

PUMPED STORAGE HYDRO-ELECTRIC PROJECT TECHNICAL GUIDANCE

**Revision 0
October 5, 2007**

Index

Section	Page
1. Design Basis	2
1.A Hydrology, Hydraulics and Spillways	3
1.A.1 Hydraulics	3
1.B Civil Design	4
1.C. Controls and Control Logic	6
1.C.1 Fail Safe Design	6
1.C.2 Direct Action Pump Mode Shutdown	8
1.C.3 Redundancy	8
1.C.4 Ease of Testing and Calibration	9
1.D Timing of Overtopping - Capacity of Pumps vs. Capacity of Spillway	9
1.E Operating Cycle	11
1.F Staff and Unstaffed	12
2. Organizational Processes	13
2.A Training	13
2.B Procedures	14
2.B.1 Normal Ops	15
2.B.2 Abnormal Ops	16
2.B.3 Emergency Conditions	17
2.B.4 Alarm Response	17
2.B.5 Preventive Maintenance	19
2.C Design change/ Configuration Control Program	19
2.D Organization and Responsibilities	20
3. Instrumentation and Monitoring Equipment	21
3.A Instrumentation Design Considerations	21
3.B Testing/ Calibration/ Operation	24

Pumped Storage Technical Guidance

This document provides criteria for Pumped Storage Hydro-Electric project owners to assess their facilities and programs against. This document specifically focuses on water level control and management. Pumping is the principal feature that sets pumped storage projects apart from conventional hydro projects and overtopping of a project reservoir is the principal failure mode that could impact dam and public safety. Therefore, control and management of water levels is critical to assuring dam and public safety.

Every Pumped Storage project has very unique design features that may make some of the items discussed in this document unnecessary or less beneficial. Each item mentioned in this document is intended to challenge the owner to question and evaluate the need and benefit to their particular project. Sufficient consideration, evaluation, and justification should be provided by the owner as to whether each criterion is utilized and to what extent it is used.

1. Design Basis:

Design basis encompass the assumptions made by the original engineers, and subsequent engineers as the plants have been modified, to assure safe and reliable operation of the project. The design basis for a pumped storage hydro-electric project must consider many factors to ensure safe and reliable operation of the project. The design basis can accommodate many different designs and still meet the desired outcomes. This section defines the various design basis areas and factors that should be considered, evaluated, and documented for a pumped storage project.

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 (ODBD). 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.

1. A. Hydrology, Hydraulics and Spillways.

The hydrologic design basis for a pumped storage facility, as for a conventional hydro project, is mainly concerned with determining the appropriate Inflow Design Flood (IDF) and Probable Maximum Flood (PMF) for the project. Guidance on selecting the IDF and PMF can be found in Chapters 2 and 8 of the FERC's Engineering Guidelines.

1. A. 1. Hydraulics

The hydraulic design basis for a pumped storage project is concerned with the configuration and sizing of works such as intake structures, penstocks, hydraulic machinery, water passages, and spillways. The hydraulic design of these elements has great bearing on both the safety and operational efficiency of the project.

Structures intended for ultimate safety protection should be robustly designed and operationally simple and "fool-proof", and should be designed to operate well under the anticipated worst case conditions. All spillways and outlet works should also be evaluated for the effects of wave action, ice pressures, and debris collection on the hydraulic capacity and structural stability of the system. Design considerations for spillways and freeboard can also be found in Chapter 2 of the FERC's Engineering Guidelines.

Spillways can be classified as one of three types:

- Service or principal spillways – designed for continuous or frequent releases without damage to the dam and appurtenances;
- Auxiliary spillways – designed for infrequent releases during periods of high inflow in excess of the service spillway capacity;
- Emergency spillways – designed to provide protection from overtopping of dams during extreme flood events or mis-operation of the project.

Many pumped storage projects have a relatively small upper reservoir with a small drainage area. For these projects, the role of service spillway may be fulfilled by the powerhouse, e.g. the hydraulic turbines and their associated intake structure and penstocks or water passages. If there is an appreciable drainage basin upstream of the upper reservoir, a service or auxiliary spillway or outlet may be required to pass normal (non-flood) or flood flows during periods when generation from the project is not required or is not possible due to maintenance or other special situations. Projects with upper reservoirs with little or no upstream drainage basin often use the powerhouse as the only principal outlet from the upper reservoir, and may have no auxiliary or emergency spillway in the upper reservoir.

The need for an upper reservoir emergency spillway on a given pumped storage project should be evaluated based on several factors:

- Downstream hazard potential due to dam failure;
- Magnitude of the inflow design flood (IDF);
- Available reservoir storage volume above the maximum operating water surface elevation (is there volume available to store the IDF inflow without release and with reasonable freeboard?);
- Potential for mis-operation of the project in pumping mode (can the reservoir be filled to zero freeboard condition due to pumping operations?)

Emergency spillways can be of the gated or ungated type. Ungated spillways operate without human intervention whenever the reservoir elevation exceeds the spillway crest elevation, and so are considered more reliable than gated spillways. Gated spillways require either human intervention or the provision for automatic operation in order to function. If a gated spillway is intended to provide ultimate protection against overtopping and dam failure, very careful attention must be paid to the maintenance and testing of the gates, hoist mechanisms, and any automatic control systems used to operate the gates. Procedures should be in place to ensure or visually verify proper gate operation during flood events. At projects where the possibility exists for overfilling the upper reservoir due to mis-operation (over-pumping), an ungated spillway is preferable to a gated design, since it is virtually certain to operate when required. In these cases, the hydraulic capacity of the spillway should be at least equal to the pumping capacity of the plant.

If a spillway is contemplated or provided, consideration should be given to the downstream consequences of spillway operation, in particular if the spillway discharges into the lower reservoir. Analysis should be conducted to route the spillway discharge under IDF conditions through the lower reservoir or downstream watercourse to determine the effect on structures or habitations.

1. B. Civil Design.

This section focuses on the civil design features of a Pumped Storage Project that influences the reservoir levels as they may impact the safety of the dam(s). The objective of this section is to provide a check list for the owner/designer/inspector to use to verify that adequate design features are included in the civil structures of a project to preclude an uncontrolled release of water from the project that could impact public safety.

Most, but not all, pumped storage projects include the civil structures listed in the following table; furthermore, the design features indicated may not be applicable to all projects. Therefore, the checklist is simply that, a generic list for the owner/designer/inspector to use for his project, recognizing that various items

may not be applicable to his project. Also, the checklist does not include principles and considerations of other project features for controlling reservoir levels such as instrumentation, operator training, organizational process, etc as addressed in other sections of this document.

As seen on the following checklist, there are several fundamental principles that apply to all of the Civil Structures in considering features that minimize the potential for an uncontrolled release from the project. These include the following:

- Are there passive features, such as overflow spillway or un-gated crest, in place that do not require operator intervention?
- Are adequate visual inspection and monitoring programs in place on a year-round basis?
- Is adequate freeboard under static and wave conditions available and is wave protection in place?

**Generic Checklist
Civil Design Features
Control and Management of Reservoir Levels**

Civil Structure	Design Feature	Remarks
Upper Reservoir	Settlement Monuments	Monitoring Frequency
	Visual Observation of condition year-round	If year-round observation is not possible, what counter measures are in place?
	Static Freeboard	
	Wave Run-up Freeboard & Protection	
	Passive Overflow Spillway	Is year-round inspection possible?
	Overflow Spillway Channel	Maintenance Program
	Is trash control an issue?	
	Monitoring System for the Impervious Barrier	Piezometers and Weirs
	Inspection Gallery	Accessible year--round?
Conveyance System Intakes, Channels, Shafts, Tunnels. Penstocks, Valves, Gates	Inspection and monitoring systems	
	Visual Inspection of Surface Features	Accessible year-round?
	Periodic Inspection of Underground Features	
	Visual Observation of condition year-round	If year-round observation is not possible, what counter

Lower Reservoir		measures are in place?
	Settlement Monuments	Monitoring Frequency
	Passive Controlled Release System	Is Operator intervention required?
	Is trash control and issue?	
	Monitoring System for Passive Controlled Release System	Is year-round inspection and monitoring possible?
	Static Freeboard	
	Wave Run-up Freeboard & Protection	
	Monitoring System for the Impervious Barrier	Piezometers and Weirs
	Inspection Gallery	Accessible year-round

1. C. Controls and Control Logic.

Most pumped storage projects include a water level monitoring and control system for their upper and lower reservoirs' operation. Many of these systems include automatic features designed to initiate pump/turbine shutdown if the water level rises above preset maximum values. However, such monitoring and control systems may not necessarily be based on fail safe design principles and should not be relied upon to provide over-pumping protection for the reservoir.

An emergency back-up over-pumping protection system should also be provided, especially for those projects with smaller storage volume in the upper reservoir or those without adequate spillway capacity to safely accommodate pumping inflows. Given the critical safety role of the emergency over-pumping protection system, its design should include the following elements:

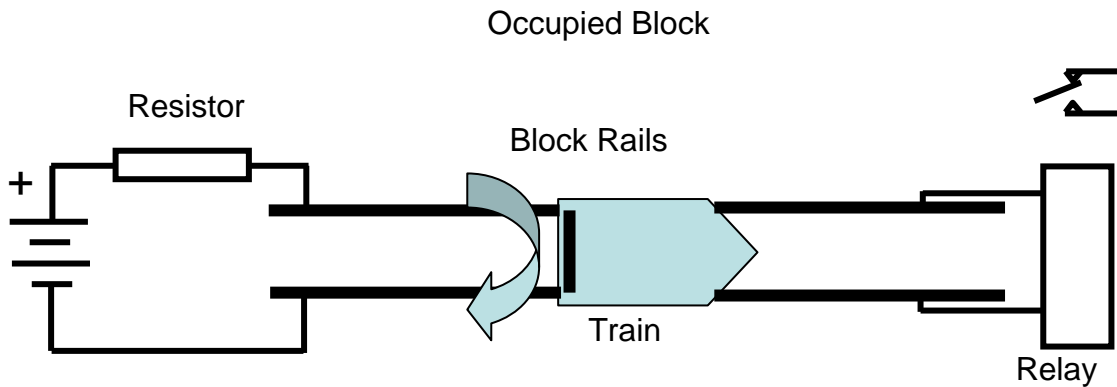
- Fail Safe Design
- Direct Action Pump Mode Shutdown
- Redundancy
- Ease of Testing and Calibration

1. C. 1. Fail Safe Design:

Fail safe designs are those where failure of any component in the system results in a predictable safe output condition. An example borrowed from the railroad industry is the classic track circuit used to detect the presence of rolling stock in a length (block) of track. This circuit is shown in Figure 1 below. A track battery at one end of the block supplies current through the rails to energize (pick-up) a track relay at the other end of the block. The track relay must be energized to allow the separate signal battery (not shown) to illuminate a green signal allowing trains into the block.

Figure 1

Railroad Detection Circuit



Relay at one end of block is normally energized by battery and resistor at other end of block. Locomotive or rolling stock axle in block shorts out current to relay to indicate block occupancy.

In normal operation, an axle and wheels anywhere in the block will shunt current from the track relay forcing it to open its contacts and illuminate the red signal. The fail-safe nature of this design causes the track relay to de-energize on any of the following conditions:

- Battery failure
- Open circuit in any wiring
- Break in rail.
- Open or short circuit in track relay.
- Conductive object across block rails.

Using gravity rather than springs to drop the relay armature when the coil is de-energized provides additional fail safe protection. Also, the relay contacts are made of materials that resist accidental welding.

For an over-pumping protection system, a fail safe design would mean that if a critical system component fails, this will be immediately noted and the

pump/turbine begins to shut down. It also means that pumps should only be operated if **all** over-pumping protection systems are working fully. In general, the pump/turbines should be shut down when the reservoir reaches a level that should not be exceeded or any component of the over-pumping protection system fails.

1. C. 2. Direct Action Pump Mode Shutdown:

Traditionally, hydro-power facilities have employed separate systems for protection versus control/monitoring functions. Protection systems generally utilize various sensors that respond to abnormal conditions and act to directly shutdown the generator/motor to prevent damage to equipment. For maximum reliability, these sensor output contacts are not routed through computers, PLCs, timers or other systems before acting to trip the generator/motor shutdown relay(s). A typical example is the mechanical over-speed sensors that initiate closure of the turbine shutoff valve to prevent or limit runaway speed operation of generators. Such devices operate without electrical power.

On the other hand, control and monitoring functions are now being performed with computers and PLCs, replacing many of the older relay logic systems. However, these control and monitoring functions should be performed within the safety limits provided by the direct acting protection system.

In his recent book, 'Hydro Plant Electrical Systems', Dave Clemens states on page 10-2 "Emergency Shutdown Controls: Although computer and PLC systems improve plant operation by providing greater flexibility in control, alarming, and sequence of events recording, the essential emergency shutdown controls should remain hardwired. This will guarantee that a safe and orderly shutdown of the plant can be accomplished in an emergency situation during which the computer/PLC has failed."

Given its critical function, the upper reservoir emergency over-pumping protection system should act directly to de-energize the pump mode master relay through the emergency shutdown circuit (86E). While an emergency shutdown is more severe on the generator/motor and pump/turbine compared to a normal shutdown (86N), the equipment experiences an emergency shutdown whenever the transmission line to the plant is suddenly lost. For maximum reliability, the excessive water level signal should not be diverted through timers or other logic functions. This direct action is analogous to the operation of generator/motor protective devices.

1. C. 3. Redundancy:

Redundancy of components can enhance the reliability of protective systems. Redundancy should not, however, be considered as a substitute for fail safe

designs. The track circuit described above is highly reliable, yet it contains no redundant components.

1. C. 4. Ease of Testing and Calibration:

To help assure the continuing proper operation of an over-pumping system, provisions should be included to allow periodic functional testing and calibration. Stilling wells for level instruments can be provided with fill and drain systems to allow testing of the instruments. This can allow testing without the need to raise or lower the reservoir.

Periodic testing should include the level sensors as well as other components to verify operation of the generating units' trip relays when upper reservoir water level reaches the preset limits. Ideally, testing apparatus should be incorporated into the system to permit testing without the need for specialized equipment or personnel.

1. D. Timing of Overtopping - Capacity of Pumps vs. Capacity of Spillway.

Adequate safeguards should be in place at Pumped Storage projects so that reservoir levels are closely monitored and controlled in order to prevent overtopping and catastrophic failure of the structure. These safeguards are needed to ensure that a consistent reaction is implemented for each pre-determined milestone reservoir water level. There are five major factors that need to be considered when selecting these milestone reservoir levels, and they are:

- 1) Availability of a spillway and its adequacy: If there is a spillway at the dam and it is adequate to handle the pumped inflow and inflows from the contributing drainage area with sufficient residual freeboard left, then the system is in good shape and minimum monitoring will be needed. All that is required in this case is to determine the impact of spillway flows on the downstream area and to implement adequate mitigating measures. If there is no spillway or the current spillway capacity is inadequate, then the threshold reservoir level must be selected to permit sufficient freeboard in order to adequately react and prevent overtopping.

- 2) Downstream hazard potential: The downstream hazard potential is critical in determining the safe level of reservoir operation. The higher the downstream hazard potential, the larger the freeboard needed to ensure there is adequate response time to prevent uncontrolled releases or overtopping resulting in harm to downstream life and property.

- 3) Type of dam: The type of dam is also important in deciding the freeboard needed. Concrete dams typically can handle some level of overtopping to some period of time without failure, rock-fill dams with free

draining downstream sections can handle very limited amount of overtopping before failing, while earth-fill dams should not be subjected to overtopping at all.

4) Remoteness of site & availability of dam caretaker: If the dam site is remote and no dam caretaker is living close by, then the freeboard selected should be increased to allow adequate response time. Remote monitoring and automatic shutoff equipment should be closely monitored, controlled and maintained to reduce or eliminate the possibility of malfunction and any resulting problems. If the dam site is close by or if a caretaker lives sufficiently close by, this situation improves the response time dramatically and the needed freeboard could be relaxed somewhat.

5) Weather: The weather and weather conditions could impact the inflows into the reservoir, could impact the accessibility to the site, or impact the time of response to an emergency at the site. All these factors should be accounted for when determining the required reservoir level and amount of freeboard needed.

In order to adequately select a safe operating level and the needed amount of freeboard to prevent overtopping, the previously discussed factors should be studied thoroughly and should be made components of models simulating the dam and reservoir so that competent engineering calculation can produce the following:

- The time the reservoir level will take to reach the spillway crest from the operating level.
- The time the reservoir level will take to reach the dam crest.
- The time of overtopping before failure of the structure occurs.

Once these parameters are adequately computed, then the safe water level that the reservoir could be operated to and the needed freeboard to prevent overtopping and catastrophic failure can be selected and implemented. Equipment such as alarms, surveillance cameras, and automatic pump shutoffs should be selected with enough redundancy to ensure that the response time needed is available.

Experience has shown that allowing water to be stored against parapet walls constructed on the crest of rock-fill or earth-fill dams is not a sound engineering practice. These walls are prone to settlement, cracking, undermining if not constructed properly, or overturning and sliding during overtopping. This could greatly reduce the needed response time. If at all possible, water should not be allowed against these parapet walls.

1. E. Operating Cycle.

Market conditions have, in some instances, changed the way projects are operated. Rather than weekly or daily pumping cycles many projects are now subjected to multiple pump/generate cycles each day as the price of electricity in the local market fluctuates. At facilities where over-pumping can lead to critical failure modes, changing from weekly pumping to daily pumping increases the probability of failure seven times, nearly an order of magnitude. Multiple daily cycles may increase the probability two or three times more.

Many pumped storage projects were designed 40 or more years ago prior to the de-regulation in the electric industry in the United States and the development of today's sophisticated SCADA systems. These changes combined with market pressures, has resulted in the partial or full automation of facilities which were originally designed to be operated by people located at the facility.

Changes in on-site staffing and remote operation of pumped storage facilities also have the potential to increase the probability of an over-pumping incident. Reduction in on-site staffing often results in operating decisions being made by an individual who has additional duties beyond those that existed for a dedicated local operator (i.e. responsibility for more than one facility). These additional responsibilities can increase stress on the operator increasing the probability of a human factor error, and/or result in a lack of focus on critical instrumentation resulting in an increased probability of an over-pumping failure.

Remote operation of pumped storage projects places greater reliance on instrumentation and communication systems to provide critical data to operators who may be located distant from the facility. Loss of a key instrument or communication system may leave the remote operator without the means to control and monitor reservoir water level.

Remote operation may also result in the operator of the facility being unfamiliar with the specific critical components of the facility that are related to controlling and managing water levels and the consequences of a potential over-pumping incident.

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 (ie. 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.

Design Basis issues should also be included in the design change / configuration control program as outlined in Section 2 of this document.

1. F. Staff and Un-staffed.

Remote operation of pumped storage projects may present additional risks that were not considered in the original design basis of the facility. Remote operation of a hydroelectric project places a higher reliance on the SCADA and control systems than might be required for a locally controlled plant. Additionally, remote operators may have responsibilities in areas unrelated to the safety of the project and may not be familiar with the specifics of safety related issues at hydroelectric projects in general and pumped storage projects in particular. Owners of remotely operated pumped storage projects should assess the training of operators to assure that they have an understanding of the critical failure modes and know what steps to follow if pre-set limits are exceeded.

On January 13, 2006 the Federal Energy Regulatory Commission (FERC) issued a letter to all licensed pumped storage projects requiring them to be staffed and monitored twenty-four hours per day, seven days per week. The letter specified that this requirement could be waived, or modified, by the appropriate FERC Regional office at such time the licensee demonstrates the ability to prevent

over-pumping or that an over-pumping condition does not have a detrimental affect downstream of the project. The letter required this situation to be verified each year by the licensee. The January 13, 2006 FERC letter or more current FERC guidance should be considered by the licensee when determining the staffing of a pumped storage project. Un-staffed operation should only be considered when robust fail safe systems, procedures and processes are in place to support unattended operation. It may be appropriate to perform a Fault Tree analysis to support unattended operation. Design conditions specified in the Civil Design and Timing of Overtopping sections should be considered in this analysis.

2. Organizational Processes

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.

2. A. Training

Training programs should be developed for pumped-storage projects to keep personnel up to date on operational and dam safety requirements. There are two levels of training that need to be considered. The first is an introductory training, which is geared towards the new employee to instruct them on basic fundamentals and procedures that need to be followed. The second is refresher type training for the more experienced workers to review routine procedures and information and make them aware of any changes.

Training of the emergency action plan (EAP) should be performed at a minimum on an annual basis or whenever significant changes have been made to the Dam Safety program to ensure all hydro personnel understand how to respond in the event of an emergency, are familiar with the notification flow charts and understand how to read the inundation maps. As part of the EAP training, mock tests of the EAP should be conducted annually not only for the benefit of hydro and supervisory personnel, but also as training for the emergency management agencies.

The hydro dispatch operators should have periodic training to ensure that everyone is aware of critical operational procedures and any recent changes that have occurred. There should also be written procedures that can be referenced by the less experienced employees and must be used in the event an emergency condition occurs. Since some pumped-storage projects are remotely operated it is also important to have a training program for plant personnel so they are able to operate the plant in an emergency or loss of the computer system in the event

communication is lost with hydro dispatch.

There should be training established for the instrumentation and monitoring program. This training is required to ensure consistency in the methods used to collect data as personnel changes occur within the organization. For future reference there should be written procedures in place to document the program. The procedures and training should include how and when measurements are to be taken, what the action limits are and what to do in event an action limit is exceeded. The training should include documentation of the name, time and date of the training and sign-off by the trainer that the trainees have received and understood the training goals. The use of computer based training with quizzes could assist in consistent training throughout the hydro organization.

2. B. Procedures

The organizational processes of training, procedures and configuration control are critical to the safe operation and control of reservoir levels at a pumped storage plant. Procedures are necessary for a consistent response with predictable outcomes in normal, abnormal and emergency situations. Detailed written procedures are required for all equipment and operations that impact and control upper or lower reservoir level. These procedures should cover both operation and preventative maintenance of all equipment and instrumentation that has the potential to impact actual reservoir level or display / report / record reservoir level.

Operations procedures can be subdivided into four categories: normal operations, abnormal operations, emergency procedures, alarm response procedures. Preventative maintenance procedures should be developed and performed as part of normal operations, and may be detailed in the project's Surveillance and Monitoring Plan (SMP).

In general procedures should contain some minimum level of information. Guidelines/processes should be established for training personnel on the use of these procedures and for maintaining the procedures (configuration control) to reflect current equipment configuration.

Procedure topics will be specific to each plant. Several generic topics with descriptions of purpose are provided, as a guide to the types of operational activities that should be captured under each procedure type.

Operating Procedures are necessary for all activities / processes used to control and monitor reservoir levels.

Normal operating, abnormal, emergency and alarm response procedures should at a minimum include;

- Purpose
- Definitions (of all terms used in the procedure)
- Engineering inputs, design capabilities, limitations.
- References to other procedures.
- Alarms and indications
- Detailed step by step actions
- Date of revision
- Position responsible for procedure.

2. B.1. Normal Operations

2. B.1.1 Hydraulic Coordination

Provide a systematic method of hydraulic coordination for the management of water levels, inflow and releases from the project reservoirs during normal conditions. The objective of hydraulic coordination is to maintain the reservoir levels within their design elevations to ensure optimal power production, control of water storage and for flood abatement as defined by regulatory license and design requirements.

It is necessary that primary and alternate sources of external information that can be helpful in predicting inflows or expected inflows to a project be identified. USGS, IFLAWS, National Weather Service web sites that may provide upstream flow or precipitation data to better predict and prepare for abnormal inflow conditions.

2. B.1.2 Release Structures Operation

Provide instructions for safe operation of reservoir release structures, including but not limited to spillway gates, diversion structures and low level release structures. Procedures should include all modes of operation (normal, flood), under all methods of power (primary, backup) and control (remote and local). Procedures should detail any modes of operation that could jeopardize structural integrity, e.g. unbalanced levels in adjacent conduits.

2. B.1.3 Station Service Power Operation

Provide instructions for the operation of all power sources (e.g. emergency diesel generators) used to provide power to critical instrumentation, level control systems and equipment for any and all project reservoirs. Procedures should include manual start and stop and the alignment of control for automatic start/stop operation.

2. B.1.4 Security

.

Access Control, Planning and Coordination, Cyber Security, Communications and Monitoring are to be considered for the procedures necessary to ensure project security. Procedures should also provide guidance for actions to be taken by security and operations personnel in response to security events or changes in security threat levels as issued by the Department of Homeland Security.

2. B.1.5 Inspection and Monitoring

Procedures are required for inspection and monitoring of all dams, dikes, penstocks, spillways, release structures, etc. The Surveillance and Monitoring Plans (SMP) provide a basis for these procedures.

2. B.2 Abnormal Conditions

2. B.2.1 High Inflows

The purpose of this procedure is to provide guidance for the operator to respond to extremely high inflows to either or both of the project reservoirs during heavy rainfall conditions or changes in upstream reservoir releases. These procedures would reference and be in accordance with any license requirements or agreements with state or federal agencies (e.g. USACOE).

Guidelines must be developed for preliminary station mobilization if severe weather conditions are expected/predicted. Severe weather may include high wind conditions (hurricane, blizzard, or tornado), heavy rain (defined by specific project), flash flooding caused by a rapid snowmelt, a heavy snow/blizzard, heavy sleet and/or freezing rain, or any combination of these events. The intent of this procedure would be to prepare both equipment and personnel for severe weather events and to adequately prepare and protect all exposed facilities that could be negatively impacted by the event (e.g. instrument houses that contain reservoir level instrumentation are adequately secured and protected).

2. B.2.2 Discrepancy or Loss of Instrumentation

Procedures are required to identify actions to be taken in the event instrumentation for monitoring of the reservoir elevations is unavailable or values may be in error. These actions may include selection of alternate instrumentation, investigation of the event, notification of personnel, shutting down units or limiting the operation of the pumps or generators.

2. B.2.3 Back up Station Service Power Operation

Provide instructions for the operation emergency power sources (e.g. emergency diesel generators) used to provide power to critical instrumentation, level control systems, release gates and valves and other equipment at project reservoirs in

the event normal sources are not available. Procedures should include manual start and stop procedure and the alignment of controls for automatic start/stop operation.

2. B.3 Emergency Conditions

2. B.3.1 Over-Pump Spillway

Provide guidance for operations personnel in the event that the upper reservoir over-pump spillway is utilized. These actions may include notification processes (public safety, environmental impacts, corporate and regulatory notifications, generation impacts), and be in a similar format to an EAP flowchart.

2. B.3.2 Emergency Notifications

Emergency notification procedures are included in the Emergency Action Plan (EAP) for conditions that may include changed or unusual seepage flows, settlement of dams/dikes, earthquake, reservoir elevations above the “normal maximum”, unusual releases, etc.

2. B.3.3 Emergency Dewatering

Emergency dewatering procedures document operational processes to perform emergency un-watering of project facilities, including rapid draw down (reservoirs, tunnels).

2. B.4 Alarm Response

Alarm Response Procedures should be developed for all critical alarms. Any alarm that indicates an abnormal or changed condition on a piece of equipment that controls or displays/ indicates reservoir levels should be considered critical. The procedure should establish the requirements for attention and response to alarms.

Alarm Response Procedures (Guides) should at a minimum include:

- a) Description of Alarm (Activating device, range and set point)
- b) Probable cause
- c) Automatic Operation
- d) Operator Action (immediate & follow-up, including actions to verify /establish cause)
- e) Documentation and communication of critical alarms (logbook, management)
- f) Reference drawings
- g) Reference procedures
- h) Revision date

- i) Position responsible for procedure

General Plant Actions regarding Alarms

Attention to Alarms

- Operations personnel should review and test critical alarms at the beginning of each shift.
- Management is to be aware of critical equipment operating with an alarm
- Critical alarm indicators shall be tested on a periodic basis (daily)
- Critical alarms shall be functionally tested on a periodic basis

Responding to Alarms

- Critical alarms shall be reviewed immediately upon annunciation
- Critical equipment shall not run in alarm without management approval.
- Information about unusual and critical alarms, including events pertaining to the alarm, alarm status, and actions taken are to be documented.
- Alarm set point modifications must be documented and reviewed by management

Alarm Maintenance

- Alarms shall be maintained with a high reliability and functionality
- Corrective actions for critical alarms should be assigned highest maintenance priority.

2. B.4.1 Reservoir Level Instrumentation

Provide a tool to define the sources of the alarm indicators and the appropriate operator response for alarms originating from critical reservoir related level instrumentation (conductivity probes, reservoir level devices, self check logic, rate of change checks, etc.).

2. B.4.2 Loss of Communication

Provide a systematic method to restore communication to reservoir level indication systems and operator responses in the event communication cannot be re-established. (e.g. visual observation and verification or shut down pumps)

2. B.4.3 Equipment Alarms

Provide a tool to define the sources of the alarm indicators and the appropriate operator response for reservoir equipment alarms (spillway gates, release structures, back up power equipment).

2. B.5 Preventative Maintenance

PM procedures are needed for all equipment and instrumentation for display of reservoir elevation, monitoring of project structures and for alarming or tripping of pump or generators.

Preventative maintenance procedures should be written, and scheduled on a repetitive basis for all instrumentation and equipment that is critical to safe operation of the reservoirs.

A procedure should be developed that references calibration of reservoir level instrumentation to civil structures that may be impacted by reservoir levels (crest of dam, over-pump spillway crest, spillway ogee etc.)

Preventative maintenance procedures should at a minimum include:

- a) Associated equipment, manufacturer, model #, references
- b) Tools required to perform maintenance
- c) Special equipment
- d) Parts and materials
- e) Initial conditions
- f) Precautions and limitations
- g) Instructions
- h) Post maintenance checkout
- i) Acceptance Criteria
- j) Signed verifications
- k) Position responsible for procedure

2. C. Design change/ Configuration Control Program

Each Pumped Storage project should have a design change/ configuration control program. This program should ensure the design basis of the plant is controlled and maintained through procedures and processes that assure unauthorized changes are not made to equipment important to safety. The facility design must be sufficient to support safe, reliable operations and be captured accurately on design documents such as drawings, electrical schematics and vendor-supplied documentation. Changes to design of equipment and computer controls must be identified, reviewed and approved by authorized personnel prior to implementation. This program should consider the following attributes:

- a) Procedures which define the processes for creating, reviewing, approving and implementing design changes to the facility,
- b) Design changes include but are not limited to changes to plant physical configuration, design basis, and setpoints for plant equipment or operating systems,

- c) Processes in place to prevent non-authorized design changes to the facility and commitment of the entire plant organization to not bypass the program,
- d) Engineering controls the design process to ensure the design and associated documentation meet applicable requirements and that design changes are properly evaluated prior to implementation,
- e) Provide a tiered approach which provides more review and control for items affecting dam safety and level controls,
- f) Engineering evaluation to ensure the design basis of the plant and level controls are maintained,
- g) Proposed design changes are independently reviewed by qualified personnel to determine their effect on the overall design and on any analysis upon which the design is based. Designs affecting multi-disciplines receive additional reviews by each discipline and by the operating authority.
- h) Authority for approving design changes is clearly defined,
- i) Records of design changes, including the reason for the change and the effects on existing design are maintained,
- j) Software that performs design functions or provides databases to support design functions is verified by independent calculation, test, or a combination of both and independently reviewed and approved prior to use. Revisions receive the same review and approval and are controlled,
- k) Temporary design changes are identified, pre-approved and controlled,
- l) Necessary post installation testing approved by the operating authority,
- m) Training documents affected by the design change are updated and personnel are retrained in an appropriate time frame,
- n) Operating and maintenance procedures are updated,
- o) Periodic testing and periodic maintenance activities are revised as appropriate for the design change,
- p) Document control program to ensure drawings, procedures, specifications, design basis documents, vendor manuals and technical instructions affected by the design change are maintained current,
- q) Measures are in place to control revisions to documents. Obsolete revisions are removed from use or marked to prevent use.

2. D. Organization and responsibilities

Pumped-Storage Projects should have an organizational structure with clearly defined roles and responsibilities for each position within the organization. The organization structure should be set up so that appropriate levels of checks and balances are provided to prevent changes to controls, operational procedure or dam safety related equipment from occurring without the review, approval, and documentation by the appropriate individuals.

The organization should have a person responsible for a Dam Safety Program. That person should have the authority to ensure that the project is operated and maintained in a safe manner in accordance with FERC regulations.

3. Instrumentation and Monitoring Equipment

In addition to the design basis considerations for instrumentation that is discussed in section 1 of this document, the following additional considerations should be considered regarding the design, testing, operation and maintenance of level instrumentation in a pumped storage plant.

Field instrumentation is essential for operational safety. Instrumentation of a pump storage hydro-electric facility provides necessary information to the controls to determine if the system is functioning as intended and supplies continuous monitoring of the system to warn of hazards. To prevent an overtopping event of a reservoir, the water level monitoring and protection instrumentation for the pump controls should be given high consideration. Since there are many various methods of monitoring water levels, the instrumentation system should be carefully planned and implemented to be effective against failure, and the system should account for the level of risk to the public.

3. A. Instrumentation design considerations

It is important to understand the parameters of the level instrumentation system when selecting the needed instruments. General considerations when selecting the instruments should be the environment in which the instruments will be placed, the type and the amount of data that will be produced from the instruments, how the data will be processed and project costs. The water level instrumentation should be of stout construction for long-term operation in harsh environments. Also, water level monitoring instruments should operate continuously and transmit accurate information to the pump/turbine controls quickly. The data that is collected from the instruments should not be excessive as to reduce the processing effort for the evaluator. Since most modern instrumentation data is electronically stored, processed and displayed, the task of interpreting all of the information has been simplified. This will allow the evaluator to make better judgments faster. Further consideration should also be taken for the instrumentation that is embedded within the structure itself to avoid future costly retrofit projects.

Refer to table Table 9-3.1.1 of the FERC [Engineering Guidelines for the Evaluation of Hydropower Projects](http://www.ferc.gov/industries/hydropower/safety/guidelines/eng-guide/chap9.pdf) manual for a description of advantages and disadvantages of common water level instruments.
<http://www.ferc.gov/industries/hydropower/safety/guidelines/eng-guide/chap9.pdf>

3. A.1. Alarms

Various alarm and indication schemes are installed in Pump Storage facilities to indicate and record the operation of selected equipment or instrumentation and to provide identification of equipment problems or hazards such that prompt corrective action can be undertaken. This is accomplished by the use of annunciators, SCADA, indication lamps, digital fault recorders, and sequence of events recorders.

3. A.2. Alarms vs. Tripping

The method of how the pumping units are governed must be evaluated for the amount of automation that is in place at each facility. A facility with continuous and competent staffing could safely operate with more warning alarms and less hard trips of the pumping equipment than an automated system. Each manned facility should have at least one trip mechanism in place. Automated facilities should have several tripping mechanisms in place to avoid over-pumping.

3. A.3. Communications Systems

The type of communications systems used to send and receive data/control/protection signals between the reservoir and the generators vary greatly. In some cases the signals/data travel through copper wires. The signals can be sent over phone lines or fiber optic cable. Other systems use microwave or satellite technology. Each technology has advantages and disadvantages. The hard wire option works well when the distances between the reservoir and the powerhouse are not great. The hard wire system can be susceptible to storm damage, lightning strikes and vandalism. Phone lines or fiber optic cable can be used in place of the hard wire option. The disadvantages are similar to the hard wire system. Microwave systems require an unobstructed line of sight. This can be a challenge in forested areas. Snow accumulations can also block microwave signals. Satellite systems are available but can be expensive. As the communications systems become more complicated, additional personnel are required to maintain the systems. The more complex the communication system, the more infrastructure will be required. Additional buildings with adequate heating and cooling may be required. Lightning protection for the communication equipment is recommended. In most cases redundant communications systems should be considered. The primary Communication System for transmittal of data from critical instrumentation should be hardwired circuitry. The potential for interference and/or failure is significantly less than radio transmitted signals. If redundant instrumentation is supplied, the second system could be radio transmitted signals, but the reliability would be a concern. If redundant systems are hardwired, consideration should be given to using separate wire-ways to reduce multiple failures from physical damage.

3. A.4. Time for Response

An evaluation of the design basis of the project time for response should be completed. This would include calculations of how long until overtopping occurs at various reservoir and pumping/generating levels. This table would be used to evaluate the fault tolerance/intolerance of the system, staffing, and the controls and shutdown design basis.

3. A.5. Security

The National Electrical Safety Code and other codes require that areas containing electrical supply conductors or equipment must be enclosed with fences or other barriers as to limit the likelihood of entrance of unauthorized persons or interference by them with critical equipment. Where facilities are located near residential areas, it is also desirable to attractively shield the station from the curious or critical eyes of passing motorists or neighbors. Public safety and the protection of facility equipment from vandalism are the main reasons for enclosing substations in fences.

3. A.6. Computer, Electronic, and Mechanical Controls

The type of control and protection system used at a facility varies widely and any type can be effective based on the level of staffing, redundancy, and risk of overtopping (i.e. amount of freeboard, site configuration).

Processing computers and PLCs allow for a much higher superiority when measuring the rate of change when filling an upper reservoir. The trending capabilities of these two systems can be easily set up to cover a wide timeframe for evaluation of anomalies. Other systems using chart recorders do not offer the same options, but the information can be valid if the systems are fully functional.

Generally, the higher level of processing computer systems offers the capability to provide the operator with the greatest amount of information in the quickest amount of time. PLC systems follow behind, but are limited in processing speed and data capabilities. Electromechanical controls have been a mainstay in our industry but generally require more interpretation by the system operator. Mechanical protection devices that prevent overtopping are also effective.

Any control and protection system is only as good as the quality of information it receives and the functionality of the system. Inadequate or poorly maintained instrumentation/control devices in the field can defeat the effectiveness of any system.

3. A.7. Power Sources and Reliability

The instrumentation system associated with the prevention of an over-pumping event should use a reliable primary power supply and be supplemented with standby generators or an uninterruptible power supply. The type, size and

maintenance of the power supply should be considered for the monitoring/control/protection systems to maximize reliability.

3. A.8. System Redundancy

An appropriate level of system redundancy should be provided to account for instrument malfunctions. The amount of instruments that are required should be based on the level of automation, potential for the loss of life, and financial and environmental risks. Redundancy of the system also provides different means of tracking similar metrics, which improves the accuracy and credibility of the instrumentation.

3. B Testing/ Calibration/ Operation

3. B.1 Calibration of Levels

The calibration of Reservoir Level Monitoring/Control/Protection Equipment should be part of the Preventative Maintenance Program and findings should be documented to create an equipment history.

3. B.1.1 Weekly Calibration/Verification

Instrumentation for measuring Reservoir Level should be verified on a regular interval, usually weekly, comparing the measured value of the instrument(s) to a known source such as a fixed gauge.

During verification, the system should be visually inspected for structural or mounting deficiencies and/or physical damage that could affect the accuracy of the instrumentation.

3. B.1.2 Monthly Calibration/Verification

Monthly checks of instrumentation used for measuring Reservoir Level should include all items covered in the weekly checks. Additionally, calibration of the instruments should be checked over their entire measurement range to insure their capability to react to a change in level. These calibrations should include the entire circuit loop from the measuring instrument to the monitoring, control, or protection devices.

3. B.2 Visual Surveillance

On site observation by the hydro plant operators is the best choice for reservoir monitoring. For most pump storage operators/owners this is not a viable option. The next best option is the use of video cameras. Cameras that can view a lighted staff gage or some other form of actual elevation indication are used in the industry. The technology in this area has improved significantly and all but the most remote sites can be effectively monitored by video cameras. The

cameras can also function as part of a general reservoir security plan. If the pump storage operators/owners relies on visual surveillance of reservoir elevation as the primary source of data then redundant cameras, power sources and communications paths is recommended.

3. B.3 Functional Testing vs. Simulation

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.

3. B.3.1 Functional Test Frequency

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

3. B.4 Testing of Alarms

All controls and alarm systems that relate to a system that is important to dam safety should be tested prior to using them to operate the project. This should be determined by the design basis analysis.

3. B.5 Credibility of Instruments and Outputs, Instrument checks

The more critical or accurate a data quantity is to the overall operation, the more important it is to assure the value is within an acceptable accuracy. This section identifies several possible ways to determine degraded accuracy. When degraded accuracy is determined, the expected result is that effort to resolve the problem and return the system to its original designed fault tolerance level occurs soon. Error detection of variable sensing quantities, like water level and flow, can occur by many mechanisms. The following subparagraphs are intended to help power plant personnel consider what is possible and reasonable.

3. B.5.1 Comparable Quantities Credibility

Variables, like MW's, can be compared to other inputs. For example, a critical process that has at least three similar inputs can be set up to automatically reject or identify an input that is not tracking and continue the control process using the unaffected equipment. If only two inputs are used or remain functional, it is impossible to select between them without further observation to judge which element is the good device.

3. B.5.2 Basic Credibility of Instruments and Outputs

Each device or configuration usually has normal bands of operation and ranges that are not expected. Unexpected ranges should be flagged for attention when they occur. If possible, the sensor should be selected and calibrated so that failure modes that result in no output, or full scale output, will not be within normal operation ranges. That way, if the unit fails to one of those levels, it is easy to automatically determine that the input is malfunctioning.

3. B.5.3 Correlated Information

A hydro unit generating or pumping at a specific MW amount will pass a given amount of water. That amount of water use can then be used, with a known pool configuration, to calculate the expected reservoir level change over time. An alarm may be produced if the rate-of-change range calculated is not what was observed by direct level readings over time. If inflows other than pumping are accurately known, they are combined with pumping flow and reservoir curves, to determine expected reservoir level change. A reservoir change that is not tracking within a predetermined range indicates a problem somewhere

3. B.6 Control Survey

The early detection of structural deformation is critical for safety. If a problem is detected, actions may be taken to minimize the weakening of the structure such as lowering water levels, until the problems can be properly addressed. Benchmarks for a control survey should be placed on and off site and referenced to an established survey monument.

3. B.7 Preventative Maintenance

An instrumentation system must be maintained during its service life to function reliably. Poorly maintained instruments will increase the risk of inaccurate data and system failure. For some elements, preventive maintenance is not necessary because there is sufficient redundancy to vote the non-functioning value out and use remaining input values. The equipment should be repaired soon though, so that a second and more critical failure is unlikely to occur. Maintenance and recalibration procedures should be performed and scheduled as per manufactures' recommendations. The owners' personnel that is responsible for the maintenance should be competent and be adequately trained on how the facility and the instrumentation functions. Since most instrumentation has warranty periods, the option of purchasing a maintenance contract from a reputable company may be a worthy consideration. All records of data gathering, maintenance and recalibration should be kept by the Owner. This service record could be used to establish a general behavior of each site.