Senior Leaders
Dam Safety Seminar
Understand Risks

“Quality (risk) analysis could both facilitate two-way communication between top management and individuals with substantial knowledge about each of the relevant aspects of utility operations and provide a clear understanding of all the information available to make a key risk management decision.”

Leadership

“The critical common element is an unwavering commitment to safety at the top of an organization: the CEO and board of directors must create the culture and establish the conditions under which everyone in a company shares responsibility for maintaining a relentless focus on preventing accidents.”

(The accidents they are talking about are not OSHA accidents)

National Commission on the BP Deepwater Horizon Oil Spill (2011)
“Likewise, for the entire industry, leadership needs to come from the CEOs collectively, who can apply pressure on their peers to enhance performance.”

National Commission on the BP Deepwater Horizon Oil Spill (2011)
Outline

How Dams Fail – A Historical Perspective
Consequences of Dam Failures
Organizational and System Failures
What Dam Safety is Not
What Dam Safety is Not

A Compliance Exercise
What Dam Safety Is

A Legal, Ethical, & Moral Responsibility
Each licensee hereunder shall be liable for all damages occasioned to the property of others by the construction, maintenance, or operation of the project works or of the works appurtenant or accessory thereto, constructed under the license and in no event shall the United States be liable therefore.”
H.R. 3753

SECTION 1. FINDINGS.

The Congress finds that actions by the Federal Energy Regulatory Commission (‘FERC') leading to the acceptance and approval of the surrender of a hydroelectric license for Project No. XXXX, including, but not limited to, the FERC's failure to ensure, during the effective period of the issued hydroelectric license, that the project's facilities were adequately maintained, rendered the project unfit for operation and thereby wasting the hydraulic potential of waters of the United States.
“Engineers shall hold paramount the safety, health and welfare of the public and shall strive to comply with the principles of sustainable development in the performance of their professional duties.”
FERC Dam Safety Program
Regional Organization
Breadth

- Over 2900 jurisdictional dams
- 800 High Hazard Potential Dams (likely to cause loss of life in a failure)
- 200 Significant Hazard Potential Dams (likely to cause significant economic and/or environmental consequences)
- Heights from 0.5 feet to 770 feet
Oroville Dam
California
770’ high
Earthfill
Boundary Dam
Washington
340’ high
Concrete Gravity-Arch
Shoshone Diversion
Idaho
1.5' high
Concrete Gravity
Swift 1 Dam
Washington
412’ high
Earthfill
Wishon Dam
California
260’ High
CFR
Hells Canyon Dam
Idaho
323’ high
Concrete Gravity Dam
Principal Elements of Program

- Owner’s Dam Safety Program
- Inspections
  - Owner’s
  - FERC
  - Independent Consultant (Part 12D)
- Potential Failure Mode Analysis/ Risk Assessment
- Surveillance and Monitoring Plans and Reports
- Emergency Action Plans
- Analysis
- Security Assessments
- Public Safety Programs
How Dams Fail

A Historical Perspective
Concrete Gravity Dams
Austin Dam (PA) – Sliding on Foundation
St. Francis Dam (CA) Abutment Failure
Ashley Dam (MA) Piping of Foundation
Concrete Arch Dams
Gleno Dam (Italy) Overtopping and Sliding
Vaiont Dam (Italy) Landslide into Reservoir
Sweetwater Dam (CA) Abutment Failure
Earthfill Dams
Noppikoski Dam (Sweden) Overtopping
Lower San Fernando (CA) Liquefaction
Banquiao (China) Overtopping
Southfork (PA) Overtopping
Rockfill Dams
Taum Sauk (MO) Overtopping
Dam Failure Statistics
The average annual probability of a given dam having a failure is about $1 \times 10^{-4}$ per year.
For dams built in the United States before 1959, on the average one in fifty failed.
Annual Probability of a Dam Failure in a Portfolio of Dams

Depending on how many dams you own the annual probability of a having a dam failure varies widely.

- 1 dam 1 in 10,000
- 10 dams 1 in 1,000
- 50 dams 1 in 200
- 100 dams 1 in 100
To answer the question as to does 50 years of "successful" operation mean we don't need to worry about a dam any more, the data suggests that >50% of incidents of dams that survived their first 5 years occur after the dam is 50 years old.
How are Incidents for Different Types of Dams Distributed?

% of Incidents That Occur At An Age Greater Than

By Type of Dam

- Earthfill
- Rockfill
- Gravity
- Arch
- All

Age

%
% of Incidents that Occur at an Age Greater Than by Failure Mode After 1st 5 Years of Operation

Flooding
Seepage
Structural
Dam Safety Evaluation (Traditional)
Is the dam here today? (check static stability)

Will the dam be here after a big storm? (check spillway capacity)

Will the dam be here after a big earthquake? (Check seismic stability/potential for liquefaction)
Current State of Practice

- Standards
  - Broadly Drawn – can’t recognize uniqueness of each dam
  - Generally don’t address issues that can’t be analyzed (Operational issues, Human Factors)
  - Singular – can’t address combination of events
  - May work against ALARP principle
Current State of Practice

- Risk-Informed (as generally practiced)
  - Linear
    - doesn’t address parallel events
    - doesn’t address interactions of “separate” systems
  - Subjective – Rely on expert elicitation
    - Good News – we don’t have a lot of failures
    - Bad News - Don’t have a lot of data to make informed estimates of probabilities
The Federal Aviation Administration has a requirement that “no single failure or probable combination of failures during any one flight shall jeopardize the continued safe flight and landing of the aircraft.”
In the dam safety community we do the first part, examining a single failure, fairly well.

In few instances do we adequately address the combination of failures – the system failures.

An example is the thought that we don’t need to simultaneously consider earthquake and flood loading. What we often overlook is the fact that if an earthquake severely damages a critical component such as a spillway, we only have until the onset of the next rainy season to repair the damage without endangering the dam and the population at risk.
What Are We Seeing Today?
The Taum Sauk Project is located on the East Fork of the Black River approximately 90 miles southwest of St. Louis, Missouri.

Taum Sauk is a pumped storage project owned by AmerenUE. It was the first large pumped-storage project to begin operation in the U. S.

The project includes an upper reservoir, a shaft/tunnel water conduit, a 450-MW PH with two pump-turbine units, and a lower reservoir.
Taum Sauk

- Dam Type: Concrete-faced rockfill
- Dam Height: 84’
- Reservoir Capacity: 4350 ac-ft
- Spillway Capacity: N/A
- Pumping Capacity: 5258 cfs
- Flood of Record: N/A
Construction

- The dike was topped with a 12’ layer of rock placed in 4’ lifts and compacted with a vibratory roller. The crest was 12’ wide.
- The 10’ high parapet wall was cast in place on top of this layer.
- The shotcrete face slab had a design thickness of 10 inches with No. 7 bars at 12 inches both ways.
- The face slab was placed in 60’ wide panels.
- Expansion joints used 3/4-in asphaltic expansion joint material and U-shaped copper water stops.
- A reinforced concrete plinth was placed at the toe of the concrete face.
Settlement

- Settlement of the rockfill varied between 1 and 2 feet with the lowest area at Panel 72, where the top of the parapet wall was 1596.99. (Original top of wall was El 1599)

- Several other panel areas ranged in elevations from El 1597 to 1598. (November 6, 2004 survey data)
Leakage/Seepage

- Leakage from the Upper Reservoir was a problem, beginning in September 1963, only a few months after first filling.
- Seepage suddenly increased to 103 cfs requiring emergency repairs including; excavation, grouting, a concrete cutoff, joint repairs and plugging two holes in the floor with concrete at panels 91 and 92.
- Three days later additional leakage caused another shut-down and repair. The repair consisted of excavating a 230’ long by 4’ wide trench excavated to “rock” and backfilled with concrete at Panels 90 to 93 and 95.
Leakage/Seepage

- Additional repairs were made in subsequent years, mostly on leakage through the horizontal and vertical joints in the concrete facing.
- Particular emphasis was on the joints between the concrete facing and bedrock, the joint at the toe of the parapet section, and the joint between the concrete facing and plinth.
- Leakage increased significantly (40 to 100 cfs) after an extended outage in 1999 due, in part, to more frequent cycling of the facility.
- To reduce seepage, a geomembrane liner was installed in 2004, significantly reducing the leakage to about 5 cfs.
Typical Project Operation Prior to Deregulation

- The Taum Sauk facility was operated about 100 days a year prior to deregulation of electric power markets in the 1990’s.
- Pumping generally occurred only on weekends.
- Only one pump was used for pump-back.
Typical Project Operation After Deregulation

- The change in the market made it profitable to run the facility around 300 days a year.
- The pump/turbine units were upgraded in 1999, a decision likely influenced by deregulation, increasing the efficiency and profitability.
- The new pump/turbine runners had a maximum pumping flow of 3,000 cfs per unit compared to 2,450 cfs per unit for the original runners.
- Two pumps were used for pump-back.
- In total the probability of over-pumping increased 15 times
Typical Project Operation After Deregulation

- A typical daily cycle in the summer was to generate in the morning, pump back in the afternoon, generate in the evening, and pump back again in the early morning.

- Generation and pump-start and duration was determined by system needs and controlled from Ameren’s Osage Plant.
Other Changes in Plant Operation

- In the 1967 safety report, J.B. Cooke recommended visual oversight of all pumping operations. UE implemented the recommendation.
- Between 1968 and 2005 UE ended visual oversight of pumping.
In 2001 Ameren prepared plans to install an 80-mil reservoir liner in order to reduce leakage.

The liner was anchored about 1 ft below the top of the parapet wall and near the top of the upstream plinth.

As part of the “project improvement” the old reservoir control systems were replaced by a new system in November of 2004.
Remediation

The original reservoir monitoring system consisted of:

- (1) three Warrick conductivity sensors at elevations 1591.00, 1596.0 and 1598.0,
- (2) a float riding on a cable guided roller assembly in a pipe to monitor upper reservoir levels for normal shutdown of the units, and
- (3) a set of mercury switches tied to a float in a stilling well for High and High-High backup pump shutoff.

The system components were anchored to the dam.
Remediation

- In 1994, a differential pressure transducer was added to provide secondary level indication.
- In 2000, the original skate system, encoder, and chart recorder were replaced with a differential pressure level transducer, PLC, and a digital level indicator at the upper reservoir.
- A staff gage attached to the parapet wall allowed calibration of the instrumentation.
- Because the staff gage was fixed to the parapet wall, it settled along with the wall. Ameren believes that, due to settlement, the upper reservoir was actually operating at El 1595 instead of El 1596.
Remediation

- The over-pumping protection systems were replaced during installation of the liner in 2004.
- Four 4-inch-diameter High Density Polyethylene (HDPE) pipes, to house the pressure sensors, were placed down the upstream slope of the dike at parapet wall panel 50.
- The new system was not anchored to the concrete face because it was decided that the new liner should not be penetrated by anchor bolt holes.
Remediation

- Stability of the HDPE pipes was provided by a system of unistrut sections, steel bolts, turnbuckles, jam nuts, eyebolts and U-shaped cable lock bolts tied to two stainless steel cables.
- The cables were anchored only at the plinth and at the base of the parapet wall.
- Down slope movement of the HDPE pipe assembly was limited by clamps placed on the cable just below the eyebolt connection to the pipe assembly.
- No restraint to upslope movement was included.
Remediation

- At the time of the failure, the upper reservoir control system consisted of two sets of sensors sending signals through three independent PLCs.
  - One set of sensors were two Druck pressure transducers used to monitor reservoir levels
  - The second set of sensors consisted of four Warrick conductivity sensors.
    - Two of the Warrick sensors (HIGH and HIGH-HIGH) were to determine if water levels in the upper reservoir were too high.
    - The other two Warrick sensors were to determine if water levels in the upper reservoir were too low.
    - Activating these sensors would start a hard shutdown of the generator/pump units.
 Remediation

* At the time of the breach the elevations of the Warrick sensors were 1597.4 (HI) and 1597.66 (HI-HI), respectively.
* The staff gage was removed.
* Due to several “false” shut-downs, the Warrick sensors were rewired in parallel rather than series, thereby requiring both sensors to activate prior to initiating a pump shut-down.
Prior Overtopping

- On September 25, 2005 Ameren employees observed water pouring over the parapet wall along the northwest portion of the reservoir, describing the incident as resembling “Niagara Falls.”

- The operators manually shut down the pumps and turned on the generating units to lower the reservoir.
The plant operator sent an e-mail to his supervisors on Sept. 27th warning them about continued overtopping of the upper reservoir after the second overtopping incident.

“Overflowing the upper reservoir is obviously an absolute 'NO-NO,'" "The dam would severely erode and cause eventual failure of the dam...“ and “If water continued to spill over the top of the wall, it could cause a section to collapse and then it would be all down hill from there — literally.”
Remediation

- After installation of the liner and new reservoir level measuring instruments in 2004, but before October 2005, the 1st pump off and 2nd pump off were set at El 1594 and 1596, respectively.
- In October, 2005 Ameren noticed movements of the HDPE pipes housing the pressure sensors.
- After October 2005, the first pump off was set at El of 1592 and the 2nd pump off at El 1594.
- At El 1594.2, shutdown for both pumps was to be initiated if they were not shutdown already.
- Unfortunately, Ameren did not know with certainty how much the sensors had moved.
The Upper Reservoir of the Taum Sauk Pumped Storage Project was overtopped during the final minutes of the pumping cycle on the morning of Dec. 14, 2005. Data indicate that pumping stopped at 5:15 AM with the initial breach forming at about the same time. Once overtopping began, erosion started at the downstream toe of the 10’ high parapet wall. Erosion progressed below the parapet wall, likely causing instability and resulting in the initial loss of one or two parapet wall sections.
Subsequent erosion and breach of the rockfill embankment formed a breach about 656’ wide at the top of the rockfill dam and 496’ at the base of the dam. The peak discharge from breach was about 273,000 cfs which occurred within 10 minutes of the initial breach. The complete evacuation of the reservoir occurred within 25 minutes.
Consequences

- Downstream of the breach was Johnson Shut-Ins State Park, a popular recreation area that draws nearly 250,000 visitors annually.
- The flood wave swept down Proffit mountain causing extensive erosion and environmental damage.
- The flood wave passed into the Black River causing inundation and extensive damage to the State Park.
Consequences

- The consequences from the failure could have been far worse had it occurred at a different time of year.
- The failure occurred around 5:15 AM with flood waters quickly reaching the park.
- Fortunately, the campground was empty during the middle of December, resulting in no deaths.
- Hundreds of sleeping campers may have perished in the state park campground had the failure occurred on a busy summer weekend.
A Systems Perspective of the Failure
Contributors to Failure

Design

- Large pumped storage was new technology
- Dumped Rockfill
- Steep slopes
- Didn’t take advantage of new state-of-practice
- Water stored on 10’ high parapet wall
- No spillway
- Reliance on control system to prevent over-pumping
- Control system placed near intake/outlet
Contributors to Failure Construction

- Fines were left in the fill – especially at the closure section
- Failure to remove all substandard material from beneath dam footprint
- Outer shell of the dike contained more sandy and pebble sized materials in the closure section
Contributors to Failure Performance History

- Excessive settlement, lowest point 2’ lower than design
- Large (4-5 inches) offset of parapet wall sections – torn waterstops?
- Excessive seepage
- Joint opening
Contributions to Failure
Operation History

- Deregulation
- Change from 100 days/yr to 300 days/yr
- Change from 1 pump cycle/wk to 2-3 cycles/day
- Change from 1 pump to 2 pumps
- Upgrade pumps from 2,450 cfs to 3,000 (20% increase)
- Visual surveillance of pumping to none
- Failure to take action after earlier over-pumping events
Contributions to Failure Remediation

- Design of revised water level control system didn’t consider settlement of parapet walls or the affect of the inlet/outlet vortex
- Sensor pipes not fastened to dam
- Staff gage removed
- Changed winter operation from -2 feet to normal full pool
- Misplacement of emergency shut-off sensors (above lowest point on wall)
- Wiring Warrick sensors in parallel
- Uncertainty in sensor movement
Figure 2 – Interaction Flow Chart – Taum Sauk Upper Dam Failure
Operational Failure Modes

- Can you get there?
- Will it Work?
- Stuff Happens – Just don’t let it happen to you!
Operations Potential Failure Modes

- In extreme events such as floods or earthquakes access to a dam may be cut off and power lines, microwave reflectors, radio towers may be knocked out.

- Example
  - Gates are local operation only.
  - Access to dam is prevented during floods due to inundation of access road
SCADA Issues

- Supervision Control And Data Acquisition (SCADA) systems are becoming more common as owners react to cost pressures by reducing staff, remotely operating units and automating data acquisition.
- License and grid conditions often require owners to more accurately control their units.
- SCADA system failures have contributed to several incidents and failures including Taum Sauk Dam.
SCADA Failures

- Failure to Open on Demand
- Failure to Close on Demand
- Closure without Demand
- Open without Demand
Events Leading up to Incident

- During high flows the Cowlitz Falls project is required to flush sediment through low level outlets to prevent flooding upstream.
- The design of the dam has the low level outlets beneath the radial gates.
- The control system is designed to NOT allow the sluice gates to open while the spill gates are open due to excessive vibration in the sluice gates.
Events Leading up to Incident

- In 2003, the Cowlitz Falls project was undergoing a SCADA upgrade.
- An early storm had Cowlitz Falls spilling.
- Without operator intervention, the sluice gate opened, bypassing both the intent of the SCADA system and a PLC designed to lockout the sluice when the spill gate was open.
Lessons Learned

- Automated supervision, control and data acquisition (SCADA) systems pose some serious dam safety issues
- Need for careful and thorough testing
- Can’t test all possibilities – only test what you can think of
- Need for keeping documentation current
- Need for operator training after initial installation and subsequent updates
Operations Potential Failure Modes

- Change in gate operations from a few times a year to daily (for fish passage)
- Lubrication schedule remained the same.
- Gearbox stripped, gate dropped on one side
Folsom Dam Gate Failure
Static Failure Modes
Contributing Factors

- Lack of Gate Maintenance
- Gate Binding
- Concrete Deterioration in Crest Structure or Chute
- Improper Construction
Lack of Gate Maintenance

- Corrosion of key gate members or components, reducing member capacity
- Reduced reliability of back-up power supplies
- System problems not identified by regular exercising of gates
Rivet heads deteriorated
Consequences

- The spillway at Palagnedra Dam was completely blocked with debris.
- Water spilled over the main concrete dam and through a low spot upstream on the right bank.
- 50,000 cu meters of glacial moraine material was washed out from the downstream side of a 40 m high diaphragm wall upstream on the right side of the reservoir nearly causing failure of the wall.
Logbooms

- Logbooms may not be adequately strong to withstand large rafts of debris
  - Forces on anchorage is very large
  - Connections are often weak link
- Failure of a logboom may make things worse by allowing debris to knit together rather than passing singly over dam
Lessons Learned

- Spillway blockage due to debris is NOT an uncommon problem
- Narrow spillway openings can be a critical failure mode
- Logbooms are not necessarily the answer and can make things worse
Can You Get There?
Heading west
Can a Problem in a PH Cause a Dam Failure at a Remote Project?
Sayano-Shushenskaya
Sayano-Shushenskaya

- **Dam Type:** Gravity Arch
- **Dam Height:** 242 meters / 794 ft
- **Reservoir Capacity:** 31.3 km³ / 25.4M ac-ft
- **Spillway Capacity:** 12,800 m³/s / 455K cfs
- **Powerhouse Capacity:** 3,500 m³/s / 124K cfs
- **Flood of Record:** 24,300 m³/s
Sayano-Shushenskaya

- No low-level outlet – maximum draft 45 m
- Est. storage volume in top 45 m – 18.1 cu km
- No TSV on the penstocks
- Reservoir filled as dam was raised
- Upstream monoliths raised first
Sayano-Shushenskaya

- Certification for Operation in 2000 noted need for additional spillway capacity
- Construction of additional spillway capacity delayed due to lack of funding
Sayano-Shushenskaya

- Turbine has large area of rough operation
  - Need for new design recognized in 2000
  - Plant control system does not take into account area of rough operation
- Operates in Unified Electric System – Siberia
- Constructed under Russian state ownership
- Privatized in 1993
Can a Problem in a PH Cause a Dam Failure at a Remote Project?
Background Information

- During construction the spillway was used to pass water.
- During construction a flood resulted in 4500 m³/s being discharged through the spillway.
- The spillway stilling basin was severely damaged while passing 4500 m³/s - 7m of the foundation was eroded.
- The flood also overtopped the partially constructed dam cracking the dam-foundation interface and some concrete monoliths.
- The damage to the spillway was repaired.
Background Information

- The foundation and monoliths were grouted (under 200 meters of head)
- In 1988 a flood of 4400 m³/s damaged the stilling basin again
- Again, the stilling basin was repaired
- A new tunnel spillway is being constructed
How Could a Dam Failure Occur?  
Part 1 - Reality

1) Under Normal Operation
2) A fire at a remote power plant causes the system dispatcher to transfer load-following responsibility to SSH hydro plant
3) SSH staff start Unit 2 and place in load following mode
4) Operation of Unit 2 over the course of 30 years causes partial to complete fatigue failure of the bolts holding down the turbine head cover
How Could a Dam Failure Occur?  
Part 1 - Reality

5) In load following mode Unit 2 transitions through the rough operating region on several occasions
6) The fatigue failure of the head cover bolts reaches a critical state
7) The turbine head cover tears loose ejecting the turbine through the generator
How Could a Dam Failure Occur?
Part 1 - Reality

8) The open head cover allows water to flood into the powerhouse
9) The flooding water knocks out station power cutting power to the penstock intake gates
10) Water flows for half an hour until the gates can be closed using manual operators
11) The flooding damages the powerhouse to the extent that all 10 units are forced off line and only two units will be available to help pass flow in the coming runoff season
How Could a Dam Failure Occur?  
Part 1 - Reality  

12) Damage to the powerhouse results in the majority of inflow passing through the spillway for an extended period  

13) Operation through the winter results in icing over the spillway and collapse of a crane used to access the stilling basin for repair
How Could a Dam Failure Occur?
Part 2 - Hypothetical

14) Higher than normal snowfall in the watershed may lead to larger than normal runoff (assume flood of record)
15) The high runoff requires the spillway to run full
16) The excess inflow rapidly fills the reservoir
   - 19 days if one tunnel spillway and two units are available
   - 12 days if only two units are available
   - 7 days if the service spillway becomes inoperable
17) The excess inflow overtops the dam reinitiating the crack at the dam foundation interface
18) High spillway flows destroys the stilling basin bottom and begins to undercut the dam toe
19) Undercutting continues as the spillway passes flow.
How Could a Dam Failure Occur? Part 2 - Hypothetical

20) Cracking of the dam-foundation interface leads to increased uplift under the dam

21) The combination of continued toe undercutting and increasing uplift under the dam leads to a sliding failure of the dam
How Big a Problem is This?

- Everything except the last 2 slides is a reality
- Over one million people live downstream of the dam
- There is an embankment dam 12 miles downstream that would fail if overtopped
Hoover Dam
Height – 726.4’
Crest Length – 1244’
Res. – 28.5M ac-ft
How Big is Big?
<table>
<thead>
<tr>
<th>Source</th>
<th>Initial State</th>
<th>Second State</th>
<th>Third State</th>
<th>Fourth State</th>
<th>Final State - Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>Turbine has large range of rough operation</td>
<td>Commissioning reports recommends new turbine design</td>
<td>Fabrication of new turbines delayed for financial reasons</td>
<td>Vibration due to rough operation loosens some head cover bolts and causes fatigue fracture in others</td>
<td>Head cover fails and powerhouse floods rapidly</td>
</tr>
<tr>
<td>Construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Operated within Siberian Electric Grid</td>
<td>Unit 2 overhauled by company closely related to Sayano-Shushenskaya management</td>
<td>Headcover bolts not replaced during overhaul</td>
<td></td>
<td>To Figure 8</td>
</tr>
<tr>
<td>Owner’s Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Societal Decisions</td>
<td>Constructed under state ownership</td>
<td>Project privatized in 1993</td>
<td>Load control transferred to Sayano-Shushenskaya</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outside Influences</td>
<td>System load control at Bratskaya PH</td>
<td>Fire at Bratskaya PH</td>
<td>Unit 2 selected to follow load - unit makes multiple excursions through the rough zone</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5 – Interaction Flow Chart – Failure of Sayano-Shushenskaya Powerhouse Turbine Headcover
<table>
<thead>
<tr>
<th>Design</th>
<th>Initial State</th>
<th>Second State</th>
<th>Third State</th>
<th>Fourth State</th>
<th>Final State - Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Flood during construction resulted in cracking of base and monoliths</td>
<td>Spillway jet velocity high</td>
<td></td>
<td></td>
<td>Undercutting of dam toe results in increased tension at heel of dam. Base of</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dam re-cracks leading to increased uplift under dam and reduced normal forces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Stability is compromised and dam monoliths in spillway sections slide</td>
</tr>
<tr>
<td></td>
<td>PH req’d to pass flood flow</td>
<td>All inflow must pass through spillway until PH is repaired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No low-level outlet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction</td>
<td></td>
<td>Commissioning documents note need for additional spill capacity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Turbine headcover has failed (from Figure 6A)</td>
<td></td>
<td>Construction of additional spillway delayed for financial reasons</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner’s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Societal</td>
<td>Constructed under state ownership</td>
<td></td>
<td>Project privatized in 1993</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decisions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outside</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Influences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Things to Consider

- **Impacts of Deregulation**
  - Profit Driven Environment vs. Guaranteed Rate of Return
- **Operational or Physical Modifications for Environmental or Other Reasons**
  - Spillway gate operation
  - Low level outlet operation
  - Lake level restrictions
  - etc
- **Impacts of Increasing Use of SCADA Systems**
  - What happens if you lose communication link
- **Impacts of Increasing Use of Remote Operation**
  - Can you get to a site in inclement weather or emergency
Things to Consider

- Human Factors
- Organizational Factors
Consequences of Dam Failure
Stored Energy in Oroville Reservoir
Approximately 128 times the energy in the atomic bomb dropped on Hiroshima
2,200 Deaths
The Monument to the Unknown Dead, 1892. It still stands in Johnstown's Grandview Cemetery.
Rexburg

11 Deaths
>500 Deaths
2500 Deaths
The Taum Sauk failure cost Ameren between $1.5 and $3 Billion in direct and indirect costs.
53. If any one be too lazy to keep his dam in proper condition, and does not so keep it; if then the dam break and all the fields be flooded, then shall he in whose dam the break occurred be sold for money, and the money shall replace the corn which he has caused to be ruined.

54. If he be not able to replace the corn, then he and his possessions shall be divided among the farmers whose corn he has flooded.
English Common Law

John Rylands (1801-1888), owner of the Ainsworth Mills, Lancashire, UK, whose impoundment flooded his neighbor’s mine, giving rise to the concepts of dangerous accumulations, escape of same, and liability without fault.
Importance of a Robust Owner’s Dam Safety Program
Volume 18 of the Code of Federal Regulations Part 12 contains the FERC regulations related to Dam Safety

These regulations should be viewed as a minimum. They do **NOT** define an appropriate owners’ dam safety program.
Why Does the FERC Require a Written ODSP

- Every Dam is unique – we cannot write guidelines that cover every possible failure mode.
- Dams are not just a combination of individual components.
- Dams are a complex system operating within a larger system; the power grid.
Why Does the FERC Require a Written ODSP

- Dam failures are generally NOT caused by a single factor such as earthquakes or extreme floods.

- Many, if not most, failures are due to some form of mis-operation or other human or organizational factors.

- Taum Sauk
“the careful and responsible management of something entrusted to one’s care”
Common Causes of Organizational Accidents

Organizations that are often complacent about safety due to the low frequency of adverse events, arrogant about the probability of an adverse event happening to them and ignorant of the real risks inherent in their operations.

Regan, P., 2012, Call to Stewardship, USSD
Common Causes of Organizational Accidents

Organizations focused on meeting the letter of regulatory requirements but ignoring the underlying spirit and purpose of the regulations

Regan, P., 2012, Call to Stewardship, USSD
Common Causes of Organizational Accidents

Organizational safety programs focused on personal safety rather than system safety

Regan, P., 2012, Call to Stewardship, USSD
Common Causes of Organizational Accidents

Organizations being driven by financial performance resulting in decisions being made to operate systems near the boundaries of safety

Regan, P., 2012, Call to Stewardship, USSD
Common Causes of Organizational Accidents

A tendency to fixing symptoms of problems rather than determining the underlying causes and fixing the fundamental problems

Regan, P., 2012, Call to Stewardship, USSD
Common Causes of Organizational Accidents

Poor communication within, and outside, of organizations
Common Causes of Organizational Accidents

A lack of corporate safety culture in many organizations (System safety not personal safety)

Regan, P., 2012, Call to Stewardship, USSD
Complacency, Arrogance & Ignorance
Complacency

“It won’t happen because It’s been fine for a long time.”
Arrogance

“It might happen, but not to me.”
Ignorance

“What is It?”
Complacency

“Believing that past non-events predict future non-events (forgetting to be afraid)”

James Reason, Author of *Managing the Risks of Organizational Accidents*
Complacency
(Related to Focus on Financial Performance)

“Absent major crises, and given the remarkable financial returns available from deepwater reserves, the business culture succumbed to a false sense of security. The *Deepwater Horizon* disaster exhibits the costs of a culture of complacency.”

National Commission on the BP Deepwater Horizon Oil Spill (2011)
Complacency
(Related to Focus on Personal Safety)

“Awards for slip and fall reduction promote complacency. . . They create the illusion of protection in workplaces where process safety management hasn’t been properly implemented. The safety plaques are paper shields, easily immolated in explosions, along with the workers they beguiled.”

Gerard, L.W., Safety Awards that Endanger Workers’ Lives, May, 2010
“... an August 2005 incident in Pennsylvania during which 100 million gallons of fly ash spilled into the Delaware River through a breached plug in an ash settling pond did not prompt any response or study within TVA of TVA’s own potential ash pond risks.”

McKenna Long & Aldridge LLP, et.al, 2009, A Report to the Board of Directors of the Tennessee Valley Authority Regarding Kingston Factual Findings
“Incidentally, Mr. Jack Shepley of the F.P.C. Washington Office called Mr. Vencill recently and asked for some information about the upper reservoir level detection and pump shutdown which I sent him. . . . I told him there would be no structural damage if the pumps failed to shut down, but there would be some washing of the roadway surface.” (emphasis added)
Taum Sauk (MO)
Ignorance

“There is no evidence top management has taken the steps necessary to be well-informed about the key aspects of decisions selected to manage major risks that concern PG&E.”

Ignorance
(Related to Focus on Financial Performance)

“The ignorance of technical risks is a byproduct of PG&E’s overall focus on financial performance ...”

Focus on Regulatory Requirements
The Panel noted that while PG&E was “targeting efforts to comply” in reality;

“PG&E was skirting the requirements of the integrity management regulations through use of an ‘exception’ process, whereby critical repairs and other activities were delayed.”
“...we seriously question whether PG&E has embraced the spirit of the pipeline integrity regulations.”
Focus on Personal Safety
Not System Safety
Focus on Personal Safety

“Disasters don't happen because someone drops a pipe on his foot or bumps his head. They result from flawed ways of doing business that permit risks to accumulate.”

“Consider this: BP had strict guidelines barring employees from carrying a cup of coffee without a lid - but no standard procedure for how to conduct a ‘negative-pressure test’, a critical last step in avoiding a well blowout. If done properly, that test might have saved the *Deepwater Horizon*."

“Management’s focus in recent times appears to have been on the occupational safety of its employees and lacking an equivalent focus on the public safety aspects of its system.”
Focus on Financial Performance
Focus on Financial Performance

“... it should not be forgotten that commercial success in a competitive environment implies exploitation of the benefit from operating at the fringes of the usual, accepted, practice.”

Rasmussen, J., Risk Management in a Dynamic Society: A Modelling Problem, 1997
Focus on Financial Performance

“Closing in on and exploring the boundaries of the normal and functionally acceptable boundaries of established practice during critical situations necessarily implies the risk of crossing the limits of safe practice.”

Rasmussen, J., Risk Management in a Dynamic Society: A Modelling Problem, 1997
“Divers were summoned and they ascertained that the new sensor conduits had become detached from their mountings along the sloping concrete face of the reservoir. . . . Unfortunately, permanent repairs were postponed until regularly-scheduled maintenance the following spring to avoid an additional shutdown of the facility.”

Rogers, J.D., Overview of the Taum Sauk Pumped Storage Power Plant Upper Reservoir, 2008
Fixing Symptoms not Problems
“Symptomatic solutions are usually easier, faster, and cheaper to implement than long-term fundamental solutions.”

Marais, K., et.al., Archetypes for Organizational Safety, September 2003
“Initially, positive results to symptomatic solutions are seen immediately, as the visible symptoms are eliminated. Once a symptomatic solution has been successfully applied, the pressure to find and implement a fundamental solution tends to decrease.”

Marais, K., et.al., Archetypes for Organizational Safety, September 2003
“The underlying problem remains.”
“In 2003 and 2006, seeps along the west side of the Kingston dredge cells were discovered. The ‘fixes’ put in place to remedy these seeps were limited to patching the specific leaks.”

McKenna Long & Aldridge LLP, et.al, 2009, A Report to the Board of Directors of the Tennessee Valley Authority Regarding Kingston Factual Findings
“As evidenced by its limited corrective actions, TVA focused on the earlier incidents as the problem, rather than as a symptom of a larger trouble.”

McKenna Long & Aldridge LLP, et.al, 2009, A Report to the Board of Directors of the Tennessee Valley Authority Regarding Kingston Factual Findings
“Investigating the cause of incidents beyond the specific physical occurrences into the functioning of systems is fundamental to a robust safety program.”

McKenna Long & Aldridge LLP, et.al, 2009, A Report to the Board of Directors of the Tennessee Valley Authority Regarding Kingston Factual Findings
Poor Communication
“Employees tended to use the concept of ‘silos’ to refer to two related, but yet distinct, phenomena - (1) the more common use of the term indicating a lack of collaboration among various business units across TVA or within a particular department and (2) the tendency within TVA not to readily share information with one’s superiors.”

McKenna Long & Aldridge LLP, et.al, 2009, A Report to the Board of Directors of the Tennessee Valley Authority Regarding Kingston Factual Findings
“Frequently, employees cited poor communication and abundance of organizational silos that have impeded their ability to understand what work was being undertaken and hence the quality of the work.”
Lack of Corporate Safety Culture
Corporate Safety Culture

“the way safety is perceived, valued and prioritized in an organization. It reflects the real commitment to safety at all levels in the organization. It has also been described as how an organization behaves when no one is watching.”
Corporate Safety Culture

“A number of concerns surfaced in the course of our investigation that go to this issue of whether PG&E has a high functioning organization, capable of fulfilling its mandate for safe and reliable gas service.”

“We think this failing is a product of the culture of the company – a culture whose rhetoric does not match its practices.”

Corporate Safety Culture

“Whether it is the regulated entity or the regulator, the issue of organizational culture is an aspect the Panel felt could not be ignored.”

Corporate Safety Culture

“Both organizations failed to understand the critical technical and managerial nature of the pipeline integrity mandate and neither created an environment in which excellence was demanded.”

Corporate Safety Culture

“\textquote{The Panel believes both of these institutions must confront and change elements of their respective cultures to assure the citizens of California that public safety is the foremost priority.}”

Key Elements of a Safety Culture

- an informed culture
- a reporting culture
- a just culture
- a flexible culture
- a learning culture

Key Elements of a Safety Culture

_Informed Culture_ - one in which those who manage and operate the system have current knowledge about the human, technical, organizational and environmental factors that determine the safety of the system as a whole.

Key Elements of a Safety Culture

*Reporting Culture* - a culture in which people are willing to report errors and near misses

Key Elements of a Safety Culture

*Just Culture* - a culture of ‘no blame’ where an atmosphere of trust is present and people are encouraged or even rewarded for providing essential safety-related information, but where there is also a clear line between acceptable and unacceptable behaviour

Key Elements of a Safety Culture

**Flexible Culture** which can take different forms but is characterized as shifting from the conventional hierarchical mode to a flatter professional structure, and,

Key Elements of a Safety Culture

**Learning Culture** - the willingness and the competence to draw the right conclusions from its safety information system, and the will to implement major reforms when the need is indicated.

This disaster was preventable if existing progressive guidelines and practices been followed—the Best Available and Safest Technology. BP’s organizations and operating teams did not possess a functional Safety Culture. Their system was not propelled toward the goal of maximum safety in all of its manifestations but was rather geared toward a trip-and-fall compliance mentality rather than being focused on the Big-Picture.

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
BP

It has been observed that BP’s system “forgot to be afraid.” The system was not reflective of one having well-informed, reporting, or just cultures. The system showed little evidence of being a high-reliability organization possessing a rapid learning culture that had the willingness and competence to draw the right conclusions from the system’s safety signals.

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
BP

The Macondo well disaster was an organizational accident whose roots were deeply embedded in gross imbalances between the system’s provisions for production and those for protection.

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
BP

This disaster also has eerie similarities to the BP Texas City refinery disaster. These similarities include:

a) multiple system operator malfunctions during a critical period in operations,

b) not following required or accepted operations guidelines (“casual compliance”),

c) neglected maintenance,

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
BP

d) instrumentation that either did not work properly or whose data interpretation gave false positives,

e) inappropriate assessment and management of operations risks,

d) multiple operations conducted at critical times with unanticipated interactions,
BP

g) inadequate communications between members of the operations groups,

h) unawareness of risks,

i) diversion of attention at critical times,

j) a culture with incentives that provided increases in productivity without commensurate increases in protection,

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
BP

k) inappropriate cost and corner cutting,
l) lack of appropriate selection and training of personnel, and
m) improper management of change.

Deepwater Horizon Study Group
Investigation of the Macondo Well Blowout Disaster
In both cases—the BP Texas City and the BP Macondo well disasters—meetings were held with operations personnel at the same time and place the initial failures were developing. These meetings were intended to congratulate the operating crews and organizations for their excellent records for worker safety.
Both of these disasters have served—as many others have served—to clearly show there are important differences between worker safety and system safety. One does not assure the other.
Alternatively
Shell Oil

Shell Oil has a corporate policy, Goal Zero, that encourages workers to call for work to stop when they suspect that something is proceeding improperly.

Shell gives awards to what they term ‘Goal Zero Heroes’. So, rather than just recognizing worker safety, Shell also recognizes those who have taken action to prevent system failures.

http://www.shell.com/home/content/environment_society/safety/culture
“All employees have the right and responsibility to shut down, in an orderly fashion, any system that they believe to be endangering the public, environment, themselves or co-workers.”
Where Do We Go From Here?
“I think we have to be frank with ourselves, not just about what it will cost to upgrade our infrastructure, but what it will cost if we fail to do so.”

Liveris, A., "Make it in America: The Case for Re-Inventing the Economy"
Leadership

“The critical common element is an unwavering commitment to safety at the top of an organization: the CEO and board of directors must create the culture and establish the conditions under which everyone in a company shares responsibility for maintaining a relentless focus on preventing accidents.”

(The accidents they are talking about are not OSHA accidents)

National Commission on the BP Deepwater Horizon Oil Spill (2011)
“Likewise, for the entire industry, leadership needs to come from the CEOs collectively, who can apply pressure on their peers to enhance performance.”

National Commission on the BP Deepwater Horizon Oil Spill (2011)
Acknowledge Ownership and Responsibility

The Independent Review Panel on the San Bruno explosion recommended the CPUC require:

“certification by senior management of the operator that parallels the certifications now required of corporate financial statements pursuant to Sarbanes-Oxley.”

(The Sarbanes-Oxley Act, enacted after the financial collapse of ENRON, requires financial audits of companies address the risks to a company’s financial well being.)
Solve Problems
not
Symptoms
Communicate

“To meet the challenge of addressing the complexities inherent in risk management, the leadership of the organization needs to establish and promote a thorough and honest company-wide communication system.”

Keep Learning

“It should not be necessary for each generation to rediscover principles of process safety which the generation before discovered. We must learn from the experience of others rather than learn the hard way. We must pass on to the next generation a record of what we have learned.”

Jesse C. Ducommun – ex Vice President Amoco

“Large organizations, either in the private sector or public sector, always have a churning of staff. . . . The result is that when something bad happens, or even if something good happens, few people know those solutions which have proven to work in the past and those that have failed miserably.”

Shamah, J., How soon they forget: Organizational memory and effective policies, May 2009
Understand Risks

“Quality (risk) analysis could both facilitate two-way communication between top management and individuals with substantial knowledge about each of the relevant aspects of utility operations and provide a clear understanding of all the information available to make a key risk management decision.”

Understand Risks

“. . . it is the job of the CEO and senior management to assess and manage the company’s exposure to risk.”

“The audit committee should discuss the company’s major financial risk exposures and the steps management has taken to monitor and control such exposures.”

NYSE Listing Standards Part 7d
Understand Risks

An organization's risk maturity is gauged by the priority, proactive thought, and serious effort allocated to manage the most significant risks facing an organization. Collectively, risk management and risk culture are the foundations that influence how well decisions about risk are made.
Understand Risks

Quality risk analysis to support strategic and policy risk management decisions at PG&E does not exist. There is no evidence top management has taken the steps necessary to be well-informed about the key aspects of decisions selected to manage major risks that concern PG&E, such as its top ten catastrophic risks.

PG&E Risk Factors 2010

- operating limitations that may be imposed by environmental laws or regulations, including those relating to GHG, or other regulatory requirements;
- imposition of stricter operational performance standards by agencies with regulatory oversight of the Utility’s facilities;
- environmental accidents, including the release of hazardous or toxic substances into the air or water, urban wildfires, and other events caused by operation of the Utility’s facilities or equipment failure;
- fuel supply interruptions;
- equipment failure;
- failure or intentional disruption of the Utility’s information systems, including those relating to operations, such as the advanced metering infrastructure being deployed by the Utility, or financial information, such as customer billing;
- labor disputes, workforce shortage, and availability of qualified personnel;
- weather, storms, earthquakes, wildland and other fires, floods or other natural disasters, war, pandemic, and other catastrophic events;
- explosions, accidents, dam failure, mechanical breakdowns, and terrorist activities; and
- other events or hazards.
PG&E Risk Factors 2011

- the release of hazardous or toxic substances into the air or water;
- fuel supply interruptions or the lack of available fuel which reduces or eliminates the Utility’s ability to provide electricity and/or natural gas service;
- the failure of a large dam or other major hydroelectric facility;
- the breakdown or failure of equipment, electric transmission or distribution lines, or natural gas transmission and distribution pipelines, that can cause explosions, fires, or other catastrophic events;
- the failure of new generation facilities to perform at expected or at contracted levels of output or efficiency;
- use of new or unproven technologies;
- the failure to take expeditious or sufficient action to mitigate operating conditions, facilities, or equipment, that the Utility has identified, or reasonably should have identified, as unsafe, which failure then leads to a catastrophic event;
- operator or other human error;
- cyber-attack;
- severe weather events such as storms, tornadoes, floods, drought, earthquakes, tsunamis, wildland and other fires, pandemics, solar events, electromagnetic events, or other natural disasters; and
- acts of terrorism, vandalism, or war.
“Any profession, be it law or medicine, or engineering, empowers the individual with special talents that benefit the public, and the wise use of these talents for the public good is expected. To do otherwise is to be professionally immoral.”

Vesilind, P., “Responsibility”, Bucknell University
“Never sacrifice safety for cost, no matter how urgent your client may become. He does not recognize the danger and you should. If you cannot agree with him, resign your engagement, for sooner or later the reckoning will come.”

Hatton, C., New England Water Works Association, 1912
Do onto others ........

Would you live with your family below your dam?
Future Initiatives
Initiatives

- Owner’s Dam Safety Programs
- Risk-Informed Decision-Making
- Time Sensitive EAPs
Redlands Dam
and the
Grand Canyon Flood
On August 17, 2008 the Redlands Dam on a tributary stream to the Colorado River failed leading to wide spread reporting of flooding, stranded hikers and helicopter rescues.

The event was even reported on BBC World News.
The Sensation

- A Google search of “Redlands Dam” returned 542,000 hits
- A Google search of “Redlands Dam Grand Canyon” returned 230,000 hits
The Headlines

- “Grand Canyon Flood Caused By Redlands Dam Breach”
- “Dam breaks near Grand Canyon; hundreds evacuate”
- “Grand Canyon rescue as dam bursts”
- “Redlands Dam Breaks, Evacuating Grand Canyon”
The Stories

- Heavy rains caused the Redlands Dam near the Grand Canyon to fail, causing some flooding in the small village of Supai, Ariz. on Aug. 17, 2008.
- Hundreds of people are evacuated from the Grand Canyon after an earthen dam broke.
- Grand Canyon National Park spokeswoman Maureen Oltrogge said water from the Redlands Dam had caused flooding in a side canyon.
“Authorities have found all 11 people who were unaccounted for after a dam burst, causing major flooding in Supai Canyon”

“Redlands Earthen Dam was breached about 45 miles upstream from Supai, flooding parts of the canyon and nearly washing away rafters, park officials said”
The Reality

- Redlands Dam was a ranch stock pond.
- It was too small to be listed on the National Inventory of Dams.
- The flooding for the most part was the result of extreme rains that caused even the Colorado River hydrograph to spike.
Reservoir about 800’ x 500’

Redlands Dam Aerial

Dam breach here

Reservoir about 800’ x 500’
The Diamond Creek Gage is at mile 226 on the Colorado River. Havasu Creek dumps into the Colorado at mile 157. The Redlands Dam is at least 55 miles up Havasu/Cataract Creek. That is more than 120 miles that the water would have to travel in just 8 hours (15 miles an hour). However, the flash flooding was reported in the Havasu campground between 1 AM and 3 AM Sunday. So, the dam break didn't cause the jump in the Diamond Creek gage on Sunday afternoon. It was the large area of heavy rain that fell between the Redlands Dam and Supai Village.
The Message

- Any dam failure may get more attention than you can possibly imagine.
- Dam breaks affect all of us due to public perception. How many people really understand that the dam break had essentially nothing to do with the flooding in the Grand Canyon?
- All DAMS MATTER!
Tirlyan
10 m
7,000 ac-ft