseen interactions and the failure of the controls to perform as intended. Some redundancy of controls may be useful, but there are limits to the value of redundancy.

**Design Basis Changes.** Another part of the PSTG includes the following language:

“Accordingly, when the operational basis of a pumped storage facility has changed or
a change is being contemplated, the original design basis of the facility should be reviewed and the following items considered in order to assure the owner the safety of the facility has not been compromised to an unsafe level. The following items should be considered when making physical or operational changes at a project to assure that the operational basis is either; 1) not affected, or 2) the new operational basis provides sufficient levels of safety.

Do the proposed changes in the operating design basis result in increased probability of over-pumping due to an increased number of pump-generate cycles?

Do proposed changes in the operating design basis result in increased usage of equipment?

Do proposed changes necessitate changes to maintenance schedules (i.e. increased frequency of lubrication or inspections of mechanical equipment)?

Does increased start-stop cycling increase the probability of failure of electro-mechanical components such as switchgear, monitoring devices, etc?

Do proposed changes in staffing result in a reduction of dam visual monitoring?

Is an increase in instrumentation prudent to offset a reduction in visual monitoring?

Does a change in remote operation require an enhanced training program so that remote operators are familiar with key safety issues at the project such as the potential failure modes, the emergency action plan, the potential impacts of adverse operations, etc?

The above list is not all inclusive, but is intended to encourage thinking about the potential impacts of design basis changes on the safety and reliability of projects.”

Another part of the evaluation of design basis changes includes whether the dams are remotely operated and whether visual observation is possible.

An example of the start of a design basis analysis can be seen in a chart, Figure 3, provided in a paper by Mr. Patrick Regan. This chart is an example of developing an original design basis for Taum Sauk dam and then tracking the changes to the design basis through the history of the project to failure. Using this tool, one can see each of the design basis changes, i.e., this is another way to see the factors that led to failure.

Incorporating such an analysis at vulnerable dams can help a reviewer to see if the dam is

---

5 Project Operational Basis and System Design, Patrick Regan, Hydrovision International Conference, July 2011
still being operated consistent with the original design basis and whether that original design basis is still true to what is currently known about the dam. That is, the analysis may reveal flaws in the design basis. Then we can see if changes to the design basis have been adequately accommodated by changes in operation and monitoring of the dam.

![Figure 3 – Design Basis Analysis](image)

**Instrumentation and Monitoring.** For full discussion of these issues, refer to the PSTG. The most critical issue is kind and frequency of testing of overtopping protection control schemes (OPCS) as taken from the PSTG. The determination of whether the OPCS should be functionally tested or simulated is discussed as follows:
“This determination should be based on the project’s design basis and the fault tolerance of this basis. For projects that are relatively fault intolerant, functional testing is the preferred method of testing over-topping protection systems. If possible the reservoir should be allowed to rise to trigger alarms and pump/turbine shutdown systems. If there are significant problems that would prevent functional testing, every attempt should be made to simulate a functional test. However, an engineering evaluation of the reasons for choosing the simulation test should be made prior to concluding that a functional test will not be performed. If dam safety concerns are the reason a functional test is not chosen, the alarm and shutdown levels are possibly set too close to the top.

The functional test should be performed at least once per year.”

In addition, the instrumentation and controls should provide an adequate picture of the potential problems at the dam. Without this, the operators will not be able to respond appropriately to those problems.

Organizational Processes. Again from the PSTG:

“Adequate organizational processes should be in place at Pumped Storage projects so that reservoir levels can be properly controlled and managed. These processes are necessary to ensure a consistent and systematic approach to quality related activities which could affect reservoir level controls/protection and thus public and dam safety. Four of these key processes are training, operating procedures, design change/configuration control, and the organization structure.”

This is the part of failure prevention that is farthest from the comfort zone of typical dam safety engineers trained in civil engineering. As can be seen at Taum Sauk and many other failures, the weakness or strength of the ODSP has a large impact on whether failures occur or not.

The PSTG presents a fairly detailed review of how good organizational processes are needed at pumped storage projects, which is not repeated here. What is apparent in this review is that operational failure modes are particularly resistant to linear analyses. Without a robust ODSP, it is difficult for most outside observers to catch all of the issues that might lead to an operational failure. In contrast, it is very likely that a properly trained and supervised operations staff would understand enough to catch most problems.

Owner’s Dam Safety Program. Another primary issue is whether problems can be reported to levels high enough in the organization to be given the proper hearing. An overtopping occurred at the Taum Sauk Dam in September 2005 that should have alerted the owner to the problems that occurred in December 2005. However, operational needs were thought to be more important than resolving problems with the controls. Obviously, in hindsight, they were not.
The figures listed below are again taken from Mr. Patrick Regan. They show the relationship between an inadequate ODSP and a good program. Figure 4 shows the march toward failure using several factors, for example, design and construction flaws as well as operational and organizational factors such as the ODSP as they existed throughout the project history. Figure 5 shows how a good ODSP is likely to have led to decisions that would have prevented the failure of Taum Sauk.

**Figure 4, Taum Sauk Issues that Led to Failure – From Patrick Regan**

In the 1968 letter shown on Figure 4, the owner advises the Federal Power Commission that they don’t need to install the spillway recommended by their consultant because the dam can’t fail.

**Figure 5, Taum Sauk If ODSP Had Been Robust – From Patrick Regan**

These figures were taken from a webinar discussion with federal agency staff that was to be presented in January 2012. Technical difficulties caused the webinar to be delayed until it can be rescheduled. A detailed discussion of these charts is beyond the scope of this paper and will be discussed in a future paper by Mr. Regan.
Organizational Levels of Control. Systems engineering provides tools for evaluating the various levels of control of a system. This includes the various operational control levels of the owner, including who is responsible for what parts of the control system, from the operators to the CEO. Many failures can be attributed to failure of one or more level of organizational control or the failure to communicate between levels. Using a systems engineering approach which includes evaluating the mental models of the people in these control levels can be helpful in understanding these relationships. To adequately understand how to prevent dam failures, our industry needs to begin to develop procedures for organizational levels of control, in addition to technical controls.

The following chart, Figure 6, is taken from the Ameren Settlement Agreement and shows how the Owner’s Dam Safety Engineer provides annual certification of safety to the Board and CEO. He or she can bypass lower levels of authority if people at those levels are not adequately responding to serious dam safety problems.

Figure 6. Ameren Owner’s Dam Safety Communication Flowchart

Improvements in ODSP procedures and owner’s initiatives to improve training and their organizations will help to prevent dam failures, but a fully robust systems procedure is needed for vulnerable dams. Until we have more developed procedures, the Framework can be used.

Framework to Prevent Operational Dam Failures. Summarizing the discussion above:
1. All dams should be evaluated for their vulnerability to overtopping from operational failure modes.

2. The more vulnerable dams should be further evaluated using the procedures described above as follows:
   a. Complete a design basis document for the project.
   b. Evaluate the changes to the design basis to determine if an adequate overtopping protection control scheme is in place.
   c. Evaluate the adequacy of the instrumentation and monitoring and the testing of those systems.
   d. Evaluate the adequacy of the ODSP and the ability of the owner to respond to alarms and problems.

3. Provide a well thought out system to control the reservoir including appropriate levels of organizational control and interactions between levels.

**CONCLUSIONS**

The lessons learned from the failure of Taum Sauk Dam can be used to evaluate and protect all dams from overtopping failures.

Linear risk analysis procedures while potentially beneficial for operational PFM s will be of limited value in evaluating the many interactions of these complex systems. Systems engineering evaluates these interactions, but does not yet provide a fully developed framework for evaluating overtopping PFMs of dams as the risk procedures do.

This paper proposes a simplified Framework to begin to evaluate and manage operational failure modes without missing the complexity inherent in these systems. The Framework should be broad enough to include very simple to very complex evaluations depending on the vulnerability of the dam to an overtopping failure.

This Framework includes general procedures for analyzing the specific vulnerabilities of each dam and for reducing the likelihood of these types of failures. A current design basis document should be completed for vulnerable dams and used to evaluate operational changes to the project. The owner should evaluate the adequacy of the instrumentation and monitoring and the testing of the systems to control the reservoir level. The ODSP should be evaluated as well as the level of controls in the organization.

Using a combination of monitoring and rigorous management policies, the Framework could prevent dam failures without needing to know the specific failure path or set of interactions that might cause a failure. Combined with guided use of risk analysis procedures, this could significantly reduce the probability of these failures occurring.