ENGINEERING GUIDELINES FOR THE EVALUATION OF HYDROPOWER PROJECTS

CHAPTER 17 – POTENTIAL FAILURE MODE ANALYSIS

DECEMBER 16, 2021

FEDERAL ENERGY REGULATORY COMMISSION
888 First Street NE
Washington, DC 20426

Revision Log		
No.	**Date**	**Description**

TABLE OF CONTENTS

LIST OF FIGURES

No table of figures entries found.

LIST OF TABLES

ABBREVIATIONS

BOR	U.S. Department of the Interior, Bureau of Reclamation
D2SI	Division of Dam Safety and Inspections (FERC)
DSSMP	dam safety surveillance and monitoring plan
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
MFU	major findings and understandings
ODSP	owners dam safety program
PFM	potential failure mode
PFMA	potential failure mode analysis
RIDM	risk-informed decision making
STID	Supporting Technical Information Document
USACE	U.S. Army Corps of Engineers

Page intentionally left blank

17-1 INTRODUCTION

17-1.1 General

A Potential Failure Mode Analysis (PFMA) is a process used for safety evaluations of dams and project works. Traditional dam safety evaluations have tended to focus on a limited number of "standards based" concerns such as hydraulic capacity of spillways and stability of structures under a set of pre-defined loading conditions. PFMAs are intended to broaden the scope of the safety evaluations to include potential failure scenarios that may have been overlooked in past reviews and evaluations. A PFMA is an exercise to identify all potential failure modes (PFMs) under normal, flood, earthquake, and other (ice, reservoir sedimentation, etc.) loading conditions, including all external loading conditions for water retaining and conveying structures, and to assess those potential failure modes that are significant enough to warrant continued awareness and attention to visual observation, monitoring, and remediation, as appropriate.

A PFMA is a method of analysis where particular flaws and initiating conditions are postulated and the analysis reveals the full range of effects of the flaws or the initiating condition on the system (USACE, 2014). Each method of failure is identified, described, and evaluated on its credibility and significance. Potential failure modes are a way that failure can occur, describing the means by which element or component failures must occur to cause loss of the sub-system or system function. The potential failure mode encompasses the full sequence of events from initiation (cause) through the ultimate failure effect of interest to include physical, operational, and managerial systems.

17-1.2 Definitions

The following definitions are provided to ensure that all readers have a common understanding of the terms commonly used in this document.

Failure – For the purposes of the PFMA, failure is defined as an uncontrolled release of the reservoir, in whole or in part; the inability of project features or components to perform their intended function; or project features or components performing in an impaired or compromised fashion; any of which results in an adverse consequence. This includes misoperation of project elements. Additional details are provided in Section 17-2.1.

Potential Failure Mode (PFM) – A way that failure could occur (i.e., the full sequence of events from initiation to the failure condition) for a given loading condition. Potential failure modes that result in unintended releases of water, such as the Folsom Dam radial gate failure, or potential failure modes that lead to a structure not performing or functioning as designed, such as the Oroville spillways incident, are also considered.

Potential Failure Mode Analysis (PFMA) – The process utilized to determine the potential failure modes pertinent to the structure under investigation.

Major Findings and Understandings (MFU) – The most significant items learned by the participants in the PFMA session regarding such items as the design, construction, performance, operations, and safety of the dam or feature.

PFMA Report – The document prepared to capture the information, evaluations, results, and conclusions developed during the PFMA.

Credible – A term used to indicate that a potential failure mode is considered to be physically possible and the likelihood of the potential failure mode is not considered so remote as to be negligible.

NOTE: *While this Guideline discusses the PFMA as it applies to dams and other project features, many of the subsequent sections refer to "dam" instead of "dams and other project works." This is done for brevity and is not meant to exclude other project features from the PFMA process.*

17-1.3 Purpose

A PFMA is an examination of "potential" failure modes for an existing dam or other project work(s) by a team of persons qualified by experience and training to evaluate a particular structure. It is based on a review of existing data and information, firsthand input from field and operational personnel, a site inspection, completed engineering analyses, identification of potential failure modes, failure causes and failure development, and an understanding of the consequences of failure.

The PFMA is intended to provide enhanced understanding and insight on the vulnerabilities related to performance associated with the dam. This is accomplished by including and going beyond the traditional means for assessing the safety of project works and by intentionally seeking input from a diverse team of individuals who have information on the performance and operation of the dam. A PFMA includes and uses all of the available data and information from standard engineering analyses of an existing dam.

According to federal guidance (FEMA, 2015), "[t]he goal of a potential failure modes analysis is to: (1) identify the site-specific credible potential failure modes for a given dam; (2) provide complete descriptions of the potential failure modes, including the initiating event and the progression of steps leading to an uncontrolled release of the reservoir; and (3) provide a general description of the magnitude of the breach, including identifying and recording the factors that make the potential failure more likely and less likely and the consequences more severe or less severe." It should be noted that the FEMA statement above does not reflect the revised guidance regarding the expanded definition of failure as provided in this document.

The goal of a PFMA is to provide input and become the foundation of the management of dam safety activities. The key to a successful PFMA is the development of detailed and

descriptive potential failure modes that provide the owner with an understanding of any potential weaknesses that may exist at the project that then allows the owner to evaluate, monitor, and take actions to reduce the possible threat to dam safety.

17-1.4 Value of PFMA

Utilizing an intensive team inquiry process beginning from a basis of no preconceived notions, the potential failure mode examination process has the ability to:

- Enhance the dam safety inspection process by helping to focus on the most critical areas of concern unique to the dam under consideration;
- Identify operational related potential failure modes;
- Identify structural related potential failure modes (e.g. internal erosion) not covered by the commonly used analytical methods (e.g., slope stability, seismic analysis);
- Enhance and focus the visual surveillance and/or instrumentation monitoring program;
- Identify shortcomings or oversights in data, information or analyses necessary to evaluate dam safety and each potential failure mode;
- Help identify potential dam safety risk reduction measures; and
- Document the results of the study for guidance on future dam safety inspections. By updating the documentation (as a living document), the benefit of increased understanding and insight lives on.

There are other outcomes that result from carrying out a PFMA in the manner described in this guidance document:

- The process of searching out all the information about the dam for the specific purpose of identifying potential failure modes (plus the involvement of a diverse group of people in the PFMA process) typically results in uncovering data and information that was previously unknown to most personnel currently involved in the dam's safety evaluation. Frequently this information plays an important role in identifying a potential failure mode.
- Credible potential failure modes and failure scenarios will be identified and documented for use and consideration.
- Certain problems, issues, and concerns that have been associated with the dam may be found to be of lesser significance than previously perceived from the standpoint of consequence, remoteness, or physical possibility.

- Enhancements to the monitoring and visual inspection programs are recognized and readily developed. Monitoring efforts can become more focused on the identified vulnerabilities.
- A wide range of persons (from the dam tender to the owner's dam safety program manager) become aware of the dam's most significant vulnerabilities and the relationship of the surveillance and monitoring programs to these vulnerabilities.
- Gaps in data, information, or analyses that prevent characterizing the significance of a potential failure mode are recognized and identified for consideration and possible action by the owner.
- Risk reduction opportunities applicable to the Dam Safety Surveillance and Monitoring Plan (DSSMP), operations, structure response, or emergency preparedness are recognized and identified for consideration by the owner.
- It provides the opportunity to easily and effectively educate all who are concerned with the dam (dam tender, owner, regulator, periodic reviewers, inspectors, designers, and others) about:
    1. The potential failure modes for the project or structure;
    2. How monitoring, including use of specific instrumentation and visual surveillance is used to look for specific symptoms, behaviors, or evidence that might provide advanced signs of a developing failure for the identified potential failure modes;
    3. How "general health" monitoring (e.g., crest monitoring, piezometers) is used as basic data to help watch for conditions that have not been previously identified as potential failure modes;
    4. How operations (i.e., regulated, normal, unusual) of this dam and others upstream and downstream may influence dam safety; and
    5. When operational scenarios or situations may require intervention or emergency actions.

17-1.5 Challenges of PFMA

The PFMA process is recognized as an improvement over strictly traditional deterministic engineering analysis approaches but, like any analysis method, it has challenges that must be identified, addressed, and overcome, some of which include:

1. It is difficult to be fully comprehensive. Many factors contribute to this, such as:
    a. There can be a lack of creativity by the PFMA team members in imagining all the ways the elements and components of a project can interact that can lead to failure or some unintended consequence.

b. The linear chain-of-events approach in developing potential failure mode pathways and events can make it difficult to envision or capture "jumps" or other potential failure mode pathways or dependencies that might not be obvious.

2. If the process does not follow a structured approach, it can lead to overlooking or missing potential failure modes or misrepresenting or improperly assessing the importance of the potential failure modes.
3. The robustness of the results can be very dependent on the experience and breadth of project team. Important or critical potential failure modes can be missed by teams comprised of inexperienced personnel or those that do not include sufficient knowledge and experience in the technical and operations disciplines represented by the project.
4. Because much of the PFMA session is conducted in a group setting, the results can be susceptible to a variety of adverse group dynamic factors. Experienced facilitators must be knowledgeable of such factors and be vigilant in correcting these when they occur.
5. If not properly scoped or scheduled, PFMA sessions can have insufficient time or resources to complete the required work. This can result in short-changing the process that can lead to missing or misrepresentation and assessment of potential failure modes.
6. Project reports and information may be lacking or may not be available that can prevent the team from understanding the structure in sufficient factual detail to identify or evaluate the potential failure modes.

Other criticisms of the PFMA process are often simply a misunderstanding of the purpose and intent of the process. At times some might expect a result or outcome of the PFMA process that is not in line with the objective of the PFMA process. Some expect more out of the PFMA process than what is intended (e.g., the ability to prioritize the urgency and actions of each potential failure mode, providing a short-list of less than five (or some other small number) potential failure modes requiring some form of action or follow up, etc.). The PFMA process is intended to identify, describe, and evaluate potential failure modes so that resulting dam safety activities can be identified. It is an initial step in the dam safety risk management process. Other than very coarse sorting, the results of the PFMA process are typically not able to distinguish priorities of dam safety activities (a risk analysis is required to achieve that particular goal).

PFMAs require periodic review and updates; it does not remain relevant if left unmaintained. The inputs, assumptions, evaluations, and results of a PFMA must be reviewed and updated on a periodic basis to incorporate:

- changes in understanding of the project from the gathering of new/updated information and analyses;
- physical or operational changes to the structures or components at the site;
- changes in project condition (i.e., loading, deterioration or aging, etc.);
- changes in understanding of engineered systems;
- advancements in technology and experience, including lessons learned from dam safety incidents and failures; and
- changes in project personnel and operating staff.

17-2 SCOPE OF PFMA

17-2.1 Expanded Definition of Failure

The PFMA includes an evaluation of all the project features and components that could result in a failure, as defined above, that could result in an adverse consequence.

All project features and components – not only common or predominant project features, but also those appurtenant features and components that are integral to the design, operation, and performance of the project (e.g., spillways, canals, outlet/discharge systems, penstocks, intakes, and non-overflow structures, etc.).

Inability to perform their intended function – inability to carry out the designed or desired purpose of the feature or element.

Impaired or compromised fashion – e.g., gate hoist or hydraulic pump fails or fails to perform as designed resulting in physical damage or operational limitations (reduced pump performance increases time to open gates in a timely manner that could lead to an increased rate of rise of the reservoir and an inability to access other gate controls or overtopping of an embankment or other adverse consequences).

Adverse consequence – any negative unintended result produced by a cause or from a set of conditions. Adverse consequences can include complete or partial loss of the reservoir, loss of human life, environmental losses, economic or financial losses, loss of cultural or historical features, loss of recreation benefits, loss of integrity/respect for the dam owner/operator, and others. Adverse consequences can be caused directly or indirectly. Adverse consequences can result from a component failure that leads to damage or inability to operate another critical component of a system resulting in an adverse consequence up to and including failure of the dam resulting in loss of the reservoir and loss of human life.

17-2.2 Approach

A PFMA is intended to be a robust investigation and evaluation to identify and assess the possible vulnerabilities of project elements, components, or structures that could fail and result in an adverse consequence. It requires a thorough understanding of the project features and components and how those elements interact and function as a system, anticipated (design) loading conditions and frequency, project operations, monitoring capabilities, project communication, and influence of human and organizational factors in operation and decision-making. The PFMA must include all design and anticipated loading conditions through the full range of loading.

Because of the complexity of dam systems, component and system complications, and system interactions and dependencies, different approaches to identifying and evaluating potential failure modes are generally required. These approaches may include:

1. Event tree approach, which is generally characterized by potential failure mode progression in a sequential chain-of-events;
2. Failure mode and effects analysis, which is used to map out the consequences of specific events that can occur during operation of an engineered system; and
3. Fault tree analysis, which is a construct that shows the logical interaction among the elements of a system whose failure, individually or in combination, could contribute to the occurrence of a defined undesired event such as a system failure.

The event tree approach has long been the predominant approach used in PFMAs in dam safety in the United States. This approach works well for potential failure modes in which a logical sequence of events from an initiating event to the complete set of possible outcomes can be described. For complex systems and systems with multiple interactions (mechanical, electrical, human influences, etc.), the failure mode and effects analysis and the fault tree analysis approaches allow for a more comprehensive understanding and systematic evaluation of the functional elements of the system to better identify and evaluate potential failure modes. Additional information on the three approaches is documented in Hartford and Baecher, 2004.

Each of these approaches has advantages and disadvantages when applying them to PFMAs.

17-2.3 Human and Organizational Factors

The PFMA must include the potential contribution and influence of human and organizational factors, such as organizational culture and decision-making authority and practices, and how these factors can contribute to failure. The propensity toward failure is determined by the balance of factors that contribute to failure versus safety. In general, the human factors contributing to failure include three categories of primary drivers (Alvi, 2013):

- Pressure from non-safety goals, such as achieving functional design, reducing cost, increasing profit, meeting schedules, engaging in competition, building and maintaining relationships, pursuing political objectives, and following personal agendas.
- Human fallibility and limitations due to misperception, faulty memory, incompleteness of information, lack of knowledge, unreliability of intuition, inaccuracy of models, cognitive biases operating at a subconscious level, use of heuristic shortcuts, adverse effects of emotions, and fatigue.

- Complexity, resulting from multiple interactions of multiple components, which exacerbates the other drivers and can result in nonlinearly large effects from small causes, as well as difficulties in modeling, predicting, and controlling structural behavior.

These primary drivers of failure lead to various types of human errors – e.g., slips, lapses, and mistakes – as well as compromised risk management due to ignorance, complacency, and overconfidence.

A fundamental human factor that helps prevent failures is an overarching dam safety culture, which entails individuals at all levels in organizations placing value on safety, having a humble and vigilant attitude, and conscientiously implementing best practices (i.e., the Owners Dam Safety Program (ODSP)). With respect to general design features, these best practices include conservative safety margins; structural redundancy, robustness, and resilience; and controllable potential failure modes. Organizational and professional best practices include:

- Sufficient staffing and reasonable schedules.
- Peer review and cross-checking.
- Thorough documentation and effective information-sharing, including allowing dissent, in order to 'connect the dots' on project issues.
- Creating teams who bring in diverse perspectives, while also having effective and continuous leadership.
- Recognizing knowledge limitations, deferring to expertise, and engaging in training.
- Using checklists.
- Careful structural modeling and use of software.
- Meeting professional, ethical, and legal/regulatory standards.
- Learning from failures.
- Promptly and effectively detecting, investigating, and responding to warning signs, including after extreme events and during "quiet periods."

Additional information on human and organizational factors is included in Appendix 17-A.

17-3 APPLICATION

17-3.1 PFMA Types

A PFMA is to be conducted for:

1. Part 12D PFMA. All FERC-regulated dams that are required to undergo Independent Consultant safety inspections, as defined in 18 CFR Part 12, Subpart D, are required to perform a PFMA and Level 2 risk analysis at the comprehensive assessment cycle. Refer to Chapter 16 of the FERC Engineering Guidelines for more specific information on PFMAs for a Part 12D Comprehensive Assessment.

2. Risk Analysis PFMA. A PFMA is the first step in conducting a semi-quantitative and quantitative risk analysis for an existing dam or a risk reduction action. A significant increase in dam safety awareness can be developed from this step. Thorough potential failure mode identifications and complete descriptions will lead to a more efficient risk analysis process. Interim risk reduction measures and study plans can be effectively developed based on the results of the PFMA.

3. Design Modification PFMA. If required by a Regional Engineer, a PFMA is to be conducted prior to major modifications or remedial work on a structure. The purpose of the PFMA is to identify and evaluate those potential failure modes that are the result of or potentially affected by the recommended modification/ remediation plan. **The design modification PFMA is generally not required to look at the entire project.** Before a PFMA can be conducted for major modifications or remedial actions, the design must have progressed to the point of a recommended alternative. The design for the proposed modification should be at least to the 60-percent level to enable the PFMA team to critically evaluate the modification for potential failure modes and to determine if construction of the recommended alternative may adversely impact other structures, resulting in new potential failure modes not considered in the pre-existing PFMA. Conceptual designs would not be adequate for this evaluation as they may undergo significant modifications during the design process, which might trigger the requirement for additional PFMAs. A PFMA may also be useful for the design team to evaluate design alternatives, but such an evaluation is not required. Potential failure modes that can result from construction-related activities, if they are known at the design stage, should also be incorporated into the design PFMA.

4. Construction PFMA. If required by a Regional Engineer, a PFMA is to be conducted prior to or during construction when the contractors proposed means and methods have the potential to adversely load or otherwise potentially compromise the structure. A construction PFMA is performed after the designs (drawings and specifications) have been completed and the contractor has been selected and has developed proposed construction sequences and procedures to

perform the work. A construction PFMA does not need to be performed for every project. The construction PFMA should include design and construction personnel familiar with the project, the proposed designs, and the planned construction activities with an emphasis on those construction activities that may result in the formation of new potential failure modes due to the construction activities (either temporarily during the construction period or could remain after construction) or exacerbate existing potential failure modes. The construction PFMA must be performed far enough in advance of the construction activities so potential modifications that might result from the PFMA can be incorporated into the construction work with the least amount of impact.

5. Post-Construction PFMA. If required by a Regional Engineer, a PFMA is to be conducted after the completion of major modifications or remedial work on a structure. The purpose of the PFMA is to evaluate the actual conditions encountered during construction, the construction methods and features as a result of the construction activities, and any design changes that may have taken place during construction. Before a post-construction PFMA can be conducted for major modifications, the construction documentation must have been completed (as-built drawings and construction summary reports). It is preferred that initial monitoring information is also available, covering a full cycle of typical reservoir operations (i.e., at least one calendar year).

A PFMA may be required for other projects or for other purposes as requested or required by the Regional Engineer.

17-3.2 Design and Construction PFMAs

Implementation of new designs and performance of construction activities have the potential to create: (1) new potential failure modes, (2) positive or adverse impacts to existing project potential failure modes, and (3) potential failure modes due to temporary construction activities. Each of these three types of potential failure modes should be considered, as applicable, during design or construction PFMAs. More specifically, design and construction PFMAs should consider, as applicable:

- New or impacts to existing potential failure modes due to new project features created by the design and construction.
- New or impacts to existing project potential failure modes due to modifications to existing project features created by the design and construction.

Potential failure modes associated with construction activities should also consider, as appropriate:

- Potential failure modes associated with temporary structures, like cofferdams, braced excavations, temporary bulkheads, etc. and their potential impacts to existing or new project features.
- Potential failure modes to new or existing structures caused by specific construction activities or modifications, like pressure grouting, dewatering, cutoff wall (barrier wall) installation, etc.
- Potential failure modes of existing structures due to changes in loading magnitude or frequency, or reduction in capacity during or after construction.

Design and construction PFMAs should be strategically scheduled at such a time as sufficient information is available to evaluate important design and construction details and methodology yet not too late as to require substantial reworking of plans and details that may result from changes to the design and construction as may be identified from the PFMA process.

The findings of design and construction PFMAs should be incorporated in a timely fashion into revised design and construction details, plans, and methodologies. Documentation of design and construction PFMAs should follow the guidance provided in Section 17-4.8.

17-4 CONDUCTING A POTENTIAL FAILURE MODES ANALYSIS

17-4.1 General

The primary product and the main focus of a PFMA is identifying and obtaining a clear understanding of each element, component, and structure for a given project and its site-specific potential failure modes. At the outset of the PFMA, the entire team must understand that the product of the exercise is not a decision document, but rather an informational resource document, developed from the combined input of the team, that is intended for use and reference for many years.

The potential failure mode "identification" is intended to go beyond a simple generic statement of the potential problem (e.g. operations, slope instability, foundation, overtopping, liquefaction, etc.). The potential failure mode identification, examination, and description must provide background information on the loadings, structural conditions, circumstances, and events at each site that identify why this potential failure mode is being considered for this site. Also, the significance of the potential failure modes for the site must be discussed in terms of the need for awareness, surveillance and monitoring, analysis and investigation, or for making operational changes, structural repairs, or modifications.

The PFMA process is a guide to help focus routine dam safety activities such as dam safety inspections and monitoring activities, as well as foundational elements for risk analyses. Both activities require and benefit from a comprehensive review and discussion of **all** available information (historical records and photos, engineering analyses, previous inspection reports, etc.). Hence, the detailed reviews commonly done prior to a dam safety inspection are still necessary. Linking the outcomes of the PFMA and dam safety inspections is efficient and effective because it allows others, not often in the direct safety evaluation loop, to participate and contribute to the outcome.

17-4.2 Overview of PFMA Process

Specific steps and actions for carrying out a PFMA for a dam or project are provided below and these steps are recommended, as a minimum, for a PFMA to be comprehensive, consistent, and complete. In completing these specific steps, it is very important that the principles of the process be thoroughly understood and followed in order for the full value of the process to be achieved. These principles include:

- Diligence in searching for and obtaining all the project background information;
- An open, investigative approach toward identifying and understanding PFMs and failure scenarios;
- Dedication of the assigned persons to the reading and understanding of all the background information on the dam prior to the PFMA session;

- Documentation is the key to capturing the insight and ideas resulting from the process; and
- Willingness of all parties to set aside their normal responsibilities and daily duties and focus on what the data, information, and experience/knowledge of individuals can teach us about the dam.

Advance planning is imperative to ensuring a successful PFMA. Some questions that should be addressed prior to conducting a PFMA include:

1. What technical disciplines should be represented on the PFMA team?
2. How many people are expected to attend the PFMA session?
3. How many days or weeks is the PFMA session expected to last?
4. Should the PFMA session be split into multiple weeks to adequately cover multiple structures?
5. What size of meeting room will be needed for the PFMA session?
6. Can the PFMA session be conducted using a virtual, web-based platform or does it need to be an in-person, face-to-face meeting?
7. What equipment and technology (e.g., Wi-Fi, multiple projectors, whiteboard, easels, hard copy drawings, etc.) should be available to ensure all participants are engaged and productive during the PFMA session?
8. Are there special considerations that should be accommodated in the PFMA session?

The Licensee should discuss these and other questions with dam safety professionals from FERC during the initial planning phase of the PFMA. Once the key members of the PFMA team have been identified and selected, these questions should be revisited, and plans adjusted accordingly.

The six general steps in the PFMA process include:

Step 1 Identify the PFMA Team participants.

Step 2 Collect background information on the project. Collect all data, studies and information on the investigation, design, construction, analysis, performance and operation of the project. All existing studies and investigation reports that relate to the ongoing safety of the dam must be included and reviewed and evaluated. A list should be made of the data available for review and considered in the PFMA and the reference list included in the PFMA report documentation.

Step 3 Perform comprehensive review of all background data on the project. The PFMA team, experienced in dam safety evaluation (familiar with dam failure mechanisms), is to review all the background information for general understanding and with these specific questions in mind:

- How could this dam or component fail? (Site-specific consideration of loadings, structure condition, and project operations)
- What happens if the dam or component fails?
- Are the identified potential failure modes recognized and being appropriately monitored by visual surveillance or instrumentation?
- What actions (immediate or long term) can be taken to reduce dam failure likelihood or to mitigate failure consequences? These actions could include any of the following: data collection, analysis or investigations, operational changes, communication enhancement, monitoring enhancement, and structural remediation measures.

Step 4 Conduct site review. This includes interviews with key owner personnel at the project, visiting the project site, and performing an inspection with a focus on potential failure modes. The site review should include observations of structural and geologic conditions, a review of project operations, and interview(s) with the project owners/operators for their input on potential failure modes.

Step 5 Conduct the PFMA session. This includes identifying potential failure modes and failure scenarios with the group of persons most familiar with design, analysis, performance, and operation of the dam. Record the identified potential failure mode, the reasons why each potential failure mode is favorable / less likely and adverse / more likely to occur and identify any possible actions related to each that could help reduce risk (i.e., reduce loading frequency, monitoring enhancement, investigation, analysis, increase detection and/or warning time, remediation, etc.). Also, specifically identify possible surveillance and monitoring enhancements and risk reduction measures for each potential failure mode.

Step 6 Document the PFMA. This includes immediately recording the major findings and understandings from the brainstorming session.

The following sections describe each step, in detail.

17-4.3 Identification of the Potential Failure Mode Analysis Team Participants

17-4.3.1 General

The PFMA participants (team members) consist of a diverse group of individuals with varying backgrounds and responsibilities. Except as provided below, these are persons who have prior experience with the evaluation, design, construction, analyses, performance, and operation of the dam, or who will obtain knowledge of the project through reading of the background material. The primary advantage of having a variety of people participate in the PFMA process (and it is a very significant advantage) is that as more ideas and more questions are put forward, the more knowledge and information is available, and a greater diversity of opinion is input to the process. The qualifications of the team members should be commensurate with the complexity and diversity of the project features and the magnitude of the potential consequences.

If the PFMA team has been chosen properly, they will participate in the workshop with the appropriate expertise, an open mind, and a willingness to achieve the best possible results. This type of approach reaches a better conclusion than any of the individual members could have on their own and it is intended to reveal all potential dam safety concerns related to the project.

17-4.3.2 Roles and Responsibilities

Some of the team members have specific roles and responsibilities and need to have the requisite experience and capability to fulfill these roles. The roles and requirements of the team members are given below:

Team Leader – The dam owner should designate a member of their staff or a designated appointee as the team leader who is responsible for coordination of the PFMA activities, including collection of the background information; coordination of the site visit and PFMA session meeting dates, location, and logistics; follow-up actions from the PFMA session; and coordination of the preparation and review of the PFMA document.

Facilitator(s) – A facilitator (or co-facilitators) is required to facilitate the PFMA session. The facilitator (or co-facilitators) also peer reviews the PFMA report. The facilitator's role in a PFMA is the most critical to the entire process and requires a significant amount of preparation. It is ideal for the facilitator to have read all the documents regarding the project. It is the role of the facilitator to lead the group discussion during the finding of facts and discovery of all pertinent information when discussing and developing a potential failure mode. Without a good understanding of the project, it makes it more challenging for the facilitator to draw the information out of the team members that is required to fully develop and understand a potential failure mode. It could be argued that the facilitator should be able to develop each potential failure mode by themselves, and while this could potentially be the case, there is no way they could know everything the team members know that is not included in the

documentation, based upon their individual experiences and daily dealings with the project. It is also critical for the facilitator to remain an impartial arbiter and not become just another member of the PFMA team.

The facilitator is responsible for the flow of the workshop to ensure that everyone stays focused and that the participants do not get sidetracked by discussions that are not relevant to the point at hand. As can occur from time to time, sidebar conversations can develop during the group discussion. While these conversations may be relevant to the PFMA discussion, most often it is important that these sidebar conversations are prevented and only those conversations that are applicable to the discussions at hand are redirected to the entire group, so everyone has the same information. The facilitator is responsible for ensuring that all important facts are recorded for incorporation into the discussion during the workshop as well as the final PFMA report.

Core Team – The core team comprises select individuals who form the nucleus of the PFMA team. Core team members are responsible for:

- Reading the project background information and documentation,
- Participating in the site review,
- Attending and participating in the PFMA session, and
- Reviewing and providing comments on the draft PFMA report.

Unless otherwise approved by the facilitator, **the core team members are the only PFMA team members that provide input and recommendations for the screening of the individual potential failure modes**, as discussed in Section 17-4.7.8. In order to maintain their independence and not bias the group, **facilitators do not provide input and recommendations for the screening of the individual potential failure modes**.

The core team generally consists of the following persons:

- Independent Consultant(s) who have completed a recent Part 12D report or are scheduled to complete the next Part 12D inspection, as well as any additional members of the IC Team, may serve as core team participants. See Chapter 16 of the FERC Engineering Guidelines for more information regarding the role of the ICs during a Part 12D PFMA.
- Technical representative(s) of the owner's staff (i.e., owner's chief dam safety engineer, other dam safety personnel) and/or their consultants.
- Subject Matter Experts. Competent, experienced scientific, engineering, and operational professionals representing technical disciplines and operations needed to fully evaluate the design, construction, operation and maintenance of the project features and components. The number and experience of the professionals should

be commensurate with the complexity of the project and magnitude of the potential adverse consequences. The effectiveness of the process is dependent on the technical understanding of the potential failure modes that are developed and evaluated by the team. Complex components or systems (gates, SCADA systems, etc.) may require additional specialized expertise. These may also be approved members of the IC Team.

The team leader may or may not be assigned by the owner as one of the designated core team members. This is because the coordination and logistic activities may keep the team leader from being able to meet the review of background material requirements. If the owner and team leader consider that this may be the case, another representative of the owner should be designated to participate in the core team review of all the background material.

The core team members and technical representatives of the owner's staff are specifically assigned the responsibility to read and review all the project background material. Subject matter experts are recommended to read and review all the project background material; however, as a minimum, they must read and review the project background material that is relevant to their technical expertise.

Note taker(s) – The note taker is perhaps the second most important person in a PFMA session (other than the facilitator). It is the responsibility of the note taker to capture, in writing, the key discussions and concepts during the PFMA. A good note taker can capture a group discussion in a few sentences and does not attempt to simply record each statement made. Comprehensive notes are of utmost importance as they form much of the content of the PFMA report and record the key inputs, assumptions, and thoughts of the subject matter experts in building the case for the results of the risk analysis.

The note taker should make sure all notes are clear and capture the discussions of the group, including the intermediate decisions that are made prior to moving on to the next subject. It can be helpful if the note taker uses a computer projector to display the notes in real-time during the meeting. This helps the participants see what is being captured and ensures the notes adequately capture the information, intent, and decisions. (A word of caution: the PFMA team members must not get caught up in wordsmithing each word of the notes. Otherwise, the meeting will get bogged down and progress will come to a halt. Team members should ensure that the recorded information is accurate, but wordsmithing should be reserved for reviewing the final report.)

Other tips:

- Taking notes during a PFMA meeting is distinctly different than administrative note taking. It is extremely helpful if the note taker is an engineer with knowledge of the project in general. This is important because the note taker must be familiar

with engineering terms and concepts so that they can be appropriately and timely captured during the discussions.

- It can be more efficient if the note taker is the primary author of the PFMA report. This provides an added motivation of the note taker to record good notes and can improve the quality of the final product.
- It is also important to identify a backup or secondary note taker to supplement or provide a backup set of notes in case the primary note taker becomes distracted or cannot be present.
- If a projector is used to display the notes real-time, consider having them on a separate projector from project drawings, photographs, etc.

FERC Dam Safety Professional(s) – Dam safety personnel from FERC must attend and participate in the PFMA. FERC personnel are responsible for providing technical and regulatory oversight of the PFMA session. FERC personnel will provide input when the team misses or has incorrect information and will inform the owner's representative(s) and facilitator when the PFMA process is not following established FERC guidelines. FERC personnel may suggest candidate potential failures during the brainstorming session, may suggest more likely/less likely evaluation factors, and may suggest interim risk reduction measures and dam safety management activities if such information has not been discussed by the PFMA team. FERC personnel may ask clarifying questions related to the information discussed, figures presented, etc. in order to ensure the factual project information is being presented.

FERC personnel will provide comments regarding the screening of potential failure modes when, in the opinion of the FERC personnel, the core team has not adequately justified the screening of the PFM. The lack of comments by FERC personnel during the PFMA workshop does not indicate acceptance or approval of the team's findings.

Operations and Maintenance Staff – In formulating the team it is important to include individuals with intimate knowledge of the project operations and structures, especially the senior dam tenders and those responsible for collecting monitoring data. The PFMA sessions should include the project's key operating staff who will be able to clarify operating rules and procedures and will learn about the failure modes developed in the process. The benefits from including these personnel include bringing focus to the most likely modes of failure based on engineering judgment and increasing the general awareness of dam safety issues by sharing knowledge at all levels. Experience has shown that it is very helpful and valuable to include senior (experienced) field personnel in the actual PFMA session because all information has not been written down and in certain cases assumptions in written reports differ from what is done or known in practice. It is important that the operations and maintenance staff be encouraged to participate fully and openly in all discussions without any fear of reprisal by their management for indicating things may not be done in the correct manner or in perfect

conformance with what is considered official documentation. The field personnel also can verify data and information discussed in the session.

Supplemental Resources – In addition to the team participants there are other people who have specific technical knowledge or experience that may be useful to the team. These people would be notified and asked to be available or on call on the day of the PFMA session. This could include persons involved with the construction of the facility, seismotectonic specialists, hydrologists, structural engineers, electrical engineers, mechanical engineers, geotechnical engineers, field personnel, inspectors, instrumentation personnel, emergency preparedness personnel, etc. If there has been a major change to the project (anchoring program) or if there is a complex instrumentation program (unique instrument), it is useful to have the responsible engineer/operator make a short presentation during the workshop so that all participants have a common understanding of the issue. Also, if not already a designated Core Team member, an engineering geologist with dam experience should participate in the PFMA and should review all geological background material, make appropriate observations during the field review, and participate in discussions of foundation related potential failure modes.

17-4.3.3 General Selection Criteria

The following criteria should be considered when selecting PFMA participants:

- The core team members should have knowledge and experience related to dam safety evaluations. It is especially helpful to have persons who have experience and knowledge related to dam failures and who have an inquisitive/investigative mindset.
- Persons who had experience with the original design and/or construction of the project can provide invaluable insights and data. Wherever possible, they should be recruited for the PFMA field and data review and the PFMA session. Alternatively, they can be available by phone to answer questions raised during the session.
- State dam safety personnel, including the dam safety inspector responsible for the subject project, can provide valuable data, information and insights into the project and should be invited to participate.

The qualifications of the PFMA facilitator include:

- Be a licensed professional engineer or licensed engineering geologist with a minimum of ten years of experience in the evaluation, design, construction, monitoring, and operation of dams.
- Have experience in the type of project they are facilitating (e.g., embankment dam, concrete dam, or hydraulic structure, etc.). To a certain extent, the lack of expertise in one type of dam or another can be partially mitigated by having one or

more co-facilitators that are experts in that field in order to assist in the technical aspects of the project. It is not necessary for them to be an expert for the structures, but they must have a general understanding of how they operate and what case histories have taught the dam safety community with regards to design and operational weaknesses.

- Have an excellent understanding of dam incidents and failures and be able to draw on that knowledge during the PFMA process.
- Have training and experience participating in a PFMA similar to that described in this guidance. This includes:
    - Attended a FERC-sponsored PFMA training workshop (or equivalent PFMA training). FERC will periodically provide training opportunities to help develop PFMA facilitators.
    - Have assimilated the information and written the report for at least one PFMA.
- Possess good communication and group leadership skills.

It is also recommended that the facilitator have previous PFMA experience as a co-facilitator serving under the supervision and training of an experienced facilitator. They must fully understand the objective and requirements of the PFMA and what constitutes a fully developed and acceptable potential failure mode. This ensures that the person leading the PFMA process knows not only how the process is carried out, but also is aware of what can be accomplished. This is especially critical if the Core Team members have not been through a PFMA.

Below are some additional knowledge, skills, and abilities a facilitator should possess:

- *Independent/Objective*. It is of utmost importance that the facilitator remains completely independent during the development of a potential failure mode. Their role is not to act as a decision-maker, nor to influence anyone's decision regarding the development of a potential failure mode; it is to guide the team towards the different options available in the development of a potential failure mode and the facts surrounding the different steps of a potential failure mode. The facilitator should not make any comments or innuendos along the lines of how unbelievable or ridiculous a potential failure mode is, or how "that would never happen" as discussions are taking place. It is totally appropriate for them to ask the typical, how, what, why, and when types of questions to get the team to think things through, though they should remain cognizant of their tone and strive to remain neutral. They should help guide the team in a discussion that keeps them focused along the correct paths without directing or biasing them which path to take.

- *Interrogator*. In conjunction with being independent, a good facilitator is able to lead the group discussion by asking questions that will help lead them down the most suitable path of a fully developed potential failure mode. It is important that the facilitator remain independent when asking these questions. At each decision point in the process, a short discussion is often necessary to determine the different possibilities for the progression of the potential failure mode. They can ask the group questions about which path is the most likely to progress and suggest the different options. Therefore, it is critical for the facilitator to have a good understanding of all the mechanisms that can present dam safety issues related to the type of structure being evaluated. For example, an understanding of mechanisms related to seepage and internal erosion, slope stability, overtopping erosion, and liquefaction are important when evaluating an embankment dam. If the project involves a concrete dam or concrete features, the facilitator must also understand sliding, overturning, structural strength, and general performance of concrete structures.
- *Motivational Speaker*. This may seem like an odd characteristic for a facilitator; however, team members may be present that are shy, reserved, or quiet during the discussions. This may be a result of their personality or their belief that they have nothing to offer to the process. These individuals may feel a bit intimidated by others in the room and may not have the confidence to speak up. Those experienced in the PFMA process realize that these individuals often contribute some of the most critical and insightful information during the PFMA workshop. Regardless of their official role or position, it is important for the facilitator to motivate all individuals to participate and play an active role in the discussion. This can often be done by asking direct questions about the project or procedures and emphasizing the importance of what they contribute to the overall understanding and safety of the project.
- *Referee*. It is sometimes necessary for a facilitator to act as a referee during a discussion in order to successfully resolve differing opinions and uncertainties about certain aspects of the project. These differing opinions can result from a lack of understanding of the project or issue being presented and, in some cases, could be someone attempting to manipulate or adversely influence the process. Depending upon the circumstances, it is possible that a team member is a major decision maker that does not want to spend money and will make every effort to convince the team that the potential failure mode is not credible and a problem does not exist when it clearly does exist, or there is sufficient uncertainty to require additional investigation or research before making a final determination. It is critical for the facilitator to keep everyone on the same path of fact finding and sticking to the knowns. If unknowns are discovered during the discussion, additional studies or analyses may be in order to clearly identify whether the proposed potential failure mode is credible.

Some limitations of PFMA facilitators:

- Ideally, the facilitator will have limited prior project experience with respect to examining the dam's operation and history. This is considered an advantageous situation, but not a requirement, with respect to providing a fresh and vigorous look at the structure.
- A person is not eligible to serve as a facilitator for a design or construction PFMA for which they are the engineer-of-record for, or contributed substantially to, a significant analysis, design, or construction effort. However, the facilitator may be from the same organization provided they did not have a significant role in the analysis, design, or construction effort and can demonstrate their independence to serve as a facilitator.
- Licensees and their staff are not eligible to facilitate a PFMA on their own structures.
- Individuals serving as a contracted Chief Dam Safety Engineer (CDSE) or other members from their organization may not serve as a facilitator for projects in which they provide such services.
- Individuals serving as a contracted Chief Dam Safety Coordinator (CDSC) or other members from their organization may not serve as a facilitator for projects in which they provide such services.

Licensees must submit the name of the proposed PFMA facilitator and any proposed co-facilitator(s) along with a resume of each individual to the appropriate FERC Regional Engineer for review and approval at least 90 days prior to the start of the PFMA. Each resume must include documentation clearly demonstrating the facilitator(s) qualifications and completion of the required training as provided above. Documentation for proposed PFMA facilitators for Part 12D Reports should be submitted in accordance with the provisions of Chapter 16 of the FERC Engineering Guidelines. FERC-required PFMA sessions should not be conducted until the PFMA facilitator(s) has been approved. Submittal of the names and qualifications of PFMA core team members is not required.

17-4.4 Collection of Background Information

The team leader, working in conjunction with the facilitator, FERC dam safety professional, and other project staff, collects and gathers for review, all background information on the project. The data and information can be collected in a centralized location for reading by the core team members and would also need to be available during the PFMA session. Alternately, the information is stored electronically, and the information made available to all participants. The general rule is: **collect all information on the project**. If there is a question about the need to collect certain material, the facilitator and owner should discuss this in advance.

If the Supporting Technical Information Document (STID) has been properly assembled and maintained in accordance with Chapter 15 of the FERC Engineering Guidelines, this step will require far less effort than collecting the data from separate files on an ad hoc basis.

The types of material which should be collected (if available) include but are not limited to the items listed below:

- Any FERC or state agency construction inspection reports (these have been found to be extremely useful, particularly if the original construction predates the Federal Power Act).
- Current or most recent dam safety engineering analyses, including stability and stress analyses.
- The most recent monitoring and instrumentation data along with the historical records of monitoring data. Large scale, easily readable, plots of monitoring data over the life of the dam have proven extremely valuable and should be available at the PFMA session. (The licensee or consultant should also provide verification that the instrumentation is properly functioning.)
- The most recent surveys for each of the project structures (i.e. horizontal and vertical survey data). A detailed survey of the crest of all structures including dam crest surface elevations and service and emergency spillway crest elevations to confirm the freeboard assumed in the discussions. The elevations of the ground surface that could result in overflow around the structures should also be considered. Also, the project datum should be stated (i.e., conversion of project records to NGVD).
- Current hydrologic studies and the associated flood routings, dam breach, inundation studies, and consequence analyses.
- The current Emergency Action Plan and any Sudden Failure Assessment as described in Chapter 6 of the FERC Engineering Guidelines.
- The most up-to-date aerial photographs of the dam, other project structures (spillway(s), dike(s), etc.), reservoir, and downstream areas that could potentially be impacted by failure of the project structures.
- Original and subsequent modification design and construction reports, other supporting design or construction reports (foundation reports, exploration reports, etc.), as-built drawings, and photographs.
- Boring logs, field testing results, and laboratory testing results.
- Any underwater inspection reports and preferably the underwater inspection that was conducted as part of the most recent Part 12D inspection.

- Recent and historical meteorological (https://www.ncdc.noaa.gov/data-access) and pertinent river records from project or nearby dam or gage records (http://waterdata.usgs.gov/nwis).
- Operation records (particularly historical) of primary and secondary (e.g. fuse plugs) spillways, discharge rating curves, mechanism and response times for gate opening (e.g., stanchion gates, bulkheads, flashboards, gates) and problems (e.g., ice, debris).
- The most recent seismic loading parameters that have been prepared for the site and print records of recent seismic activity (http://earthquake.usgs.gov/); and
- Any dam safety incident reports.

(**Note**: *Basic seismic, meteorological and/or stream flow data, and consequence information should be reviewed to ensure that previous findings or assumptions related to potential failure mode hazards or consequences are up to date. Hence, recent data and information should be brought to the session or generated at the session as necessary. This will ensure that the PFMA report is an accurate representation of the likely potential failure modes and consequences based on the best information that was available on the date the PFMA was conducted*.)

A listing of the data available for review and considered in the PFMA should be prepared for use by the core team in reviewing the materials and included in the PFMA report documentation. Team members are to review all of the above information searching for site specific conditions or situations that would lead to failure, as defined above.

If not already available, the owner should establish a means to retain and archive all the information collected for the PFMA. Again, already having a comprehensive STID that fulfills the requirements of Chapter 15 of the FERC Engineering Guidelines should reduce the effort associated with this task.

An advance review package on the dam should be prepared for all participants – this package should consist of material already prepared that provides an overview of the dam and its performance. The purpose of an advance package is twofold: to give the facilitator familiarity with the dam prior to the site review and to refresh knowledge of the dam and stimulate "potential failure mode thinking" by all participants prior to the PFMA session. The previous Part 12D Report, the most recent FERC dam safety inspection report, and the STID provide a good "advance package document" to give to the facilitator and the core team (and any other proposed participants) for familiarization with the project prior to the site review. The advance review package should be sent to site review participants prior to their travel to the site.

17-4.5 Comprehensive Review of Background Material

The project information should be reviewed prior to performing the site visit and review. The review of the project information can be performed prior to the team gathering at the site, provided the project information is delivered to the project team members in advance or the information review can be performed at the site or other project location. There are advantages for the team members having the project information in advance of the site visit so team members can become familiar with the project documents and information. Likewise, there are advantages to having a dedicated time set aside in a group setting for efficiency in sharing the collected data and to provide a "captive" condition to ensure that the material is reviewed by all the core team members. Being together also allows for collaboration on items that may need clarification by the entire group. This review of the material should take place at a convenient location considering the location of the site, data, and where the PFMA session will take place. The background material should preferably be in the same as room as the PFMA session in order to facilitate finding reference material during the PFMA session.

17-4.6 Site Review of the Dam and Project

Typically, the PFMA team is first assembled at the time of the site review. This is a good occasion for the facilitator to review the basic concept of the PFMA process and the objectives of the site review and ask if there are any questions. These guidelines lay out what is to be accomplished in the PFMA and although the core team has likely read them, the licensee's operating staff probably is less familiar with the process. Therefore, it is helpful to have a quick review of the process to make sure everyone is on board. Likewise, if the core team gathers to do the review of the project information, it is appropriate for the facilitator to have a quick discussion of the plan and objectives of the review.

Prior to the PFMA session, a project site visit should be performed. At a minimum, the owner's personnel and core team should participate in the site visit; however, other PFMA participants could also attend. During the site visit the participants should be "thinking" about potential failure modes and looking for evidence of potential changes from the observations and results from prior inspections. The basic purposes of this site review are:

1. to let those participating on the PFMA team, who have not seen the site, see it;
2. to have the team "think/see" PFMs in the field; and
3. to discuss the site and operations with site personnel in their own environment. Owners may find it valuable to include all or most of the employees that they plan to have participate in the PFMA also participate in the site review.

17-4.7 Conduct the Potential Failure Mode Analysis Session

17-4.7.1 General

A description of the PFMA session is given below. It is important for the facilitator to involve all participants in the discussions and give everyone an opportunity to provide their knowledge, understanding and views on the PFMs, consequences and possible risk reduction actions / measures.

Just as discussed for the site review, at the outset of the PFMA session, the facilitator should give some introductory remarks about the PFMA session goals, objectives, and process, and should discuss with the entire team that the product of the exercise is not a decision document but rather an informational resource document, developed from the combined input of the team, that is intended for use and reference for many years.

17-4.7.2 Group Dynamics

PFMA sessions are typically multi-day meetings attended by a variety of individuals and professionals with varying perspectives and understanding of the project. Such meetings can be subject to a number of factors that can compromise the judgment and decision-making of the PFMA team, due largely to subconscious cognitive processes and group dynamics, which can result in team members aligning their views too readily in order to preserve group harmony rather than engaging in sufficiently thorough critical, and constructive discussion and debate.

Bias and heuristics are important concepts to be aware of in conducting a PFMA. Bias is a tendency, trend, inclination, feeling, or opinion, especially one that is preconceived or unreasoned. They can be systematic errors that one makes in specified circumstances. A heuristic is a simple procedure that helps find adequate, though often imperfect, answers to difficult questions – a kind of a mental and often unconscious shortcut. Both bias and heuristics can have a dramatic and negative influence in the identification and evaluation of potential failure modes. These must be recognized, and to the extent possible, the facilitator must strive to minimize their impacts. Vick (2002) describes many of these in detail. Some common bias and heuristics are included in Appendix 17-B (adapted from Kahneman, 2011).

Sometimes during the PFMA session the team may encounter one or more of the situations listed below. The PFMA facilitator must recognize these signs and redirect the group toward a more positive direction.

- A dominant individual may drive the team into their way of thinking by overwhelming them with filibustering or other techniques that eventually drive the entire team into thinking the way they do. It takes a fairly strong facilitator to deal with this, and usually requires emphasizing and bringing out the opposing point of view as well as drawing others into the conversation.

- People may not say what they actually believe or think for fear of appearing unknowledgeable and will tend to go along with the rest of the group even though they have important input. This requires the facilitator to draw out their opinions by directing questions specifically at these individuals that are best suited to address the particular topic being discussed.
- A contrary individual may have valuable information even though their approach to communication may be difficult or challenging to the rest of the group. This information and these opinions should not be quickly dismissed without due consideration.
- The group gets tired due to the duration and rigors of the meeting and people agree just to get it done. The facilitator is not immune to this trap. If it is obvious that proper attention is not being paid to something, it is important to stop, take a break, and discuss ways to invest proper time for the evaluation. This may even require postponing the completion of the PFMA for a few days, like over a weekend.

Improving the quality of subjective judgment and decisions towards rationality can be accomplished through training in the cognitive nature of subjective thinking. Such training, particularly for facilitators, can help to guide the PFMA team in directions that ensures rational subjective judgment and rational subjective decision-making during the process of identifying and evaluating potential failure modes.

17-4.7.3 Project Summary and Overview

As discussed earlier, it is critical to provide all the documentation to all team members prior to the workshop. It is important for the owner's representative to prepare a presentation for the team that summarizes all of the important information of the project. This presentation should be one of the first items on the PFMA agenda. It should be appropriate for the complexity of the project and consider including the following items:

- Summary of project features and key project information,
- Overview of regional and site geology (including summary of site investigations),
- Summary of original design,
- Summary of construction with an emphasis on construction issues or other elements of construction that could influence the performance of the project,
- Summary of significant modifications to the project since it was completed,
- Summary of operational performance,
- Summary and interpretation of instrumentation data and understanding of dam performance under all postulated loading conditions,
- Findings of significant engineering analyses,

- Summary of design flood and seismic studies,
- Summary of the standard operation of the project, and
- Summary of potential life loss and other consequence estimates.

The length and depth of information should be scalable to the size of the project and the dam safety concerns associated with it. For large, complex projects this presentation may take several hours.

At the conclusion of the presentation, the team should discuss the adequacy of the project documentation provided for the PFMA and determine if any deficiencies exist for specific project features or components in being able to identify and evaluate potential failure modes.

17-4.7.4 Project Components and System Understanding

Dams are engineered systems and significant thought must be put into the details surrounding the interactions between the various components and features of a particular facility. Prior to identifying project potential failure modes, a complete understanding of the physical project features, components, and elements and the interactions, relationships, and dependencies of those physical elements in a systems context must be undertaken and developed. More information on this approach is included in Appendix 17-C. This understanding must include the identification of potential backup systems and redundancies as well as operational protocols, standing operating procedures, lines of communication, feedback, and authorities and responsibilities of project personnel. Organizational culture of the dam owner and operator and the human factors and influences on operations and decision-making must also be understood and incorporated into the project and system understanding.

Only after this assessment and understanding has been completed can the project team begin the process of comprehensively identifying, describing, and evaluating potential failure modes for the project.

17-4.7.5 Identification of Potential Failure Modes

An adequate job of identifying potential failure modes can be performed only after all relevant background information for a dam is diligently collected and thoroughly reviewed. This includes information related to geology, design, analysis, construction, flood and seismic loading, operations, and performance monitoring. Photographs, particularly those taken during construction or unusual events, are often vital to identifying vulnerabilities.

It is important to include, but also think beyond, traditional analyses when identifying potential failure modes. Some of the greatest risks for uncontrolled reservoir release and operational issues may be due to operational problems or potential failure modes that do

not lend themselves to standard engineering calculations. Therefore, it is also important to have operational staff involved with the process.

After reviewing the background project information, and gaining an understanding of how the project works, the first step in identifying potential failure modes is to have a brainstorming session where the team attempts to determine every possible way that the dam could fail, as defined in Section 17-2.1. This also includes potential failure modes associated with operational failures of the mechanical and electrical portions of the project that do not result in an uncontrolled release of water or failure of the dam, but result in significant consequences or safety concerns. This could include items such as failure of a turbine, pump, gate, or similar items that prevent them from discharging water that results in significant consequences or creates operational limitations that could potentially impact the safety of the facility. This should be done for each loading condition (normal, flood, seismic, and other (ice, reservoir sedimentation, volcanic eruption, etc.).

Brainstorming is intended to be a group creativity technique in which participants can think freely and spontaneously suggest ideas in a non-judgmental environment. **Evaluation or criticism of ideas generated should be put on hold until after all ideas have been identified**. By suspending judgment, it is hoped that participants will be more open and less encumbered to generate new ideas, including perhaps more unusual ideas.

In order not to be biased or constrained by previously identified potential failure modes, **the brainstorming session should NOT use lists of previously identified** potential failure mode**s**. Although this information will be considered after the brainstorming session is complete, this approach forces the team to be creative and to think critically about the different ways failure may occur. Only after the brainstorming session is complete should lists of previously identified potential failure modes be reviewed to see if potential failure modes may have been missed in the brainstorming session and to see where there is duplication of potential failure modes between efforts.

The brainstorming session must be structured and methodical to minimize the possible oversight of a potential failure mode. Consider the possibilities for failure by loading condition (static reservoir, hydrologic, seismic, ice, debris impact, and any other loading relevant to the site) for each component of the project (main dam, spillway, gates, dikes, outlet works, power plant, etc.). Typically, it is recommended to start with the static loading condition since it is generally considered to be the simplest loading condition for most to understand, it defines the loading most are familiar with seeing on a day-to-day basis, and the frequency of loading condition is more straight-forward.

For example, one place to start with an embankment dam could be to brainstorm all possible static potential failure modes associated with internal erosion (piping) through the embankment. Once the team has completed that focused part of the project, they could proceed to the next focused part of the project, such as internal erosion through the

foundation of the embankment. This focused approach would be completed on each aspect of the project and under the different loading conditions. This helps prevent missing an important component, failure mechanism, or pathway of the project.

The facilitator elicits 'candidate' potential failure modes from the team members, based on their understanding of the vulnerabilities of the dam and project from the data review and field conditions.

Consider the broader definition of failure and don't limit the identification of potential failure modes to just an uncontrolled release of the reservoir or a dam breach. Also consider total system operation aspects (communication and response [i.e., personnel, remote telemetry], system functionality and interrelationships, facility access, weather conditions, equipment) with respect to the possibility of their contribution to development of a potential failure mode/failure scenario.

As each 'candidate' potential failure mode is identified, a short description of the failure mode is recorded on a flip chart, white board, computer, or by some other method to distinguish it from other similar potential failure modes. Sometimes this preliminary or developmental discussion of the initial 'candidate' potential failure mode suggestion may lead to two or more separate or related potential failure modes that are then identified separately. At this stage the description of the potential failure mode is typically limited in detail so that the group can understand the location, general pathway, and failure mechanism of the potential failure mode so as to distinguish it from other similar potential failure modes. Typically, the detailed description of the potential failure mode and overall failure sequence is discussed after the brainstorming session is completed.

Once brainstorming is complete, the team should consider other potential failure modes from other prior reports, available potential failure mode lists, or templates that were not identified in the brainstorming.

If past PFMA reports (or higher level risk studies such as a Level 3 or Level 4 risk analyses, as defined by Chapter 2 of the FERC Risk-Informed Decision Making Risk Guidelines) have done an adequate job of identifying and describing the potential failure modes and no new factors are apparent that would change the past write-ups, little to no revision may be needed in identifying and developing potential failure modes, except for any brainstormed potential failure modes that were not previously identified. However, a careful review of all potential failure modes and their descriptions are needed to ascertain that the past findings are in fact still applicable.

In reviewing potential failure mode descriptions from past PFMAs and other engineering studies, it is important to ask the following questions:

1. Are the potential failure modes sufficiently detailed?
2. Is the case for each potential failure modes adequately made?

3. Has new information become available either through investigation, performance, operation, methodology changes, etc., that would revise or update the potential failure modes?

The following suggestions are provided to help more easily identify missing or incomplete potential failure modes:

- Separate identified potential failure modes by individual structure (e.g., main dam, auxiliary dike, spillway, outlet works, powerhouse, etc.) and loading condition (static, seismic, and hydrologic). Recognize that different loading conditions may activate the same failure mechanism and failure pathway. For example, if an internal erosion (piping), stability, or landslide potential failure mode exists as a potential failure mode under normal or static loading, it may be activated by unusual loading such as flooding or earthquake shaking. Thus, it may be a potential failure mode under all three loading conditions.
- Within the above categories, group similar-type potential failure modes together (e.g., internal erosion potential failure modes, overtopping potential failure modes, gate potential failure modes, etc.). There may be different potential failure mode pathways that need to be considered depending on the site conditions. For example, internal erosion through the embankment, internal erosion from the embankment into the foundation, internal erosion through the foundation; or overtopping of the main embankment leading to erosion of the embankment, overtopping (outflanking) of the embankment leading to erosion of the abutment materials; etc.

Depending upon the size of the project, the brainstorming session could take a few hours to more than a day. It could also result in tens or more than a hundred brainstormed potential failure modes, also dependent upon the size and complexity of the facility. A list of commonly considered mechanisms and pathways to consider when identifying potential failure modes is included in Appendix 17-D and could be used to identify missing potential failure modes after the brainstorming session. **Do not use the list as a reference to guide the brainstorming session.**

Potential failure modes should be identified independent of previously assigned potential failure mode categories (Category I through IV) as defined in previous versions of Chapter 14 of the FERC Engineering Guidelines. Other items and topics included as part of 'Other Considerations' or 'considered but not developed' in previous PFMA documents should also be carefully evaluated to consider their possible merits as candidate potential failure modes. Section 17-4.7.8 of this Guideline discusses a procedure for evaluating potential failure modes, including a discussion of standardized terminology that replaces the previous potential failure mode categories.

Potential failure modes related to physical and cyber security and acts of terrorism are not considered. However, the PFMA process may be applicable in assisting a licensee in evaluating the vulnerability and risk associated with acts of terrorism.

Additional considerations in the identification of potential failure modes are included in Appendix 17-E.

The process of identifying potential failure modes results in a list of candidate potential failure modes by project component and loading condition. An example summary table is shown in Table 1. From this list each potential failure mode is described and discussed in more detail and screened as described in the following sections.

17-4.7.6 Description of Potential Failure Modes

For the team to have an adequate understanding of the potential failure modes, each potential failure mode must be described in detail. A potential failure mode is a detailed description of a sequence of events, commencing with an initiating condition, progressing in a step-by-step manner, until a negative event occurs. It cannot be emphasized enough, **it is important to develop the potential failure mode description fully, from initiation through step-by-step progression to breach and uncontrolled release or to an adverse consequence**. There are three parts to the description:

- **The initiator**. This is the loading or physical condition that leads to initiation of the PFM. For example, this could include reservoir increases due to flooding (perhaps exacerbated by a debris-plugged spillway), strong earthquake ground shaking, malfunction of a gate or equipment, deterioration of project features, an increase in uplift, or a decrease in strength.
- **Failure progression**. This includes the step-by-step development of conditions that lead to the breach and uncontrolled release of the reservoir or an unsatisfactory performance or outcome. The location where the failure is most likely to occur should also be highlighted. For example, this might include the path through which soils will be transported in an internal erosion situation, the location of overtopping in a flood, or anticipated failure surfaces in a sliding situation.
- **The resulting impacts**. The method and expected magnitude of the 'failure' (breach or uncontrolled release of the reservoir or other adverse consequence) is also part of the description. This would include how rapid and how large the expected breach would be, and the breach mechanism. For example, the ultimate breach from an internal erosion failure mechanism adjacent to an outlet conduit might result from progressive sloughing and unraveling of the downstream slope as a result of flows undercutting and eroding the toe of the dam, until the reservoir is breached, at which point rapid erosion of the embankment remnant ensues, cutting a breach to the base of the conduit.

During the development of a potential failure mode description, it should be kept in mind that it is assumed there is a 100-percent chance of each step occurring as you move to the next step in the progression of events. **Only upon completion of the detailed description of the potential failure mode is there a discussion regarding the likelihood of the potential failure mode developing**. There is a tendency by many to decide of how likely the potential failure mode is to occur when developing the step-by-step progress. This mindset must be avoided in order to adequately develop a potential failure mode. However, there are always exceptions which prevent the entire process from becoming a prescriptive process and make it more of a rational thinking process.

As the team develops the step-by-step progression of a potential failure mode, there are often points in the progression where there are numerous paths that could be taken to complete the development of the potential failure mode. For example, seepage through an embankment can take many different paths, but a single path must be selected in order to fully develop the potential failure mode. In cases like this, discussion is typically required for the team to decide which path is the most likely to occur. It is sometimes easy to determine which direction is the most likely, but there are instances where a significant amount of discussion is required to make a decision. It is important to document each option at each fork in the pathway, as it represents a separate potential failure mode. Some facilitators will have the note taker create a separate list that captures the different paths the potential failure mode could take in order to allow for discussion later. This list is sometimes referred to as a "parking lot" to keep the ideas until later in the workshop to ensure nothing important was missed.

A common misconception is there is no need to separate all of the potential failure modes out individually and many of them can be "lumped" together. Some people claim that it has been easier to "lump" multiple failure mode pathways or multiple loading considerations into a single potential failure mode rather than developing multiple individual potential failure modes. Unfortunately, this thinking has the potential to miss a critical element or elements in identifying potential vulnerabilities. The most important reason to individually identify and evaluate each potential failure mode is that when the team is trying to mentally track several different thoughts or branches of a potential failure mode at one time, it is typical that some get confused about the exact path being discussed and discuss incorrect information about an element of the potential failure mode. In some cases, this may not be significant, but it is not always possible to know what could be missing without having that unique discussion for each potential failure mode. It is typical that once the discussion is held, many of the potential failure modes are very similar making it easy to document individually. It is also possible that once the discussion is held and it is found that different branches of a potential failure mode result in identical consequences, it may be acceptable to lump some of them together. Creating sketches and drawings of each potential failure mode pathway greatly assists in keeping this clear to all team members.

Visual aids are also very useful during the development of the potential failure mode. This can consist of items as simple as a plan view of the project posted on the wall, photos of the project in the area of concern, or a sketch on a white board or flip chart. This is particularly useful when drawn by the individual who initially suggests the potential failure mode being discussed. For example, it is often very beneficial to have visual aids to draw the actual path of internal erosion potential failure modes to assist the team in an understanding of the actual requirements for the potential failure mode to fully develop. This concept is also applicable to most potential failure modes when attempting to determine which failure mechanism is being discussed. It is highly recommended that these sketches be included in the final PFMA report.

Other considerations include:

- The location(s) where potential failure modes are most likely to develop are included in the description. "Foundation liquefaction" is not an adequate failure mode description. A better description would read something like, "liquefaction of a continuous saturated loose sand layer in the dam foundation identified in borings between stations 2+50 and 5+50 that leads to a flow slide of the downstream slope, loss of freeboard, and overtopping erosion failure of the dam."
- Any time the discharge capacity of a spillway or outlet gate exceeds the safe downstream channel capacity or could impact recreationists, potential failure modes associated with collapse or misoperation of the gates should be considered.
- If a landslide appears to pose a threat to the safety of the dam, whether from an embankment integrity concern or a reservoir seiche wave, it should be listed as a potential failure mode. If a slide poses an operational hazard or could injure workers or recreationists, it is not a dam safety failure mode, but should be discussed.

The influence of human and organizational factors, where appropriate, should also be considered and included in the description of potential failure modes.

Some example considerations in describing potential failure modes are included in Appendix 17-F.

As potential failure modes are described and developed, they should be:

- Well-described, for the reasons discussed above;
- Comprehensive, in that all the ways that failure of the structure could occur are identified (there are no missing potential failure modes); and
- Separate, distinct potential failure modes are identified for each individual potential failure mode pathway. In general, separate potential failure modes should be identified when any one of the following conditions are met:

- Failure mode location/pathway is different,
- Loading condition/initiating event is different,
- Likelihood of failure is substantially different,
- Monitoring for PFM is substantially different,
- Breach location and geometry is substantially different,
- Consequences are substantially different, or
- Risk reduction actions are substantially different.

At the conclusion of this step in the PFMA process, each potential failure mode should have a complete description of the proposed failure process from initiation to failure and should have a plan view and cross section depicting the failure mode pathway.

The nature of the breach (or other failure condition) is defined and the potential adverse consequences of failure are discussed. The potential failure mode should be developed so that each step in the failure mechanism from the loading condition to the final failure condition is sufficiently defined so that the Dam Safety Surveillance and Monitoring Plan can be developed to detect a developing failure as soon in the process as possible.

To aid in describing each potential failure mode (as well as subsequent steps in the PFMA process), a potential failure mode template is provided in Appendix 17-G. This template, or one very similar to it, should be completed for each identified potential failure mode. Following this template will ensure a consistent framework for documenting each potential failure mode and that all applicable information for each potential failure mode will be captured.

17-4.7.7 Adverse and Favorable Evaluation Factors

All the data, information, factors and conditions that suggest the ways that the potential failure mode is more likely or less likely to occur (adverse factors and favorable factors) are noted.

The following discussion in this section is excerpted from Best Practices in Dam and Levee Risk Analysis (BOR/USACE, 2019). After the team has completely described a potential failure mode, it is then evaluated by listing the adverse factors that make the failure mode "more likely" and the favorable factors that make the failure mode "less likely". These are based on the team's understanding of the facility and background material. The facilitator captures these in bullet form on a flip chart or the note taker/recorded captures these in a computer file or template (see Appendix 17-G). However, these must also be fleshed out in the documentation so that someone picking up the report in the future will understand what the team was thinking. It is the facilitator's job to review the report and ensure that this happens.

As an example, consider an internal erosion potential failure mode. A list of adverse and favorable factors might look like the following. Regular text shows how they might be captured during the PFMA workshop, while text in italics indicates how they would be fleshed out in the report.

Adverse or "More Likely" Factors:

- The gravel transition zones do not meet *modern "no erosion"* filter criteria *relative to the core base soil*.
- The gravel transition zone may be internally unstable, *leading to erosion of the finer fraction through the coarser fraction and even worse filter compatibility with the core*.
- The reservoir has never filled to the top of joint use; *it has only been within 9 feet of this level; most dam failures occur at reservoir levels reached for the first time, which may occur here for a 50 to 100-year snowpack*.
- The core can sustain a roof or pipe*; the material was well compacted (to 100 percent of laboratory maximum) and contains some plasticity (average PI~11).*
- There is a seepage gradient *from the core* into *the downstream* gravel transition zone, *as evidenced by the hydraulic piezometers installed during original construction (and since abandoned).*

Favorable or "Less Likely" Factors:

- Very little seepage is seen downstream, *the weir at the downstream toe, which captures most of the seepage through the dam, records about 10 gal/min at high reservoir when there is no preceding precipitation, indicating the core is impermeable; this level of flow is unlikely to initiate erosion*.
- The core material is well compacted *(to 100 percent of laboratory maximum) and has some plasticity (average PI~11), both of which reduce its susceptibility to erosion*.
- There are no known or suspected defects in the core where erosion could initiate; *benches in the excavation profile that could cause cracking are above the joint use elevation*.
- If erosion of the core initiates, the gravel transition zone may plug off before complete breach occurs, *according to the criteria for "some erosion" or "excessive erosion" by Foster and Fell (ASCE J. Geotech. and Geoenv. Engr., Vol. 127, No. 4, May 2001)*.

All of this information is captured by the note taker to facilitate documenting the suggestions. A flip chart or using the potential failure mode template on a computer with

projector to record the potential failure mode information can be used. The use of a computer can assist in recording and organizing the details which makes it possible to efficiently complete the PFMA report. When a computer is used to record the session, a person other than a core team member should take the notes to ensure the core team members can actively participate in the discussions. The note taker should be an experienced dam engineer.

The consequences of failure and the circumstances surrounding a failure (advance warning, detection possibilities, impact of the failure, etc.) should be discussed for each potential failure mode since these factors play a role in assessing the significance of the potential failure mode. Experience has shown that it is necessary, valuable, and instructive to specifically raise the topic of "consequences" as part of the PFMA and brainstorm site-specific factors and potential failure mode consequence-related factors (in the event they have been overlooked during the technical discussion of the potential failure mode).

When each site-specific potential failure mode is identified, the nature of the breach / uncontrolled release of the reservoir or adverse consequence that may occur is discussed and some general qualitative estimate of the range of consequences (low, moderate, high, extremely high) that may result are identified. The emergency action plan response to potential failure scenarios is examined and any concerns with the plan are identified.

17-4.7.8 Screening of Potential Failure Modes

The identification of potential failure modes often results in a long list of candidate potential failure modes. In order to provide value and direction, this list of candidate potential failure modes must be sorted and prioritized, and distinctions made between those potential failure modes that need further effort or study versus those potential failure modes that need less attention versus those potential failure modes that need no further effort. The process of sorting potential failure modes is termed screening. Screening of potential failure modes can (and typically does) occur throughout the development of the potential failure mode process (i.e., identification (after initial brainstorming), description, and discussion of adverse and favorable factors). Screening can occur at any point in the potential failure mode process (after brainstorming has been completed) when sufficient information on the potential failure mode has been identified and discussed to properly justify the screening of the potential failure mode. Each potential failure mode must be screened using the following factors and in the order they are provided:

1. Is the potential failure mode physically possible?
2. Does the potential failure mode lead to failure (uncontrolled release of the reservoir or result in potentially significant adverse consequences due to the inability to function or functioning in an impaired or compromised fashion)?

3. Is the potential failure mode so remote as to not be a dam safety concern? (i.e., no additional efforts are typically warranted – no studies or risk reduction considerations are needed.)
4. Is the potential failure mode in progress or imminent?

Additional screening steps are required for potential failure modes that do not result in uncontrolled release of the reservoir but do lead to adverse consequences. Those steps are described later in this section.

The potential failure mode screening process is shown on Figure 1.

The screening of each candidate potential failure mode should follow this process and will result in the grouping of candidate potential failure modes by disposition.

The first factor or question in the potential failure mode screening process is intended to screen out candidate potential failure modes that are not physically possible to occur. The loading or physical conditions described in the potential failure mode are not physically possible to occur. If the potential failure mode is not physically possible, then the candidate potential failure mode is ruled out and the justification for why it is no longer considered a potential failure mode is documented in the report.

Example justifications for ruled out potential failure modes include:

- Internal erosion (piping) through the auxiliary dike under normal loading. This candidate potential failure mode was identified and ruled out as a potential failure mode because it is not physically possible to occur. The normal reservoir water surface is lower than the upstream toe of the dike. The dike embankment never retains the reservoir under normal loading.
- Liquefaction of the foundation soils under seismic loading. This candidate potential failure mode was identified and ruled out as a potential failure mode after it was discovered from the construction records that all the foundation soil material was excavated to bedrock prior to construction of the embankment. No foundation soils exist below the embankment; therefore, this potential failure mode is not physically possible.

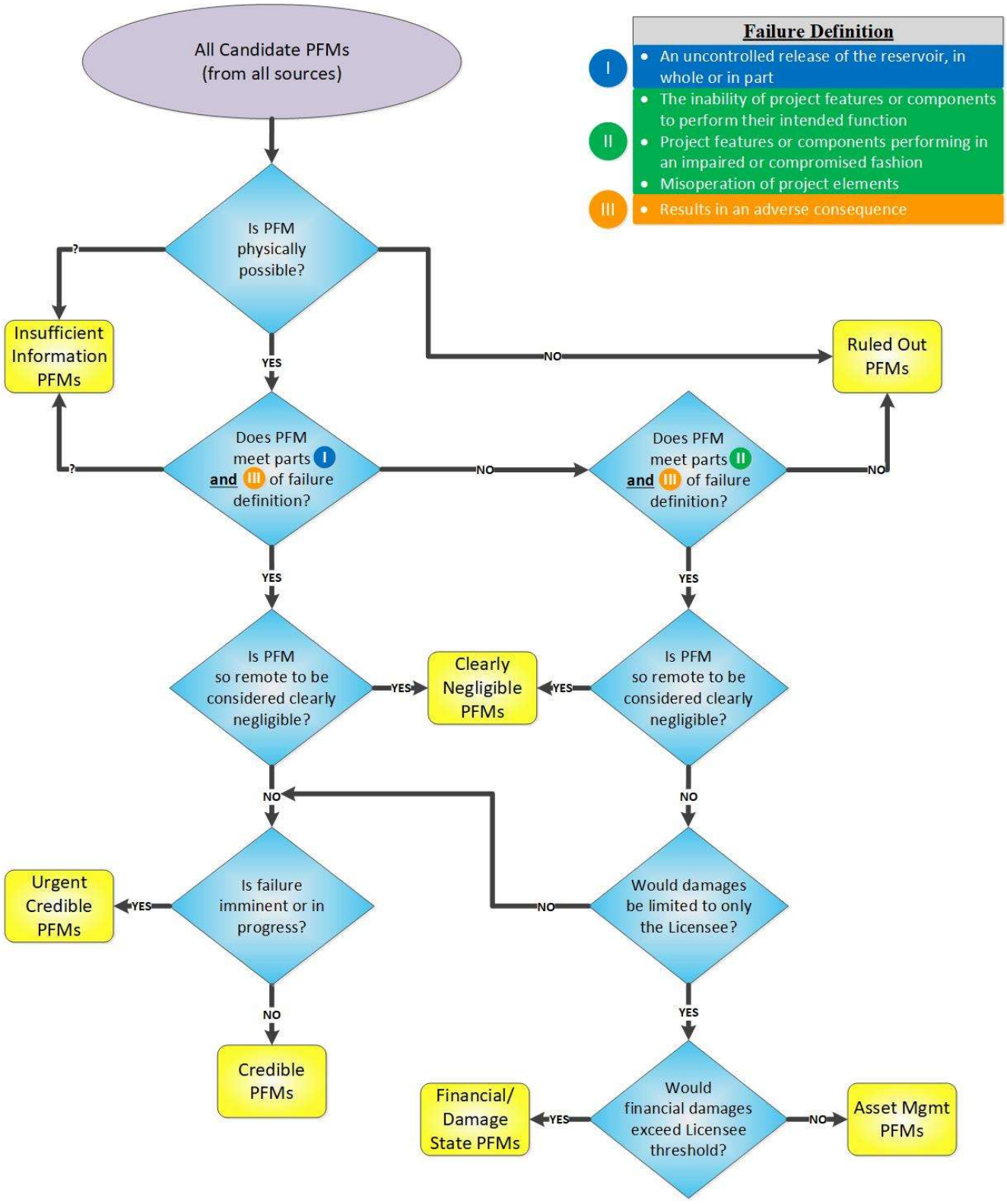


Figure 1: Potential Failure Mode Screening Process

In some cases, it may not be possible to determine if the potential failure mode is physically possible due to insufficient information. In that case additional information gathering, investigations, studies, etc. may be necessary to further evaluate the potential failure mode. Every attempt should be made to place potential failure modes in one of the other potential failure mode screening groupings based on even the limited amount of information that may be available. It is recognized that this can be a difficult task; however, this will assist the dam owner when it comes to evaluating the prioritization of efforts related to the potential failure modes. Screening potential failure modes as 'insufficient information' should be used sparingly and only as a last resort when all other efforts to place the potential failure mode in one of the other potential failure mode screening groupings has been unsuccessful. Information that could be used to reduce the uncertainty (investigations, analyses, monitoring, etc.) should also be identified to assist in scoping of potential dam safety efforts. In addition, increased monitoring may be an appropriate interim risk management activity while information is being collected.

If the answer to the first screening step is yes, then the screening continues to the next step. This second screening step is intended to screen out potential failure modes that do not meet the definition of failure. The definition of failure, as defined in Section 17-1.2 and expounded on in Section 17-2.1, can be thought of in three parts.

> Part I - an uncontrolled release of the reservoir, in whole or in part;
>
> Part II - the inability of project features or components to perform their intended function; or project features or components performing in an impaired or compromised fashion; and
>
> Part III - any of which results in an adverse consequence.

Misoperation of project elements is included of Part II.

The combination of Parts I and III has been the traditional definition of failure. The combination of Parts II and III is the expanded definition of failure to take into account those potential failure modes that may not lead to uncontrolled release of the reservoir, but do impact the safety and operation of the project (e.g., Oroville Flood Control Outlet spillway failure of 2017).

The second screening step has two parts. The first part asks the question, does the potential failure mode meet Parts I and III of the definition of failure? Emphasis is placed on the word "and" in this question because both parts of the question must be answered in the affirmative to pass to the third screening step. This means that the potential failure mode must result in some uncontrolled loss of the reservoir, either in whole or in part AND the result of that loss leads to adverse consequences. Loss of human life is considered an adverse consequence. Other adverse consequences include economic, environmental, cultural, and other non-monetary consequences and their

significance depends on the magnitude of the consequence. Financial consequences (replacement, repair, modification, etc. of a component, structure, or other project feature) to the licensee without directly or indirectly impacting any other entity are also included. (See Chapter 18 of the Engineering Guidelines for additional discussion of these consequences).

Similar to the first step in the screening process, a potential failure mode could be screened as an insufficient information potential failure mode when very limited information is available or there is large uncertainty in evaluating if the potential failure mode would result in an uncontrolled release of the reservoir or if any adverse consequences would results from such a release. In that case additional information gathering, investigations, studies, etc. may be necessary to further evaluate the potential failure mode. Similar to the first step in the screening process, every attempt should be made to place potential failure modes in one of the other potential failure mode screening groupings based on even the limited amount of information that may be available.

If the answer to the first part of this screening step is no, then either the potential failure mode does not result in an uncontrolled release of the reservoir OR such loss does not result in adverse consequences. In this case the potential failure mode passes to the second part of this screening step: does the potential failure mode meet Parts II and III of the definition of failure? Again, emphasis is placed on the word "and" as both parts of the question must be answered in the affirmative to pass to this screening step. The purpose of the second part of this screening step is to screen out potential failure modes that do not meet the overall definition of failure (all three parts of the definition as stated above) or pass the potential failure mode on to additional screening steps.

If the answer to both questions in the second screening step are no, then the candidate potential failure mode does not meet the definition of failure and these candidate potential failure modes are ruled out and the justification for why they are no longer considered potential failure modes is documented in the report.

An example justification for a potential failure mode that has been ruled out due to not meeting the definition of failure includes:

- Failure of the radial gate under seismic loading. This candidate potential failure mode was identified and ruled out as a potential failure mode because it does not lead to an uncontrolled release of the reservoir, no damage to the gate is expected under any seismic loading that would render the gate inoperable, and does not result in significant adverse consequences. The normal reservoir water surface is below the top of the concrete ogee section and water under normal loading is never on the upstream surface of the gate. Failure of the gate under seismic loading is not expected due to the low seismic loads. (Note: This potential failure mode would not be ruled out if the gate was damaged due to seismic loading

considering the possible consequences that could result due to the time to repair the gate and if it would be required for use prior to being repaired.)

If the answer to the second screening step is yes, then the potential failure mode proceeds on to the third step in the screening process.

The third screening factor is intended to separate out those potential failure modes that are considered so remote a failure likelihood to be considered negligible as defined below.

So remote as to be considered clearly negligible:

- The likelihood of the PFM leading to failure is so minute so as not to be considered credible
- In quantitative terms, an annual frequency less than 1:1,000,000
- Confidently would not plot on a Level 2 risk matrix

So, if the answer to question 3 is yes, then the candidate potential failure mode is considered to be clearly negligible and the potential failure mode is excluded from further consideration because even though the potential failure mode may be physically possible, it is clearly so remote that the likelihood of failure is negligible.

The justification for the potential failure mode is documented in the report. In most cases monitoring may not be warranted for these potential failure modes. Just because a potential failure mode is clearly negligible does not mean that it should not be re-evaluated under each subsequent PFMA. Additional methods or information may have come to light since the last review that could indicate a closer look is warranted.

The following is an example justification: "The chance of a major rain storm occurring in the upstream basin at a time when freezing temperatures at the site prevent the spillway gates from opening is considered to be extremely remote, since temperatures in the drainage basin are consistently much lower than those at the dam. Although concerns were expressed regarding this issue in the Eighth Part 12D Report, the team decided that dam overtopping erosion resulting from this condition is so remote as to be considered negligible."

Additional example justifications are provided in Appendix 17-H.

The final screening step for potential failure modes that have followed the screening path that include uncontrolled release of the reservoir is to screen these remaining potential failure modes into urgent and non-urgent potential failure modes by evaluating if the potential failure mode is in progress or imminent. If the potential failure has initiated and is in progress or failure is considered imminent, then urgent or emergency actions may be warranted. These potential failure modes are considered 'urgent' potential failure modes.

Increased monitoring or other interim risk reduction actions may be warranted. If not, then the potential failure mode is considered a credible potential failure mode.

For potential failure modes that have followed the screening path that do not result in uncontrolled release of the reservoir, additional screening steps are required. For these potential failure modes, the next screening factor is distinguishing between consequences that affect only the licensee and those consequences that have impacts to others, including life loss, economic, environmental, cultural, and other non-monetary consequences. Potential failure modes that have these latter consequences are returned to the uncontrolled release of reservoir screening branch and are then screened into urgent and credible potential failure modes as described above. Potential failure modes that have no other consequences other than financial implications to the licensee only are carried to the final screening step described below.

The final screening step for potential failure modes that have followed the screening path that do not result in uncontrolled release of the reservoir but instead result in a financial consequence (replacement, repair, modification, etc. of a component, structure, or other project feature) to the licensee without directly or indirectly impacting any other entity, are screened against a financial threshold determined by the Licensee. The Licensee should determine an appropriate financial threshold above which a financial investment to replace, repair, modify, etc. a failed component, structure, or other project feature would result in extreme adverse budgetary or financial hardship to the Licensee. This financial threshold will likely vary by project and licensee. In any case, a financial threshold greater than $10 million should not be used. Potential failure modes that exceed this financial threshold are considered financial/damage state potential failure modes. Those potential failure modes that are less than the financial threshold are asset management potential failure modes.

17-4.7.9 Disposition of Potential Failure Modes

A summary of the disposition (urgent, credible, clearly negligible, etc.) of all the potential failure modes evaluated during the PFMA should be compiled into a table. The PFMA team should review the disposition of the potential failure modes to verify the proper disposition or revise to a proper disposition. The following are typical ‘next steps’ for each of the standard potential failure mode dispositions:

Urgent: Urgent potential failure modes should be carried forward into the identification of potential dam safety management activities (discussed in the next section) to identify potential immediate risk reduction measures and follow-up activities. Within seven days of identifying an urgent potential failure mode in a PFMA session the licensee must contact the appropriate FERC Regional Office to discuss the development of a plan and schedule to address the urgent potential failure mode.

Credible: If the PFMA is not conducted as part of a risk analysis, then carry the potential failure mode forward to identify and document potential dam safety management activities. If the PFMA is conducted as part of a risk analysis, then the credible potential failure mode is carried into the risk analysis and a risk estimate is developed. After the risk has been estimated (semi-quantitatively or quantitatively), then the potential failure mode is carried forward to identify and document potential dam safety management activities.

Financial/Damage State: These potential failure modes are treated in the same manner as credible potential failure modes.

Asset Management: It is strongly encouraged to carry these potential failure modes forward to identify and document potential dam safety management activities, otherwise, no further action is required for these potential failure modes.

Insufficient Information: These potential failure modes are carried forward to identify and document potential dam safety management activities with a focus on potential follow-up activities that could better define and evaluate the potential failure mode.

Clearly Negligible: For clearly negligible potential failure modes, ensure the written justification of the disposition is proper and appropriately documented. Typically, no further action is required for these potential failure modes (i.e., not carried forward to identify potential dam safety management activities). In some cases, monitoring or inspection actions may be identified and documented as a means to continue to exclude the potential failure mode from further study.

Ruled Out: For ruled out potential failure modes, ensure the written justification of the disposition is proper and appropriately documented. Typically, no further action is required.

17-4.7.10 Potential Dam Safety Management Activities

17-4.7.10.1 General

After potential failure modes have been screened, potential dam safety management activities should be discussed and documented for each urgent, credible, financial/damage state, and insufficient information potential failure modes. These dam safety management activities include:

- Potential Risk Reduction Measures,
- Inspections,
- Surveillance and Monitoring,
- Emergency Action Plan,

- Follow-up Studies, and
- Other.

Each of these are discussed in more detail in the following sections.

17-4.7.10.2 Potential Risk Reduction Measures

Potential risk reduction measures should be considered and documented for each potential failure mode. Potential risk reduction measures are those measures that could be considered and might have merit to reduce risk after additional evaluation, if risk reduction is deemed necessary. These risk reduction measures should consider both temporary (interim) or permanent measures as well as structural and non-structural measures. Examples of interim non-structural measures include:

- Adopt reservoir restrictions or change in reservoir operations;
- Stockpile emergency materials, e.g., rock, sand, sand bags, emergency bulkheads, lighting plants, or other operating equipment, etc;
- Improve and/or increase inspection and monitoring to detect evidence of worsening conditions to provide an earlier warning;
- Identify instrumentation/monitoring "triggers" or threshold pools that would initiate more urgent monitoring or emergency response; and
- Install early warning systems.

Examples of interim and permanent structural measures include:

- Isolate problem area (e.g., cofferdam around problem monolith(s) or other project feature);
- Improve seepage collection system;
- Lower the spillway crest to aid in prevention of failure;
- Increase spillway capacity/construct another spillway;
- Strengthen weak areas (e.g., upstream or downstream blanket to cut off/slow seepage; install tie-backs/anchors; and install additional buttresses);
- Construct stability berm;
- Increase dam height or construct parapet wall;
- Increase outlet discharge capability such as by installing temporary siphon(s); and
- Increase erosion protection where necessary.

17-4.7.10.3 Inspections

The results of the potential failure mode discussions should provide additional information and insights to the routine and special dam safety inspections. In performing dam safety inspections, the inspection should include a focused observation and evaluation that addresses each potential failure mode with an emphasis on the observations/ information that would support or refute early detection of the potential failure mode.

The potential failure mode discussions should also inform such factors as:

- Frequency of inspections
    - Is the annual inspection frequency adequate to capture observations needed to determine if a PFM is active or not?
    - If not, what frequency is needed?

- When inspections should be performed
    - Time of the year (winter when ice loading is greatest?)
    - Event (beginning of irrigation season?)
    - Reservoir elevation stage/duration (when reservoir fills above a certain elevation? Or when the reservoir has been full for more than 3 months?)

- Technical discipline experts accompanying on inspection
    - Structural engineer or gate expert
    - Mechanical, electrical, or controls engineer
    - Geotechnical engineer
    - Engineering geologist
    - Others

- Need for special inspections
    - Confined space of tunnels, adits, manholes, etc.
    - Gate inspection
    - Rope access
    - Underwater
    - Other

As is the case with any dam safety inspection, what you don't see may be as important as what you do see. The absence of, or significant change of, previously observed conditions should be noted just as the presence of a new condition. For example:

- Seepage not present when it has been historically observed for similar reservoir elevations.
- Not being able to observe seepage exit location due to vegetation obscuring the exit location or the exit (based on the potential failure mode description) is located in a submerged part of the tailrace.

17-4.7.10.4 Surveillance and Monitoring

Each potential failure mode shall be reviewed to determine whether current visual surveillance or instrument monitoring contained in the project Dam Safety Surveillance and Monitoring Plan (DSSMP) is adequate to detect the onset of the potential failure mode or the onset of conditions that may contribute to or "allow" development of the potential failure mode. Any relevant comments relating historical and current performance indicators to identified potential failure modes should also be captured. To facilitate development of DSSMPs, the PFMA team should include any comments and discussions on these items as appropriate for each potential failure mode identified:

1. The type and frequency of inspections (visual surveillance requirements) should be evaluated to address the identified potential failure modes. This item may include the recommendation of developing customized checklists for the dam. (The nature and content of the checklist, if recommended, is developed by the owner. The checklist should identify specific visual clues that may indicate a suspected potential failure mode has activated, and the checklist should provide instructions as to what step(s) should be taken once a clue is observed).
2. The current instrumentation and visual surveillance program should be critiqued. It should be determined if the existing instrumentation is operating properly and that the readings can be relied upon. In some cases, instruments may be obsolete and serve no purpose in monitoring for the development of a potential failure mode. In other cases, additional instrumentation or visual surveillance may be needed to monitor for a potential failure mode development.
3. Reporting requirements should be reviewed. Action limits may need to be established for some of the instruments and procedures developed for reporting variations in instrumentation readings. As a minimum, annual engineering review, evaluation and reporting of the instrumentation data is required.
4. In some cases, additional analyses or investigations may be required to fully evaluate the appropriate surveillance and monitoring activities for a particular potential failure mode. The PFMA team should identify what information, analyses, or investigations might be needed to accomplish this effort.

5. If enhancements to the monitoring or visual surveillance are identified by the PFMA process then priorities for improvement in the DSSMP should be discussed, and appropriate recommendations and schedules provided in the Findings and Recommendations section of the report.

The following questions should be considered in providing potential failure mode-specific monitoring factors:

- For each potential failure mode what would be an indicator of this potential failure mode actually occurring?
    - (You want to catch it at the earliest possible opportunity so action can be taken.)
- Where would I look for signs?
- What would I use to help detect it?

The potential failure mode pathway should be evaluated from the initiation location to the breach location to determine possible locations for detection that the potential failure mode is active or to monitor the conditions that might initiate the potential failure mode.

In evaluating existing instrumentation in support of evaluating potential failure modes, the following questions should be considered:

- Does the existing instrumentation and monitoring plan adequately capture this potential failure mode?
    - Right location?
    - Right equipment?
    - Right frequency of reading?
    - Sufficiently reliable (i.e., no history of large gaps in data)?
- If not, what type and location of instrumentation is needed to detect this potential failure mode?

Keep in mind the following:

- Existing instruments might not be in the location to monitor/detect the potential failure mode.
- Existing instruments might not be installed at the correct depth to monitor/detect the potential failure mode.
- There might not be enough or correct spacing of instruments to monitor/detect the potential failure mode.

- Existing instruments might not be currently measured at proper time or frequency to monitor/detect the potential failure mode.
- A malfunctioning instrument may not be able to monitor/detect the potential failure mode.

Surveillance and monitoring opportunities should also be considered for clearly negligible, urgent, and insufficient information potential failure modes where surveillance and monitoring activities are determined to be of benefit.

Additional surveillance and monitoring information can be found in Chapter 9 of the FERC Engineering Guidelines.

17-4.7.10.5 Emergency Action Plan

Each potential failure mode should be reviewed to determine if specific or unique concerns exist that could potentially affect breach assumptions, inundation findings, or other items that potentially impact the time available for warning, notification, or evacuation. Items that impact breach development time, breach dimensions, warning time, inundation characteristics, etc. must be considered and documented.

17-4.7.10.6 Follow-up Studies

Each potential failure mode should be reviewed to determine if specific follow-up studies could be considered in better evaluating the significance of the potential failure mode. Follow-up studies should be identified that are aimed to provide additional information and analyses to reduce the uncertainties identified for each potential failure mode. As much as possible, specific information or analyses should be identified and documented to focus the follow-up studies. The team should consider what specific additional information would reduce the uncertainty and increase the confidence in evaluating the disposition of the potential failure mode. For example, suggested follow-up studies might include:

- Gather additional samples of embankment zone 1 and 2 and perform gradation analysis on the samples. Perform filter compatibility analyses of these materials to assist in the evaluation of internal erosion.
- Perform a structural analysis of the spillway piers to evaluate their stability and predict their performance under seismic loads up to and including a 1:50,000 event.
- Investigate potential alternatives to supply back-up power to the spillway gate hoists.
- Evaluate the potential effectiveness of installing an early warning system for a failure of the saddle dam.

Follow-up studies should also be identified for 'insufficient information' potential failure modes. Specific information or studies should be identified that would provide the information needed to adequately evaluate whether the potential failure mode is credible or not.

17-4.7.10.7 Other Information

Any other pertinent information for each potential failure mode should also be captured that may not relate to the sections described above. This may include information the licensee or dam owner may want to identify or track for their use.

17-4.7.11 Close-out Activities

At the end of the PFMA session, the facilitator should ask the participants to reflect on what they learned during the PFMA process. After a short break for the team members to collect their thoughts, the facilitator should ask the participants to state the Major Findings and Understandings they gained during the PFMA session. Typically, this is done by going around the room and asking each participant to provide a Major Finding and Understanding and then starting again with the first person until all participants have had the opportunity to express their findings. Major Findings and Understandings may relate directly to a potential failure mode or may reflect a more general understanding about the dam or the PFMA process. Relative to a potential failure mode, Major Findings and Understandings can be related to the loading magnitude, the performance of the dam given the loading, and the potential consequences. Likewise, Major Findings and Understandings of potential failure modes can be related to performance monitoring, particular aspects of the failure progression or pathway, the influence of human factors, system influences, and emergency planning and preparedness, as well as other factors.

If any Major Finding and Understanding describes a serious dam safety issue, this should be immediately brought to the attention of the FERC-D2SI Regional Office.

The Major Findings and Understandings should be discussed and documented at the end of the session. The items noted during the session are typically abbreviated and should accurately reflect what the individual participants stated as their major finding or understanding gained during the session. Where the Major Finding and Understanding relates to a potential failure mode, a brief discussion (three to five sentences) relating the Major Finding and Understanding to the potential failure mode should be prepared and included with the Major Finding and Understanding. Appendix 17-I provides an example of a write up of major findings and understandings resulting from a PFMA.

17-4.8 Documentation of the Potential Failure Mode Analysis

For the knowledge gained, information obtained, and results achieved in the PFMA to be effectively used, the documentation of the work must:

- Be done promptly;

- Be definitive in describing the identified PFM;
- Be complete in recording factors considered relative to the viability of each PFM considered;
- Discuss possible risk reduction actions identified relative to each credible PFM (e.g., surveillance and/or monitoring, investigations, remediation activities); and
- Clearly relay the major findings and understandings achieved as a result of the process.

Depending on the purpose of the PFMA, a separate, stand-alone PFMA report may be required, or when the PFMA is performed as part of a risk analysis, the PFMA portion of the work can be summarized in a separate chapter(s) of the risk analysis report (see Chapter 18 of the Engineering Guidelines for an example of a Level 2 risk analysis). An example of a completed potential failure mode write-up using the potential failure mode template is included in Appendix 17-J.

However it is documented, the PFMA document must include a description of each potential failure mode considered and referencing key adverse/likely and positive/not likely factors, identifying any suggested visual surveillance or instrumental monitoring, describing consequences of potential failure and site-specific conditions or factors related to consequences and noting any potential actions identified (information inquiries, investigations, analyses or risk reduction opportunities). The potential failure mode should be presented pictorially whenever possible. The write up should include a brief statement as to the adequacy of the project documentation and overall quality of the data that formed the basis of the PFMA. If prepared technical presentations of new material, not contained in the record documents, were made by consultants during the course of the PFMA, their presentation(s) should be documented in, or appended to, the PFMA report.

Appendix 17-K provides an example outline for documenting the PFMA as a stand-alone document. This outline is designed to take advantage of the information collected on the potential failure mode template or flip charts during the PFMA session in order to make the documentation process simple, fast and effective. The report should also include a summary table of credible potential failure modes, similar to Table 2.

Preparing a list of the documents gathered by the owner for review, in advance of the review, has been found to serve as a valuable tool for the reviewers to use to ensure that they have seen all the materials collected and should be included in the PFMA report.

All reference material available and used by the team in the PFMA is recorded and key items of data and information are included in an appendix to the PFMA report for ready reference. Photos of past conditions or photos of current conditions, expounding key information about a potential failure mode, are highly recommended for inclusion in the body or appendix of the PFMA report. The PFMA appendix should be concise.

It is not the intent of the PFMA appendix to include all of the reports and documents that comprise the "background material" that was read and used in the discussions. However, often a key paragraph, photograph, test results or other documentation is found in a document that elucidates whether or not a potential failure mode is more or less likely, and it is valuable to include that specific information in the PFMA appendix. (e.g. photographs may show planar joints, or shotcrete treatment of the foundation, or shear keys; statements might be made by a Board of Consultants about the condition of the filter material, tests results might provide definitive information that counters what has been stated in opinions/observations in construction reports; erosion or the lack of it may have been documented following a flood). These specific pages, photos, quotations, or data that provide direct support to the "likely" or "not likely" aspects of a potential failure mode should be reproduced and included in the appendix to the PFMA report.

The report should state whether the findings are the consensus of the team. If not a consensus, the differences of opinion and reasons therefore should be documented in the report findings.

The report should include an assessment of the overall adequacy, completeness and relevance of background data that was furnished for the PFMA, identify any discrepancies, inaccuracies, or deficiencies in the records, and determine if adequate information was provided to conduct the PFMA. The report should document any potential shortcomings in the PFMA due to lack of sufficient data for consideration of specific potential failure modes.

It is important to understand that if the PFMA report does not accomplish the goals of the PFMA – identifying and obtaining a clear understanding of each dam's site-specific potential failure modes – at the discretion of the Regional Engineer, the PFMA may be required to be supplemented or redone entirely.

17-5 POTENTIAL FAILURE MODE ANALYSIS PROVISIONS

17-5.1 General

Unless otherwise provided in the FERC Engineering Guidelines or directed by the Regional Engineer, the time frame for completing the documentation of the PFMA is provided in the table below. A notable exception to this schedule is when the PFMA is completed by the Part 12D Independent Consultant Team, in which case the revised PFMA report is typically submitted in conjunction with the Part 12D Report.

Action	Schedule
Prepare draft PFMA report and submit for PFMA team review	Within 30 days of the PFMA session
Complete review of draft PFMA report	Within 60 days of the PFMA session
Prepare revised PFMA report and submit to FERC-RO	Within 90 days of the PFMA session

When a PFMA is performed in conjunction with a risk analysis, the documentation of the PFMA should follow the requirements of the documentation of the risk analysis. Refer to Chapter 18 of the FERC Engineering Guidelines for more information.

17-5.2 Updating a Potential Failure Mode Analysis

It is possible that new information could come to light in the interim between the regularly scheduled PFMAs. In this case, the licensee would prepare a supplemental potential failure mode description and provide it for distribution to the STID holders as described above. In this way, the PFMA report as maintained in Section 1 of the STID is a living document that will document the progression and variety of analyses and professional opinions that went into the current updated/appended PFMA report findings.

It is important to retain the PFMA report as prepared so that the findings, discussions and thought processes of the PFMA session are retained for future evaluations.

17-6 REFERENCES

Alvi, I. (2013), "Human Factors in Dam Failures", ASDSO Dam Safety Conference Proceedings.

Bureau of Reclamation/US Army Corps of Engineers (2019), "Best Practices in Dam and Levee Safety Risk Analysis", Chapter A-03, Potential Failure Mode Analysis, Denver, CO.

Federal Emergency Management Agency (2015), "Federal Guidelines for Dam Safety Risk Management", FEMA P-1025, Washington, DC.

Hartford, D., and G.B. Baecher (2004), Risk and Uncertainty in Dam Safety, Thomas Telford Publishing, London.

Kahneman, D. (2011), Thinking Fast and Slow, Farrar, Straus and Giroux, New York.

U.S. Army Corps of Engineers (2014), "Safety of Dams – Policy and Procedures," ER 1110-2-1156, Washington, DC.

Vick, S.G. (2002), Degrees of Belief, American Society of Civil Engineers.

Page intentionally left blank

Table 1: Notur Dam - Summary of Candidate Potential Failure Modes

PFM #	Structure/ Feature	Loading Condition	Failure Mechanism	PFM Description
ND-MD-N-IE-01	Main Dam	Normal	Internal Erosion	Concentrated leak erosion of embankment materials along left spillway training wall res uncontrolled release of reservoir.
ND-MD-N-IE-02	Main Dam	Normal	Internal Erosion	Concentrated leak erosion of poorly compacted zone 1 core material into and through d
ND-MD-N-IE-03	Main Dam	Normal	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement of the e
ND-MD-N-IE-04	Main Dam	Normal	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement caused
ND-MD-N-IE-05	Main Dam	Normal	Internal Erosion	Backward erosion piping of embankment materials into a defect in the toe drain pipe
ND-MD-N-IE-06	Main Dam	Normal	Internal Erosion	Backward erosion piping of Zone 1 core materials into void space in foundation open w
ND-MD-N-IE-07	Main Dam	Normal	Internal Erosion	Backward erosion piping of continuous foundation sand layer in lower left abutment.
ND-MD-N-SS-01	Main Dam	Normal	Slope Stability	Weak layers within the embankment that may have resulted from original construction release of reservoir.
ND-MD-N-SS-02	Main Dam	Normal	Slope Stability	Toe drains clog/become ineffective, causing a rise in the phreatic surface that result in p overtopping, and uncontrolled release of reservoir.
ND-MD-N-E-01	Main Dam	Normal	Erosion	Upstream wave action due to high winds causes significant erosion of the embankment the crest. This allows flow through the embankment, erosion of the embankment and ev
ND-MD-F-O-01	Main Dam	Flood	Overtopping	Low areas at the left and right ends of the embankment crest are overtopped during a hi embankment failure, and uncontrolled release of reservoir.
ND-MD-F-E-01	Main Dam	Flood	Erosion	Upstream wave action due to high winds causes significant erosion of the embankment the crest. This allows flow through the embankment, erosion of the embankment and ev
ND-MD-F-E-02	Main Dam	Flood	Erosion	Upstream wave action due to high winds causes significant erosion of the embankment crest.
ND-MD-F-IE-01	Main Dam	Flood	Internal Erosion	Concentrated leak erosion of embankment materials along left spillway training wall res uncontrolled release of reservoir.
ND-MD-F-IE-02	Main Dam	Flood	Internal Erosion	Concentrated leak erosion of poorly compacted zone 1 core material into and through d
ND-MD-F-IE-03	Main Dam	Flood	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement of the e
ND-MD-F-IE-04	Main Dam	Flood	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement caused
ND-MD-F-IE-05	Main Dam	Flood	Internal Erosion	Backward erosion piping of embankment materials into a defect in the toe drain pipe
ND-MD-F-IE-06	Main Dam	Flood	Internal Erosion	Backward erosion piping of Zone 1 core materials into void space in foundation open w
ND-MD-F-IE-07	Main Dam	Flood	Internal Erosion	Backward erosion piping of continuous foundation sand layer in lower left abutment.
ND-MD-F-IE-08	Main Dam	Flood	Internal Erosion	Concentrated leak erosion occurs in upper part of zone 1 core above normal pool elevat
ND-MD-F-SS-01	Main Dam	Flood	Slope Stability	Weak layers within the embankment that may have resulted from original construction release of reservoir.
ND-MD-F-SS-02	Main Dam	Flood	Slope Stability	High phreatic surface in the embankment leads to instability of the downstream embank
ND-MD-F-SS-03	Main Dam	Flood	Slope Stability	High phreatic surface in the embankment leads to instability of the downstream slope re release of the reservoir
ND-MD-EQ-LQ-01	Main Dam	Seismic	Liquefaction	Liquefaction of the low density foundation sand occurs resulting in slope failure and un
ND-MD-EQ-IE-01	Main Dam	Seismic	Internal Erosion	Concentrated leak erosion occurs in zone 1 core due to seismically-induced transverse c the reservoir.
ND-MD-EQ-IE-02	Main Dam	Seismic	Internal Erosion	Concentrated leak erosion occurs in zone 1 core due to seismically-induced transverse c embankment but does not lead to breach.
ND-MD-EQ-D-01	Main Dam	Seismic	Deformation	Seismic deformation of the embankment leads to loss of freeboard and overtopping resu
ND-SS-F-SS-01	Service Spillway	Flood	Sliding Stability	The spillway gate structure fails by sliding on a weak layer in the foundation

PFM #	Structure/ Feature	Loading Condition	Failure Mechanism	PFM Description
ND-SS-F-E-02	Service Spillway	Flood	Erosion	Cavitation of chute slab leads to erosion and damage to concrete slab
ND-SS-F-GF-01	Service Spillway	Flood	Gate Failure	One or more spillway gates cannot be opened, resulting in overtopping of the embankm uncontrolled release of reservoir.
ND-SS-F-GF-02	Service Spillway	Flood	Gate Failure	Debris (logs, bogs, ice flows) clogs one or more spillway gates opening during high flo causing overtopping of embankment, massive erosion, failure and uncontrolled release
ND-SS-F-GF-03	Service Spillway	Flood	Gate Failure	Loss of power during a high flow event prevents operation of gates, resulting in overtop reservoir.
ND-SS-F-GF-04	Service Spillway	Flood	Gate Failure	Spillway gates become overstressed resulting in structural failure (buckling) and loss of reservoir
ND-SS-F-GF-05	Service Spillway	Flood	Gate Failure	One of more spillway gates fail to close releasing the reservoir to the ogee crest. This l results in lost generation revenues.
ND-SS-F-O-01	Service Spillway	Flood	Other	Loss of communication during flood event results in delayed response or non-response failure and uncontrolled release of reservoir.
ND-SS-F-O-02	Service Spillway	Flood	Other	Lack of resources to respond during the PMF (or other large flood) results in inability t overtopping of the main dam, failure, and uncontrolled release of reservoir.
ND-SS-EQ-SF-01	Service Spillway	Seismic	Structural Failure	Transverse shaking results in overstressing of spillway piers, cracking of the concrete, l in uncontrolled release of the reservoir.
ND-SS-EQ-SF-02	Service Spillway	Seismic	Structural Failure	The spillway training walls become overstressed and fail, causing erosion and failure of uncontrolled release of reservoir.
ND-SS-EQ-GF-02	Service Spillway	Seismic	Gate Failure	Spillway gates become overstressed resulting in structural failure (buckling) and loss of reservoir
ND-ES-F-E-01	Emergency Spillway	Flood	Erosion	Flows over the emergency spillway erode the soil and rock chute floor and headcut upst undermined and fails by sliding or overturning and leads to a breach of the reservoir.
ND-OW-N-GF-01	Outlet Works	Normal	Gate Failure	An outlet gate fails in the open position resulting in uncontrolled release of reservoir.
ND-OW-F-GF-01	Outlet Works	Flood	Gate Failure	An outlet gate fails in the open position resulting in uncontrolled release of reservoir.
ND-OW-F-E-01	Outlet Works	Flood	Erosion	Large releases through the outlet works results in deep scour of the plunge pool. The de erodible silty sand layer in the foundation. High foundation pressures initiate backward and advances upstream. A thick overlying foundation clay forms a roof and internal ero results in an uncontrolled release of the reservoir through an enlarged piping channel in
ND-RR-N-SS-01	Reservoir Rim	Normal	Slope Stability	Landslide on reservoir rim fails into the reservoir resulting in a wave(s) that overtop the downstream slope resulting in breach of the reservoir.
ND-RR-F-SS-01	Reservoir Rim	Flood	Slope Stability	Landslide on reservoir rim fails into the reservoir resulting in a wave(s) that overtop the downstream slope resulting in breach of the reservoir.
ND-RR-EQ-SS-01	Reservoir Rim	Seismic	Slope Stability	Landslide on reservoir rim fails into the reservoir resulting in a wave(s) that overtop the downstream slope resulting in breach of the reservoir.

Notes:

1. The organization of this table by feature, loading condition, and failure mechanism, in that order, is just one way organizing this inf feature, failure mechanism, and then loading condition is also helpful.

2. The potential failure mode number identification is just one suggested example. In the example, the potential failure mode numberi

Table 2: Notur Dam - Summary of Credible Potential Failure Modes

PFM #	Structure/ Feature	Loading Condition	Failure Mechanism	PFM Description	Inspection Opportunities	
ND-MD-N-IE-03	Main Dam	Normal	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement of the embankment caused by soft foundation soils	Look for potential transverse cracks and seepage between sta 7+30 and 10+20 where soft foundation soils are present	We dra see are
ND-MD-N-IE-04	Main Dam	Normal	Internal Erosion	Concentrated leak erosion along transverse cracks due to differential settlement caused by abrupt foundation step in the left abutment	Look for potential transverse cracks and seepage near sta 2+30 on left abutment in vicinity of abrupt foundation step	No ins this
ND-MD-N-IE-05	Main Dam	Normal	Internal Erosion	Backward erosion piping of embankment materials into a defect in the toe drain pipe	Continue to inspect and measure toe drain discharges	Co vid pip
ND-MD-N-IE-06	Main Dam	Normal	Internal Erosion	Backward erosion piping of Zone 1 core materials into void space in foundation open work gravels downstream of core trench.	Likely no direct opportunity for visual inspection of this PFM since material would be hidden in subsurface materials. Look for depressions on downstream slope of embankment for progression of failure mode.	Mo vic lev
ND-MD-N-IE-07	Main Dam	Normal	Internal Erosion	Backward erosion piping of continuous foundation sand layer in lower left abutment.	Inspect lower left abutment groin for signs of seepage and transport of fine sandy materials.	Co pie san cha
ND-MD-N-SS-02	Main Dam	Normal	Slope Stability	Toe drains clog/become ineffective, causing a rise in the phreatic surface that result in progressive slope failure, breaching of the crest, overtopping, and uncontrolled release of reservoir.	Inspect toe drain outfalls for changes in quantity. Check for signs of slope instability on downstream slope.	Per toe cor Me pie pre
ND-MD-F-O-01	Main Dam	Flood	Overtopping	Low areas at the left and right ends of the embankment crest are overtopped during a high flow event causing massive erosion, embankment failure, and uncontrolled release of reservoir.	Inspect areas for adequacy of erosion protection and vegetation control.	Per ele
ND-MD-F-IE-01	Main Dam	Flood	Internal Erosion	Concentrated leak erosion of embankment materials along left spillway training wall resulting in erosion of embankment materials and uncontrolled release of reservoir.	Increase frequency of inspection when reservoir rises above elev. 498	Co dra see cor see

PFM #	Structure/ Feature	Loading Condition	Failure Mechanism	PFM Description	Inspection Opportunities	
ND-MD-F-IE-08	Main Dam	Flood	Internal Erosion	Concentrated leak erosion occurs in upper part of zone 1 core above normal pool elevation due to transverse cracking.	Increase frequency of inspection when reservoir rises above elev. 498	
ND-MD-F-SS-02	Main Dam	Flood	Slope Stability	High phreatic surface in the embankment leads to instability of the downstream embankment slope.	Inspect downstream slope for signs of instability (cracking, bulges, offsets, etc.)	Co exi dow em Co poi cre of Co add crit cov pie
ND-MD-EQ-IE-01	Main Dam	Seismic	Internal Erosion	Concentrated leak erosion occurs in zone 1 core due to seismically-induced transverse cracking.	Continue post-seismic inspections until reservoir is lowered	Mo the
ND-SS-F-SS-01	Service Spillway	Flood	Sliding Stability	The spillway gate structure fails by sliding on a weak layer in the foundation.	Inspect gate structure for signs of distress and offset	Co stru reg
ND-SS-F-SF-01	Service Spillway	Flood	Structural Failure	Plugging of spillway underdrains lead to increased uplift pressures resulting in failure of the concrete slab. The failed slab leads to erosion of the foundation materials and headcutting toward the crest structure. The erosion continues and undermines the crest structure resulting in sliding or overturning of the structure and release of the reservoir.	Continue to inspect condition of spillway underdrains, including measuring drain flows	Co pie slal
ND-SS-F-GF-01	Service Spillway	Flood	Gate Failure	One or more spillway gates cannot be opened, resulting in overtopping of the embankment, erosion, embankment failure and uncontrolled release of reservoir.	Continue monthly, annual, and 10-year inspection program of gates, mechanical, and electrical equipment for signs of distress.	Co pro Co test
ND-SS-F-GF-02	Service Spillway	Flood	Gate Failure	Debris (logs, bogs, ice flows) clogs one or more spillway gates opening during high flows, resulting in inability to pass flood flows, causing overtopping of embankment, erosion, failure and uncontrolled release of reservoir.	Continue daily, weekly, and monthly monitoring program of reservoir for signs of debris.	
ND-SS-F-GF-03	Service Spillway	Flood	Gate Failure	Loss of power during a high flow event prevents operation of gates, resulting in overtopping failure and	Continue daily, weekly, and monthly inspection and	Co and

PFM #	Structure/ Feature	Loading Condition	Failure Mechanism	PFM Description	Inspection Opportunities	
ND-SS-F-O-01	Service Spillway	Flood	Other	Loss of communication during flood event results in delayed response or non-response to site, resulting in embankment overtopping failure and uncontrolled release of reservoir.		
ND-SS-F-O-02	Service Spillway	Flood	Other	Lack of resources to respond during the PMF (or other large flood) results in inability to attain full discharge capacity, resulting in overtopping of the main dam, failure, and uncontrolled release of reservoir.		
ND-SS-EQ-GF-02	Service Spillway	Seismic	Gate Failure	Spillway gates become overstressed resulting in structural failure (buckling) and loss of gate resulting in uncontrolled release of the reservoir	Continue monthly, annual, and 10-year inspection program of gates, mechanical, and electrical equipment for signs of distress.	Co pro Co tes
ND-ES-F-E-01	Emergency Spillway	Flood	Erosion	Flows over the emergency spillway erode the soil and rock chute floor and headcut upstream to the crest structure. The crest structure is undermined and fails by sliding or overturning and leads to a breach of the reservoir.	Inspect condition of emergency spillway after all flows.	Per sur spi dov Per aft cor
ND-OW-N-GF-01	Outlet Works	Normal	Gate Failure	An outlet gate fails in the open position resulting in uncontrolled release of reservoir.	Continue monthly, annual, and 10-year inspection program of gates, mechanical, and electrical equipment for signs of distress.	Co pro
ND-OW-F-GF-01	Outlet Works	Flood	Gate Failure	An outlet gate fails in the open position resulting in uncontrolled release of reservoir.	Similar to ND-0W-N-GF-01	Sin
ND-RR-F-SS-01	Reservoir Rim	Flood	Slope Stability	Landslide on reservoir rim fails into the reservoir resulting in a wave(s) that overtop the embankment and erodes the crest and downstream slope resulting in breach of the reservoir.	Perform annual inspection of landslides within the reservoir rim	Co mo (su crit

Page intentionally left blank

APPENDIX 17-A: INFLUENCE OF HUMAN FACTORS

Appendix J of the Independent Forensic Team Report, Oroville Dam Spillway Incident, January 5, 2018 provides some excellent background on what the term 'human factors' involves, describes the human factor framework, and highlights some higher-level human factors that contributed to the incident. Select passages and text from that Appendix are summarized and reproduced in the sections below.

All tables and figures from "Human Factors in the Oroville Dam Spillway Incident", ASDSO Webinar by Irfan Alvi, Alvi Associates, Inc., August 2018.

1.0 BACKGROUND ON HUMAN FACTORS

The field of "human factors" considers how and why systems meet or do not meet performance expectations, with an emphasis on understanding and prevention of incidents and failures (including major incidents). The systems considered in human factors work typically include both human and physical aspects, and are sometimes referred to as "sociotechnical" systems.

The range of human factors which may be considered spans scales of individuals, groups, organizations, industries, and the broader social, economic, and political context. Accordingly, human factors involve application of social science and draws on knowledge from fields such as psychology, social psychology, sociology, cultural anthropology, management, economics, political science, and history. At the same time, because human factors approaches are often applied to physical systems, such as dams, specialist knowledge of these physical systems is also necessary. As a result, human factors is a highly interdisciplinary field.

The field of human factors has evolved and grown during the past few decades, and a variety of frameworks have been developed. These frameworks generally have overlapping aspects, but with some variety in their assumptions and the aspects they emphasize. Therefore, each framework has particular strengths and limitations. The literature on human factors is very extensive, and references [1 through 25] are a selected sample of the literature, which describe many human factors frameworks.

Human factors approaches have been extensively applied in fields such as aviation, nuclear power, chemical processing, and health care. The application of human factors approaches specifically to civil infrastructure, particularly dam safety, is more recent, with most of this work having occurred during the past decade. References [26 through 45] describe some of this work, with an emphasis on applications to dams.

2.0 HUMAN FACTORS FRAMEWORK

Additional information on general human factors framework can be found in the following references [35, 39, 40, 41, 42, and 45].

2.1 Key Observations and Assumptions

The human factors framework is based on the following observations regarding past failures of dams and other systems:

- Failures are typically preceded by interactions of physical and human factors which begin years or decades prior to the failure [7].
- The interactions among physical and human factors are often not simple and linear. Instead, they may be complex and involve nonlinear relationships, feedback loops, causes having multiple effects, effects having multiple causes, and a lack of distinct "root causes" or dominant contributing factors [5, 9, 14, 16, and 20].
- Interactions among physical and human factors usually generate "warning signs" which are not recognized, or not sufficiently acted upon, prior to failures [25].
- Physical processes deterministically follow physical laws, with no possibility of physical "mistakes." Therefore, failures – in the sense of human intentions not being fulfilled – are fundamentally due to human factors, as a result of human efforts individually and collectively "falling short" in various ways. A story of why a failure happened therefore cannot be complete without reference to contributing human factors [7].
- A natural tendency is for systems to move towards disorder and failure, in line with the concept of increasing entropy in physics. Therefore, systems such as dams are typically not inherently "safe" [6], and continual human effort is needed to maintain order and prevent failure [3, 15, and 21].
- Systems such as dams, including the people involved in designing, building, operating, and managing them, tend to conservatively have numerous "barriers" which must be overcome for failures to occur [3 and 11]. This generally makes failures unlikely and results in very low overall failure rates. However, when dealing with a large number of systems, such as the approximately 90,000 dams in the United States, it can be expected that "unlikely" failures will sometimes occur, due to physical and human factors "lining up" in an adverse way that overcomes all barriers [3].

With these observations in mind, the propensity towards failure can be viewed as being determined by the balance of human factors which contribute to failure ("demand") versus those which contribute to safety ("capacity"). Thus, applying a standard

engineering metaphor, failure results when human factors demand on the system exceeds capacity, and safety results when capacity exceeds demand.

2.2 Primary Drivers of Failure

The human factors contributing to safety "demand," and therefore the potential for failure, can generally be placed into three categories of primary drivers of failure:

- Pressure from non-safety goals [20] such as delivering water, generating power, reducing cost, meeting schedules, building and maintaining relationships, personal goals, and political goals.
- Human fallibility and limitations associated with misperception, faulty memory, ambiguity and vagueness in use of language, incompleteness of information, lack of knowledge, lack of expertise, unreliability of intuition, inaccuracy of models [46], cognitive biases operating subconsciously at the individual level [47 through 50] and group level [50 and 51], use of heuristic shortcuts [48], emotions, and fatigue.
- Complexity resulting from multiple system components having interactions which may involve nonlinearities, feedback loops, network effects, etc. Such interactions can result in large effects from small causes, including "tipping points" when thresholds are reached, and they make complex systems difficult to model, predict, and control [5, 20, and 52]. Complexity generally exacerbates the effects of human fallibility and limitations.

Pressure from non-safety goals	Human fallibility and limitations	Complexity
• Delivering water • Generating power • Reducing costs • Meeting schedules • Building and maintaining relationships • Personal goals • Political goals	• Misperception and faulty memory • Ambiguity and vagueness in use of language • Limited information and knowledge • Limited skill and expertise • Cognitive biases and heuristics at individual and group levels • Unreliability of intuition and inaccuracy of models • Effects of emotions and fatigue	• Large number of interacting system components • Interactions involving nonlinearities, feedback loops, and network effects • Large effects from small causes, including "tipping points" • Difficulties in system modeling, prediction, and control • Exacerbation of human fallibility and limitations

2.3 Human Error

The primary drivers of failure lead to various types of "human errors," which can include categories such as "slips" (actions committed inadvertently), "lapses" (inadvertent inactions), and "mistakes" (intended actions with unintended outcomes, due to errors in

thinking) [1 and 2]. In the context of dam safety, mistakes are the most common type of human errors that contribute to failures. “Violations” are also sometimes classified as a category of human errors, and involve situations in which there is deliberate non-compliance with rules and procedures, usually because the rules or procedures are viewed as unworkable in practice [1].

2.4 Risk Management

With the above caveats regarding “human errors” in mind, human errors and the underlying primary drivers of failure noted in Section 17-2.2 often lead to inadequate risk management. There are three specific types of inadequacy in risk management due to human errors:

- Ignorance involves being insufficiently aware of risks. This may be due to aspects of human fallibility and limitations such as lack of information, inaccurate information, lack of knowledge and expertise, and unreliable intuition. Complexity can also contribute to ignorance.
- Complacency involves being sufficiently aware of risks, but being overly risk tolerant. This may be due to aspects of human fallibility and limitations such as fatigue, emotions, indifference, and optimism bias (“it won’t happen to me”). Pressure from non-safety goals can also contribute to complacency.
- Overconfidence involves being sufficiently aware of risks, but overestimating ability to deal with them. This may be due to aspects of human fallibility and limitations such as inherent overconfidence bias, which results in overestimating knowledge, capabilities, and performance [48 to 50].

Effect	Definition	Drivers
Ignorance	Insufficiently aware of risks	• Human fallibility and limitations (perception, memory, information, knowledge, expertise, intuition, models, language, confirmation bias) • Complexity
Complacency	Sufficiently aware of risks, but overly risk tolerant	• Human fallibility and limitations (fatigue, emotions, indifference, optimism bias) • Pressure from non-safety goals
Overconfidence	Sufficiently aware of risks, but overestimate ability to manage them	• Human fallibility and limitations (overconfidence bias, pride)

2.5 Safety Culture

Counterbalancing the drivers of failure described in Sections 2.2 through 2.4, the human factors contributing to system capacity for safety generally emanate from what is referred to as “safety culture” [8]. While this term is sometimes interpreted as applying

specifically to worker safety and prevention of injuries on the job, the concept of safety culture is much more general and refers to safety of any system, including dams.

The general idea of safety culture is that individuals at all levels of an organization place high value on safety, which leads to a humble and vigilant attitude with respect to preventing failure [25]. For such a safety culture to be developed and maintained in an organization, the senior leadership of the organization must visibly give priority to safety, including allocating the resources and accepting the tradeoffs needed to achieve safety.

2.6 Best Practices

Experience in dam safety shows that strong safety cultures naturally lead to implementation of numerous "best practices" for dam safety risk management, with the understanding that these best practices need to be continually challenged, and, therefore, they evolve as the industry learns and improves. As a corollary, dam incidents and failures are typically preceded by long-term cumulative neglect of numerous accepted best practices. These best practices can be organized into two categories: general design and construction features of dam projects, and general organizational and professional practices.

Best practices for general design and construction features of dam projects include the following:

- Specific design and construction best practices: Generally-accepted best practices for specific aspects of design and construction should be identified and applied.
- Design conservatism: Designs should be sufficiently conservative and provide factors of safety commensurate with uncertainties and risks. To the extent possible, designs should also preferably provide physical redundancy, robustness, and resilience, as well as failure modes which generate warning signs.
- Design customization: Designs should be customized to suit features of project sites. This involves "scenario planning" during design to be ready to handle situations which may potentially be encountered during construction, testing during construction to verify that design assumptions and intent are met, and design adaptation during construction to address observed conditions.
- Budget and schedule contingencies: Provisions should be made for accommodating reasonable contingencies when establishing design and construction budgets and schedules.
- Best practices for general organizational and professional practices, which encompass all project phases and tasks, include the following:
- Resources and resilience: Sufficient budget and staffing resources should be provided, so that systems and people are not stretched to their limits, thereby

increasing error and failure rates [20]. The organization should also be resilient, in the sense of having sufficient internal diversity and adaptive capability to provide a broad and flexible repertoire of possible responses to cope with the potential challenges faced by the organization [12].

- Humility, learning, and expertise: Individuals and organizations should humbly recognize the limitations of their knowledge and skills, engage in continuing education and training, learn from study of past incidents and failures, and collaboratively draw on expertise, wherever it may be found, rather than simply deferring to authority based on position in a hierarchy [25].
- Cognitive diversity: Teams should have cognitively diverse membership, to bring in diversity of perspectives, education, training, experience, information, knowledge, models, skills, problem-solving methods, and heuristics [51 and 55]. With effective team leadership, structure, and group dynamics, cognitively diverse teams can avoid problems such as groupthink and can outperform more homogeneous teams of the "best" people. (Groupthink is a phenomenon in which deliberation, judgment, and decision-making of a group and its members are compromised due to the social tendency of group members to seek harmony and coherence).
- Decision-making authority: Decision-making authority should be commensurate with responsibilities and expertise, rather than this authority being contravened by organizational structure [25]. This is particularly the case for safety personnel, who should be selected for their positions based on having relevant experience, vigilance, caution, humility, inquisitiveness, skepticism, discipline, meticulousness, communication ability, and assertiveness.
- System modeling: Appropriate system models should be developed, with a full range of PFMs identified, and emergency action plans developed accordingly. For actively operated systems, such as large hydropower dams, these failure modes should include operational failure modes, and it may be appropriate to explicitly account for interactions of physical and human factors in the system models. Where models are implemented through software, the software should be carefully developed, validated, and used [17].
- Checklists: Checklists should be used to reduce the incidence of human errors, especially for tasks which are relatively recurrent, such as inspections [56]. Checklists should be customized for each situation, clear and unambiguous, focused on items which are important but prone to being missed, prepared at a level of detail appropriate for the time available to use the checklist, and regularly updated based on experience. Recognizing that checklists are most effective for prevention of slips, lapses, and violations, but somewhat less effective for prevention of mistakes (see Section 2.3), checklists should be used to supplement, not replace, situation-specific attentive observation and critical thinking.

- Information management: Information management should involve thorough, well organized, and readily accessed documentation; open and collaborative information sharing within and across organizations; and not being dismissive of dissenting voices. This will enable surfacing and synthesis of fragmentary information to help "connect the dots" and better understand system behavior [23 and 25].
- Warning signs: There should be vigilant monitoring to detect "warning signs" that a system is headed towards failure, while there is still a "window of recovery" available [25]. This monitoring should be conducted at regular intervals, after unusual events, and also during apparent "quiet periods." Once potential warning signs are detected, there should be prompt and appropriate investigative follow up, verification of that follow up, thorough documentation of observations and findings so that emerging patterns can be discerned and evaluated, and prompt implementation of any needed remedial actions. As a heuristic to help judge whether a potential warning sign warrants action, "simulated hindsight" can be used: fast-forward into the future, imagine that failure has occurred, and ask whether ignoring the potential warning was justifiable; if not, take the potential warning sign seriously.
- Standards: High professional, ethical, legal, and regulatory standards should be maintained – especially when lives are at stake.

In summary, organizations which have the capacity to handle demands on safety from various drivers of failure have a strong safety culture and diligently implement numerous best practices. Such organizations are mindful, cautious, humble, oriented towards learning and improving, resiliently adaptive, and maintain high professional and ethical standards. They vigilantly search for and promptly address warning signs before problems grow too large, and they make effective use of available information, expertise, resources, and management tools to properly balance safety against other organizational goals.

Organizational & Professional Best Practices

- Do the owner and regulators have sufficient budget and staff resources?
- Do people involved in the project humbly recognize the limits of their expertise, engaged in continuing education, learn from past incidents and failures, and adequately draw on the expertise available in their organizations?
- Do teams involved in the project have cognitive diversity and effective group dynamics?
- Do models adequately reflect a full range of failure modes, including operational failure modes?
- Are checklists used to help reduce errors for recurrent tasks such as inspections?
- Are the information management systems of the owner and regulators adequate to ensure that people involved with the project had the right information available when they needed it?

- Is dam safety decision-making authority commensurate with responsibilities and expertise? Do safety personnel have appropriate expertise and temperament for their roles?
- Do the people involved with the project vigilantly monitor for warning signs and then properly investigate them, with good documentation?
- Are high professional, ethical, legal, and regulatory standards maintained?

3.0 REFERENCES

[1] Reason, J. (1990) Human Error, Cambridge University Press.

[2] Senders, J. and Moray, N. (1991) Human Error: Cause, Prediction, and Reduction, Lawrence Erlbaum Associates.

[3] Reason, J. (1997) Managing the Risks of Organizational Accidents, Ashgate Publishing Company.

[4] Rasmussen, J. (1997) "Risk management in a dynamic society: a modelling problem," Safety Science, 27 (2-3), 183-213.

[5] Dorner, D. (1997) The Logic of Failure: Recognizing and Avoiding Error in Complex Situations, Basic Books.

[6] Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies, Princeton University Press.

[7] Pidgeon, N. and O'Leary, M. (2000) "Man-made disasters: why technology and organizations (sometimes) fail," Safety Science, 34 (1–3), 15–30.

[8] Patankar, M., Brown, J., Sabin, E., and Bigda-Peyton, T. (2001) Safety Culture, Ashgate Publishing Company.

[9] Strauch, B. (2002) Investigating Human Error: Incidents, Accidents, and Complex Systems, Ashgate Publishing Company.

[10] Woods, D. and Cook, R. (2002) "Nine Steps to Move Forward from Error," Cognition, Technology & Work, 4, 137–144.

[11] Hollnagel, E. (2004) Barriers and Accident Prevention, Ashgate Publishing Company.

[12] Hollnagel, E., Woods, D. and Leveson, N., Eds. (2006) Resilience Engineering: Concepts and Precepts, Ashgate Publishing Company.

[13] Dekker, S. (2005) Ten Questions about Human Error, CRC Press.

[14] Dekker, S. (2006) The Field Guide to Understanding Human Error, Ashgate Publishing Company.

[15] Reason, J. (2008) The Human Contribution: Unsafe Acts, Accidents, and Heroic Recoveries, Ashgate Publishing Company.

[16] Qureshi, Z. (2008) A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems, Report No. DSTO-TR-2094, Australian Defence Science and Technology Organisation.

[17] Woods, D., Dekker, S., Cook, R., Johannesen, L., and Sarter, N. (2010) Behind Human Error, 2nd Ed., Ashgate Publishing Company.

[18] Rosness, R., Grøtan, T., Guttormsen, G., Herrera, I., Steiro, T., Størseth, F., Tinmannsvik, R., and Wærø, I., (2010) "Organisational Accidents and Resilient Organisations: Six Perspectives, Revision 2," No. Sintef A 17034, SINTEF Technology and Society, Trondheim.

[19] Salmon, P., Stanton, N., Lenne, M., Jenkins, D., Rafferty, L., and Walker, G. (2011) Human Factors Methods and Accident Analysis, Ashgate Publishing Company.

[20] Dekker, S. (2011) Drift into Failure: From Hunting Broken Components to Understanding Complex Systems, Ashgate Publishing Company.

[21] Leveson, N. (2011) Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press.

[22] Conklin, T. (2012) Pre-Accident Investigations: An Introduction to Organizational Safety, Ashgate Publishing Company.

[23] Catino, M. (2013) Organizational Myopia: Problems of Rationality and Foresight in Organizations, Cambridge University Press.

[24] Hollnagel, E. (2014) Safety-I and Safety-II: The Past and Future of Safety Management, Ashgate Publishing Company.

[25] Weick, K. and Sutcliffe, K. (2015) Managing the Unexpected: Resilient Performance in an Age of Uncertainty, 3rd Ed., Jossey-Bass.

[26] Peck, R. (1973) "Influence of Nontechnical Factors on the Quality of Embankment Dams," in Embankment-Dam Engineering: Casagrande Volume, Wiley, 201-208.

[27] Melchers, R., (1977) “Organizational Factors in the Failure of Civil Engineering Projects,” Transactions of Institution of Engineers Australia, GE 1, 48-53.

[28] Nowak, A., Ed. (1986) Modeling Human Error in Structural Design and Construction, ASCE.

[29] Sowers, G. (1993) “Human Factors in Civil and Geotechnical Engineering Failures,” ASCE Journal of Geotechnical Engineering, 119:2, 238–256.

[30] Bea, R. (2006) “Reliability and Human Factors in Geotechnical Engineering,” ASCE Journal of Geotechnical and Geoenvironmental Engineering, 132:5, 631–643.

[31] Norstedt, U., Rollenhagen, C., and Eveneus, P. (2008) “Considering Human Factors in Dam Safety,” HRW-Hydro Review Worldwide.

[32] Regan, P. (2010) “Dams as Systems – A Holistic Approach to Dam Safety,” 2010 USSD Conference Proceedings, 1307-1340.

[33] Hill, C. (2012) “Organizational Response to Failure,” 2012 USSD Conference Proceedings, 89-102.

[34] Lord, D. (2012) “The Taum Sauk Dam Failure Was Preventable – How Do We Prevent the Next Operational Dam Failure?” 2012 USSD Conference Proceedings, 139-154.

[35] Alvi, I., (2013) “Human Factors in Dam Failures,” 2013 ASDSO Dam Safety Conference Proceedings.

[36] de Rubertis, K. and van Donkelaar, C. (2013) “Look Both Ways,” 2013 USSD Conference Proceedings, 601-620.

[37] Bryan, C. and de Rubertis, K. (2014) “Examining the Role of Human Error in Dam Incidents and Failures,” USSD Newsletter, 164, 42-49.

[38] Mattox, A., Higman, B., Coil, D., and McKittrick, E. (2014) “Big Dams & Bad Choices: Two Case Studies in Human Factors and Dam Failure,” published online at: http://www.groundtruthtrekking.org/Issues/OtherIssues/dam-failure-human-factors-cases-Teton-Vajont.html

[39] Myers, D., Ferguson, K., Alvi, I., and Baker, M. (2015) “Reexamination and Lessons Learned from the 2004 Failure of Big Bay Dam, Mississippi,” ASDSO Journal of Dam Safety, 13:2, 9-18.

[40] Alvi, I. (2015) “Human Factors in Dam Failure & Safety, Case Study: Ka Loko Dam Failure,” 2015 ASDSO Northeast Regional Conference Keynote Address.

[41] Alvi, I. (2015) “Failure of Sella Zerbino Secondary Dam in Molare, Italy,” 2015 ASDSO Dam Safety Conference Proceedings.

[42] Alvi, (2015) “Human Factors in Dam Failure and Safety,” ASDSO November 2015 webinar.

[43] Ascila, R., Baecher, G., Hartford, D., Komey, A., Patev, R., and Zielinski, P. (2015) “Systems analysis of dam safety at operating facilities,” 2015 USSD Conference Proceedings.

[44] Hartford, D., Baecher, G., Zielinski, P., Patev, R., Ascila, R., and Rytters, K. (2016) Operational Safety of Dams and Reservoirs: Understanding the reliability of flow-control systems, ICE Publishing.

[45] Alvi, I., Richards, G., and Baker, M. (2016) “10th Anniversary of Ka Loko Dam Failure, Hawaii,” 2016 ASDSO Dam Safety Conference presentation.

[46] Alvi, I. (2013) “Engineers Need to Get Real, But Can't: The Role of Models,” ASCE Structures Congress 2013, 916-927.

[47] Plous, S. (1993) The Psychology of Judgment and Decision Making, McGraw-Hill.

[48] Gilovich, T., Griffin, D., and Kahneman, D., Eds. (2002), Heuristics and Biases: The Psychology of Intuitive Judgment, Cambridge University Press.

[49] Kahneman, D. (2011) Thinking, Fast and Slow, Farrar, Straus and Giroux.

[50] Kiser, R. (2010) Beyond Right and Wrong: The Power of Effective Decision Making for Attorneys and Clients, Springer Verlag.

[51] Sunstein, C. and Hastie, R. (2015) Wiser: Getting Beyond Groupthink to Make Groups Smarter, Harvard Business Review Press.

[52] Mitchell, M. (2011) Complexity: A Guided Tour, Oxford University Press.

[53] Shaver, K. (1985) The Attribution of Blame: Causality, Responsibility, and Blameworthiness, Springer Verlag.

[54] Rescher, N. (1995) Luck: The Brilliant Randomness of Everyday Life, Farrar Straus & Giroux.

[55] Page, S. (2008) The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies, Princeton University Press.

[56] Gawande, A. (2010) The Checklist Manifesto: How to Get Things Right, Henry Holt and Company.

APPENDIX 17-B: COMMON BIAS AND HEURISTICS

Some common heuristics and biases include (adapted from Kahneman, 2011):

- **Affect Heuristic –** Judgments and decisions made by consulting one's emotions without consideration of the applicable information. (How do I feel about it?)
- **Anchoring Effect** – Occurs when one considers a particular value for an unknown quantity before developing an estimate for that quantity. Estimates then stay close to the initial number one considered. Any number that you are asked to consider as a possible solution prior to an estimate will induce an anchoring effect. Adjustment is a deliberate attempt to find reasons to move away from the anchor. Adjustments almost always end prematurely.
- **Availability Heuristic** – The process of judging frequency by the ease with which instances come to mind.
- **Certainty Effect –** Outcomes that are almost certain are given less weight than their probability justifies.
- **Confirmation Bias** – People seek data that are likely to be compatible with the beliefs they currently hold. They favor uncritical acceptance of suggestions and exaggeration of the likelihood of extreme and improbable events.
- **Conjunctive Fallacy** – Occurs when one judges a conjunction of two events more probable than one of the events by itself.
- **Halo Effect** – A common bias that plays a large role in shaping our view of people and situations. The tendency to like (or dislike) everything about a person or situation – including things you have not observed. Increases the weight of first impressions (people, situations, information) sometimes to the point that subsequent information is wasted or ignored.
- **Hindsight Bias** – The inability to reconstruct past beliefs will cause one to underestimate the extent to which you were surprised by past events.
- **Intuitive Predictions** – These predictions are generally biased and tend to be overconfident and overly extreme. Individuals have not learned to identify the situations in which their intuition will betray them. The unrecognized limits of professional skill help explain why experts are often overconfident. Whether professionals have a chance to develop intuitive experience depends essentially on the quality and speed of feedback, as well as on sufficient experience to practice.
- **Narrative Fallacy** – Flawed stories of the past shape our views of the world and our expectations (predictions) for the future. We constantly fool ourselves by constructing flimsy accounts of the past and believing they are true.

- **Optimistic Bias –** Everything is always good. Only see the favorable side of the argument.
- **Outcome Bias –** Are influenced by the planned result or past results.
- **Planning Fallacy –** Overly optimistic forecasts of the outcome of projects. Unrealistically close to the best-case scenario (planning and cost estimating).
- **Plausibility vs Probability –** They are not equal, but some folks treat them as though they are.
- **Possibility Effect –** Causes highly unlikely outcomes to be weighted disproportionately more than they deserve.
- **Probability Neglect –** The amount of concern is not adequately sensitive to the probability of harm. You are imagining the numerator and ignoring the denominator. An example – your teenager is late getting home.
- **Probability of the Rare Event –** People overestimate the probability of rare events and overweight unlikely events.
- **Subjective Confidence –** Unrecognized limits of professional skill can lead to overconfidence in experts. The main obstacle is that subjective confidence is determined by the coherence of the story one has constructed, not on the quality and amount of information it supports. "A compelling narrative fosters an illusion of inevitability." "Organizations that take the word of overconfident experts can expect costly consequences."
- **The 'Law of Small Numbers' –** A general bias that favors certainty over doubt. People are not adequately sensitive to sample size.

APPENDIX 17-C: SYSTEM UNDERSTANDING

1.0 OVERALL APPROACH

1.1 General

The following is a suggested approach for evaluating complex systems as part of a potential failure mode analysis (PFMA). This simplified approach is modeled after Halpin, et.al., 2020 and is based on limited application of the approach used for pilot semi-quantitative risk analysis (SQRA) studies. It is anticipated that through application and experience, this approach will evolve and improve over time.

Prior to developing an understanding of how the project functions as a system it is imperative to review all available project information and reports and thoroughly understand the operational aspects and procedures of the project. This background information and understanding should be used to assist in identifying and describing potential failure modes during the brainstorming session as well as evaluating relationships and dependencies within and between potential failure modes identified from the brainstorming session.

The first step of this approach is to separate the problem into two parts and to simplify the scope and effort to project specific issues. This includes:

1. Identify the primary and secondary system relationships between the components/structures of the dam and other project components; and then

2. Consider the interaction between human and physical factors.

These activities are typically done in the PFMA team environment with an emphasis on those individuals with particular knowledge of operations, governance, emergency management, and regulation. Together the findings from these two efforts, in combination with the risk evaluation from an SQRA or other risk analysis, can be sorted and prioritized for criticality, and then used to further understand the influence the risk management options and actions for the project.

1.2 Identifying Relationships Between the Physical Elements of Infrastructure

The potential failure mode process is a key enabler of this step as it has established the individual and independent points of failure within the system. The goal of this activity is to identify dependencies between the various components/structures based on the potential failure modes and discover general vulnerabilities within the system. This process is also helpful in identifying influence factors that could positively or adversely

affect other structures within the system. Potential failure modes can be evaluated and flagged as having system considerations during the potential failure mode evaluation process so they can be discussed during the system evaluations. After these initial efforts, some specific scenarios can be developed which consider more complex interactions among system components. This improves the understanding of system complexities and potential feedback loops and interdependencies.

1.3 Identifying the Interaction of Human and Physical Factors

The second effort is to include the interaction of human and physical factors. Human factors may be considered in general accordance with the framework outlined in Appendix 17-A. This element requires that the team brainstorm factors that could contribute to the potential for failure, such as pressure from non-safety goals, human fallibility and limitations, and system complexity, and discuss human errors that could result from these factors. Categories of human errors include slips, lapses, mistakes and violations. The situations and context which could lead to those errors should be explored and documented at both a global level and then at an individual structure level. The discussions cover both issues specific to the project under consideration but also the broader organizations of the owner, the regulator, and any potential stakeholders.

As a means to manage scope of work for assessing human factors and systems issues at the PFMA level, comprehensive evaluation of broad organizational issues such as the safety culture, human factors associated with the existing regulatory frameworks, and the adequacy of the current dam safety practices are programmatic in nature and go beyond any individual facility. As such, their inclusion should be considered carefully. Below is a summary of aspects of human factors and system interactions typically included and excluded from the PFMA and SQRA efforts:

Aspects typically included in a PFMA and SQRA:

- For individual potential failure modes – detection, intervention factors, decision making, and uncertainty;

- System considerations – primary and secondary relationships between components; and

- For system considerations – human actions, inactions, decisions that contribute to system performance and human errors that they could lead to: slips (actions committed inadvertently), lapses (inadvertent actions), mistakes (intended actions with unintended outcomes), and violations (deliberate non-compliance with rules and protocols).

Aspects typically excluded from a PFMA and SQRA:

- Dam safety organizational culture (trust between parts of the organization, training, expertise, biases such as overconfidence, etc.);

- Existing regulatory framework and human factors associated with it;

- Operational Plan – accept as-is, not subject to evaluation (but could consider intentional plan deviation); and

- State of the industry practice (e.g. a study or analysis performed in accordance with state of the practice proves to be incorrect at some later date).

1.4 Assessment

Once the system relationships are defined qualitatively, the influence of human factors should be added to the assessment. The modified potential failure modes can then be further developed, evaluated, and screened, as appropriate, in accordance with the guidance provided in this chapter.

At the SQRA level, risk estimates are not typically developed for any of the system interaction scenarios identified as doing this would be well beyond the scope of the SQRA process. System interactions and chain reactions have high levels of complexity that can only be captured in fully quantitative risk assessment with Monte-Carlo simulations. As stated in the Oroville Independent Forensic Team Report, Appendix J: "The interactions among physical and human factors are often not simple and linear. Instead, they may be complex and involve nonlinear relationships, feedback loops, causes having multiple effects, effects having multiple causes, and a lack of distinct "root causes" or dominant contributing factors…Such interactions can result in large effects from small causes, including "tipping points" when thresholds are reached, and they make complex systems difficult to model, predict, and control".

2.0 IDENTIFYING INFRASTRUCTURE INTER-RELATIONSHIPS

Dam systems often have multiple physical features that are separable, independent structures but are part of a larger system. Although each structure has a unique purpose, its performance can also impact other structures within the system. To identify the inter-relationships between the various structures, the assessment should systematically evaluate first order relationships and dependencies one structure at a time.

For each structure, three conditions can be considered:

1. the structure performs as intended,

2. the structure cannot be operated as intended (either the structure cannot be operated at all or the structure cannot be operated to its full capacity or capability), or
3. the structure fails and results in an uncontrolled release of the reservoir.

For some structures, not all three conditions are applicable. An example of this would be an intake structure, which can operate as intended, or it can also exist in a state where it cannot be operated (gates to allow flow into the penstocks fail in the closed position and water cannot be released through the intake structure). The third condition, uncontrolled release through the intake structure is not realistic, since there would be two ways to shut off flow through the powerplant if the flow cannot be shut off at the intake structure.

Following is an example which addresses a typical structure and provides a figure (Figure 1) that shows the relationships between other structures for a given condition. Structures that are part of the project are shown as blue ovals. Other structures that are important from the system interactions perspective but are not components of the project are shown as dash line ovals on the right side of the chart. The structure and condition being evaluated is located at the top center of the chart and distinguished from all other structures by orange color. Relationships are identified by arrows. First order relationships are shown with solid lines, second order relationships are shown with dashed lines. For clarity, not all second and higher order relationships and feedback loops describing the entire system are shown. The direction of the arrow illustrates causes and effects, while colors distinguish between impacts (orange) and dependencies/demands (blue). If there is no arrow connecting the structure being evaluated with another structure, these structures are considered independent for a given condition/scenario. These charts are building blocks and can be used to obtain a comprehensive picture of relationships among all the features under a given condition. Such a diagram would be created for each independent structure and load condition, following by a narrative conclusion.

Note: inter-relationships between physical structures are heavily influenced by the capability of water release and control at the individual structures. It is helpful to summarize these water management attributes prior to displaying the inter-relationships.

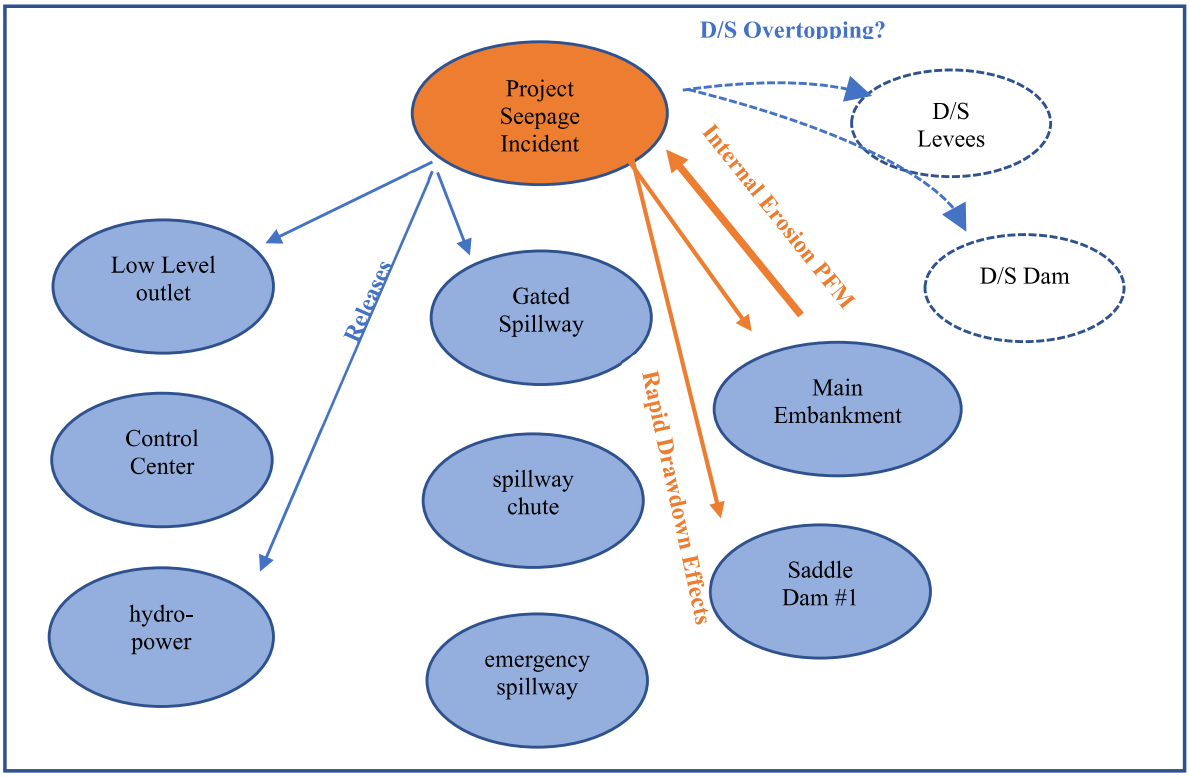


Figure 1 – Systems Relationships for Seepage Incident Example

Under condition 1, where the outlets operate as intended, there are a number of relationships as shown on Figure 1, including potential sudden drawdown impacts on the project embankments and potential overtopping of downstream dams and levees. Under Condition 2, where the outlets can't operate as intended, the seepage incident potentially worsens resulting in secondary relationships with emergency intervention and emergency notifications and evacuations, possibly. If releases through the gated spillway cannot match inflows (either due to inflows exceeding the capacity of the gated spillway or due to limitations on spillway releases imposed by the Water Control Plan), the emergency spillway will engage.

It is likely that the powerplant and the low-level outlets will be impacted by tailwater from large releases through the gated spillway, requiring a shutdown of these features when the tailwater gets high enough. Additionally, the powerplant is flooded at gradually higher releases.

Large releases through the gated spillway or combined gated spillway and emergency spillway releases) also have the potential to breach or overtop levees and/or dams downstream.

Under Condition 2 (not shown), the gated spillway could not be operated as intended and the release capacity of the spillway is limited either due to debris plugging or gate reliability issues. Limited spillway capacity would result in smaller than required releases during a flood, which would increase the maximum reservoir water surface elevation at the dam and saddle dam. There would be multiple impacts if capacity through the gated spillway was reduced:

- The powerplant and the low-level outlet would potentially be required to be operated more extensively to compensate for the reduced releases through the gated spillway.

- There could be issues created in the chute for the gated spillway if the reduced capacity through the spillway created unbalanced flow conditions (if one or more gates could not be opened at all or if debris disproportionally impacted some gates more than others).

- The emergency spillway could be adversely affected if the reduced gated spillway triggers operation of the emergency spillway, when it would not have operated if the full gated spillway capacity was available.

- The main embankment dam and saddle dam would likely experience a higher maximum reservoir water surface during a flood if the spillway capacity is reduced. The reduced capacity will result in more water being temporarily stored and will increase the maximum reservoir water surface elevation.

- There could be a benefit to the downstream levees with reduced gated spillway deliveries. For a given flood, the levees will experience lower flows and a reduced chance of overtopping or failing from other mechanisms.

For Condition 3, an uncontrolled release, a unique set of relationships would exist, with some dependent on the flow and/or discharge location: (not shown on figure).

- If the uncontrolled release was the result of a catastrophic failure of the gated spillway structure, the tailwater could increase significantly enough to flood the powerplant and the low level outlet.

- Depending on the size of the uncontrolled release, flows could exceed the capacity of the gated spillway chute and result in the chute walls being overtopped.

- Large uncontrolled releases through the gated spillway would lower the reservoir and either reduce flows over the emergency spillway or lower the chance of it being activated.

- The main embankment and saddle dam could experience rapid drawdown conditions if the uncontrolled releases through the gated spillway significantly exceeded the inflows into the reservoir.

- If the main embankment is in direct proximity of the gated spillway it may experience erosion and head-cutting.

There could be downstream impacts due to a large uncontrolled release through the gated spillway. If the flows are large enough, downstream dams and levees could be overtopped.

3.0 HUMAN FACTORS DISCUSSIONS

Human decisions, actions and inactions and the interaction of human and physical factors play an important role in the overall system performance and can influence the ultimate outcome. Human factors are considered in general accordance with the framework outlined in Appendix 17-A.

After system interactions have been mapped, the team can brainstorm factors that could contribute to the potential for failure, such as pressure from non-safety goals, human fallibility and limitations, and system complexity, and discuss human errors that could result from these factors. Categories of human errors include slips, lapses, mistakes and violations. Situations and context which could lead to those errors should be explored and documented. This should be done at a global or system level and then at an individual structure level. The discussions will invariably address both factors specific to the project, but also touch on broader organizational issues.

After the initial system evaluation process, team members can, through a facilitated process, provide individual qualitative assessments to indicate their view of importance of the more likely/less likely factors. The factors within the system wide category can be organized into subcategories and the number of points within each category summarized. Typical categories might include:

- normalization of deviance,
- impacts of a large-scale regional incident,
- reservoir operation decision-making,
- general information gathering,
- communication and decision-making,
- preparedness and resource availability,
- decisions related to maintenance,
- human error in operations, and

- others.

At this point, the list of human factors discussed can be organized into groupings of similar factors. After each factor is evaluated for a strength and a vulnerability, risk mitigation strategies for each of the most critical groupings and factors can be identified by the team.

4.0 SYSTEM RELATED POTENTIAL FAILURE MODES

Identified and evaluated system-related potential failure modes should be described, evaluated, screened, and documented similar to how other non-system potential failure modes are and as described in this chapter.

5.0 REFERENCES

Halpin, E., D. Boyer, D. Osmun, E. Sossenkina, "Evaluating Complex Systems as Part of a Semi-Quantitative Risk Assessment," USSD Annual Meeting and Conference, 2021.

Independent Forensic Team Report, Appendix F3, January 2018 Oroville Dam Spillway Incident, California Department of Water Resources.

US Bureau of Reclamation and US Army Corps of Engineers, Best Practices in Risk Analysis for Dams and Levees, Denver, CO.

APPENDIX 17-D: LIST OF COMMON POTENTIAL FAILURE MODES

NOTE: ***This list is not meant to represent a comprehensive list of all the ways a dam or appurtenant structure could fail. Each project is unique and requires a separate, detailed review of the project records and an understanding of the project operation and performance in order to identify appropriate potential failure modes for that particular project. The information presented in this appendix should only be used to stimulate thought and discussion after the completion of the brainstorming session and should not be copied verbatim into PFM titles, descriptions, etc.***

Embankment Dams

<u>Normal/Static Loading</u>

Backward erosion piping (BEP)
- Piping of embankment materials
- Piping of embankment materials into the foundation
- Piping, blowout and heave of foundation materials
- Piping of materials into drains/conduits

Concentrated leak erosion (CLE)
- Through cracks/defects in core
- Along contact with concrete structures
- Along conduits/penetrations
- Along bedrock contact

Contact erosion
- Erosion of fine particles from flow in an adjacent coarse layer within the foundation
- Erosion of fine particles from flow in an adjacent coarse layer between the embankment and the foundation

Suffusion (Internal instability)
- Erosion of fine matrix materials in a well graded or gap graded material in the embankment
- Erosion of fine matrix materials in a well graded or gap graded material in the foundation

Static slope instability of embankment
Static slope instability of foundation/abutments
Slope instability under rapid drawdown

Wave erosion of upstream slope
Runoff erosion/gullying of downstream slope

Landslide-induced wave leading to overtopping and erosion
Volcanic flow/air fall displacing reservoir contents leading to overtopping and erosion

Hydrologic/Flood Loading

Normal/Static Loading PFMs with added hydrologic loads

Internal erosion of embankment above core

Embankment overtopping and erosion
Embankment overtopping and erosion with wind and wave run up
Abutment outflanking and erosion
Structural failure/erosion of parapet wall foundation

Seismic/Earthquake Loading

Normal/Static Loading PFMs with added seismic loads

Liquefaction of embankment soils leading to overtopping and erosion
Liquefaction of foundation soils leading to overtopping and erosion
Deformation of embankment/foundation soils leading to overtopping and erosion
Deformation of embankment/foundation soils leading to cracking of the embankment and internal erosion

Fault offset in foundation leads to cracking and internal erosion
Seiche wave overtops embankment leading to erosion

Concrete-faced Rockfill Dam

Deformation and cracking of facing slab leads to internal erosion of embankment materials
Downstream slope failure resulting from piping of fine portion of "dirty" rockfill resulting in sinkhole development.
Failure of facing slab waterstops leads to internal erosion of embankment materials
Sliding instability of concrete plinth

(See Embankment Dam PFMs for additional PFMs)

Concrete Gravity and Arch Dams

Normal/Static and Hydrologic/Flood Loading

Concentrated leak erosion along foundation contact

Internal erosion through foundation/abutment materials

Static sliding instability along lift joints/base
Static sliding instability through foundation/abutments
Sliding instability due to abnormal loads (silt and ice)

AAR/ASR leads to cracking of dam and loss of strength
Freeze/thaw deterioration leads to loss of section and overstressing of concrete

Overtopping leading to erosion of abutment/foundation materials
Overtopping of dam crest creates negative pressures and induces vibrations that lead to cracking and failure

Landslide-induced wave leading to overtopping and erosion

Seismic/Earthquake Loading

Normal/Static and Hydrologic/Flood Loading PFMs with added seismic loads

Fault offset in foundation leads to cracking of dam/erosion of foundation materials

Concrete Buttress Dams

Sliding instability of buttress at contact
Sliding instability of buttress through the foundation
Deterioration of buttresses (freeze-thaw, ASR/AAR, corrosion of reinforcement) leads to structural collapse

Overstressing of upstream slab due to excessive loading (e.g., flood surcharge)

Seismic instability and loss of lateral support of buttresses in cross canyon direction

Fault offset in foundation leads to cracking of dam/erosion of foundation materials

Spillway Structures

Normal/Static and Hydrologic/Flood Loading

Erosion/scour of soil/rock channels

Concentrated leak erosion along foundation contact
Internal erosion of spillway wall backfill
Internal erosion through foundation materials

Static sliding stability of crest structure along base
Static sliding stability of crest structure through foundation
Global sliding stability of spillway structure
Overturning of crest structure

Stagnation pressure causes jacking of spillway chute slab that leads to erosion
Uplift of spillway chute slabs/inadequate anchoring causes jacking of slab that leads to erosion
Stagnation pressure causes loss of material below chute slab, collapse of slab, and erosion
Overtopping of spillway chute/basin walls leads to erosion
Cavitation damage induced failure leads to erosion
Erosion and failure of stilling basin
Uplift and sliding of stilling basin

Debris plugging of approach channel/crest structure leading to overtopping and erosion

Seismic/Earthquake Loading

Seismic failure of pier(s)
Seismic failure of spillway walls
Seismic failure of spillway bridge
Foundation liquefaction/deformation of spillway

Outlet Works

Debris plugging/landslide at intake leads to inability to release flood waters and premature overtopping and erosion
Cavitation of outlet pipe leads to erosion and uncontrolled release of reservoir
Coating damage/corrosion of outlet pipe leads to erosion and uncontrolled release of reservoir
Rockfall/lining damage in gate chamber/downstream tunnel damages outlet pipe/control gates and leads to erosion and uncontrolled release of reservoir
Seismic failure of outlet tower leads to inability to close outlet gates and leads to uncontrolled release of the reservoir

Gates (spillway and outlet works) and Stoplogs

Structural failure of gate (applies to members and connections)
    (Trunnion friction; corrosion; fatigue; excess demand such as hydrologic or seismic loading or impact from debris/barges/etc.)
Inability to operate gates due to:
    Loss of power (electrical supply, transmission)

Failure or inoperability of mechanical components (failure of winches, hoists, hydraulics, chains, ropes, etc.; failure of platforms atop which any of the aforementioned equipment rests; etc.)
Binding within piers or gate slots (e.g., accumulation of ice along seals, expansion of concrete due to AAR/ASR, lateral deflection caused by a seismic event, etc.)
Loss of access to dam/gates

Slope instability/rockfall damages gates/spillway structure

Operational/procedural errors, SCADA errors, and human error

Flashboards

Flashboards trigger before intended (e.g., at a lower pool elevation), resulting in unexpected high flows, due to excessive loading (e.g., seismic, ice, etc.) or degradation

Flashboards do not trigger when intended, with a reduced discharge/increased pool elevation and resulting effects on other project components (e.g., overtopping), due to:

Overdesign of intended-to-fail components (e.g., diameter or strength exceeding specifications)
Unauthorized modification of flashboards, including the installation of redundant restraining mechanisms (e.g., securing trippable components with ropes, chains, etc.)

Penstocks

Slope creep/landslide displaces penstock leading to rupture and uncontrolled release

Leakage from penstock saturates foundation materials, leading to loss of support, rupture, and uncontrolled release

Cavitation damage causes loss of section, overstressing and rupture of penstock, and uncontrolled release of reservoir

Coating damage/corrosion causes loss of section, overstressing and rupture of penstock, and uncontrolled release of reservoir

Rockfall or other debris impact ruptures penstock and leads to uncontrolled release of reservoir

Seismic failure of penstock supports leads to uncontrolled release of reservoir

Rapid closure of gate/valve causes excessive transient pressure (water hammer), overstressing and rupture of penstock, and uncontrolled release of reservoir

Rapid closure of intake or obstruction of air vents causes a vacuum, collapse of penstock, and loss of discharge capacity and/or uncontrolled release of reservoir

Page intentionally left blank

APPENDIX 17-E: ADDITIONAL CONSIDERATIONS IN IDENTIFYING POTENTIAL FAILURE MODES

A list of issues related to potential failure modes that have been identified in some past PFMAs is provided below (adapted from *Bureau of Reclamation, Comprehensive Review Guidelines, Section XVII – Potential Failure Modes and Risk Analysis, 2016*). It is not an exhaustive list, nor have the descriptions been fleshed out to the extent needed for complete documentation. This must be done on a case-by-case basis. However, the list provides some ideas to consider in helping to identify potential pathways and contributing factors that could lead to identifying and developing a PFM.

Overtopping Considerations

- Discharge capacity is reduced during flooding by flows that take out power plant transformers (eliminating the ability to generate and discharge through the units), power supplies to gates, or access to open gates, leading to premature overtopping.
- High tailwater floods the power plant and leads to loss of release capacity through the units, resulting in premature overtopping.
- Loss of power or communications due to lightning, earthquake shaking, or other causes leads to gate misoperation, and overtopping or life-threatening downstream releases.
- Binding of gates (possibly due to ASR concrete expansion) or mechanical failure can lead to inability to open gates and premature overtopping.
- Spillway discharge capacity is reduced when the reservoir rises to levels not envisioned in the original design and impinges on the bottom of open gates, transitioning from free flow to orifice flow, leading to premature overtopping.
- Faulty instrumentation could indicate reservoir levels and flows are within normal ranges, but dangerous inflows, outflows, or water levels are developing.
- Overtopping of concrete dams may be acceptable; however, the quality of the rock on which the flows impinge must be evaluated.
- Careful attention must be paid to the flood routings. In some cases the dam crest may be lower than assumed or shown on the drawings, crest elevations may vary between reservoir impounding structures, or the elevation of a single structure may vary (for example due to camber), creating a flow concentration possibility.
- A “fuse plug” may be relied on for flood routings that indicate the dam will not be overtopped. In such cases, the design and construction of the fuse plug should be reviewed to ensure it will perform as intended.

- Some reservoirs produce debris during flood events that could plug spillway gates and lead to premature overtopping. Log booms may or may not be able to sustain the debris load; they should be evaluated also.
- Spillways can fail to perform as anticipated due to overtopping of spillway walls, jacking of chute slabs due to "stagnation" pressures, cavitation, or erosion of deteriorated materials. The resulting erosion can headcut upstream and breach the reservoir. Defensive measures for these scenarios should be reviewed.

Stability Considerations

- In some cases, no engineering geology or rock mechanics evaluation has been performed for a concrete dam, and the rock is pronounced to be "good" due to its hardness, even though adversely oriented joints, faults, shears, foliation planes, or bedding planes can be observed in construction photos and downstream of the dam. Foundation instability could occur under a change in loading conditions.
- Two-dimensional analyses can sometimes indicate a potential problem when three-dimensional effects will result in a stable condition (for example, a narrow concrete gravity section wedged between a solid rock wall and massive spillway section, with a keyed joint).

Seismic Considerations

- Large spillway gates could release life-threatening flows, if they failed under normal operating conditions. Buckling of radial gate arms under operation (pin friction) or seismic loading may be an important consideration. Deterioration due to lack of maintenance can be a contributing factor.
- Spillway piers are designed to carry loads in the upstream-downstream direction; cross canyon seismic loading could produce high moments about the weak axis. Moment failure of a pier could result in the loss of two adjacent gates.
- Liquefaction of loose foundation or embankment soils can lead to deformation and loss of freeboard, perhaps leading to overtopping, or otherwise possibly leading to cracking and subsequent seepage erosion through the cracks.
- Seismic soil-structure interaction between an embankment and spillway wall can lead to wall failure or separation at the contact and seepage erosion through the gap.
- "Kinks" or changes in slope on a concrete gravity dam can lead to stress concentrations during seismic loading, cracking through the structure, and sliding failure. Post-earthquake analyses are helpful in evaluating this condition.
- Shake table model studies on concrete arch dams indicate the most likely seismic failure mode is horizontal cracking near the center of the structure, diagonal

cracking parallel to the abutments, and rotation of concrete blocks isolated by the "semi-circular" cracking downstream.

- Large landslides may fail quickly into a reservoir creating a wave that overtops and erodes the dam. Landslides can create a debris dam in a canyon downstream of a dam that will subsequently overtop due to dam releases and send a life-threatening wall of water downstream. Landslides can also disrupt the abutment of a dam, leading to cracking and internal erosion (in the case of an embankment dam), or abutment instability and structural distress (in the case of a concrete dam).
- Fault offset within the foundation of an embankment dam can lead to cracking and internal erosion, or in the case of a concrete dam cracking and structural distress.

Operational Considerations

In recent years, several dam failures have been attributed to operational failures, such as the failure of Taum Sauk Dam in Missouri in 2005. These can result from equipment, instrumentation, control systems (including both hardware and software), or processes failing to do what they were intended to do. This, in turn, can lead to uncontrolled reservoir release or inability to get people out of harm's way. Examples of these types of failure modes include (with some repetition of the above list for emphasis):

- Failure of a log boom allows reservoir debris to drift into and plug the spillway, resulting in premature overtopping of the dam.
- Gates fail to operate as intended resulting in premature overtopping of the dam. This could result from mechanical or electrical failure, control system failure, or failure of the decision process for opening the gates.
- Gates open inadvertently sending life-threatening uncontrolled releases downstream. This could result from control system failure, operator error, or in the case of drum gates (which drop to release the reservoir), mechanical failure. Position sensors or limit switches could fail, resulting in gate openings greater than intended.
- Loss of access to operate key equipment during a flood leads to overtopping of the dam or other uncontrolled releases.
- Loss of release capacity leads to overtopping of the dam. For example, if releases through the power plant are a major component of the release capacity and the switchyard is taken out during a flood or earthquake, that release capacity will be lost.
- Mechanical equipment failure due to changes in operation without a corresponding change in maintenance. For example, if river re-operation requires frequent gate opening to enhance fisheries without a corresponding increase in the frequency of

gate lubrication, component failure could occur when the gate is needed to pass a flood, but cannot be opened resulting in premature dam overtopping.

- Overfilling off-stream storage leads to overtopping and failure of the dam. This could happen due to faulty instrumentation, control system issues, or operator error.
- The SOP operating rule curves require operating gates that will flood out people downstream; there may be a reluctance to open the gates resulting in a delay and increased chance for overtopping the dam.
- In the case of remote operations, communications are lost along with the ability to operate the gates as needed during flooding, leading to premature overtopping; or a loss of communications leads to inadvertent opening of gates and premature releases of life-threatening flows.

Internal Erosion Considerations

Internal erosion failure modes can be quite varied. Certain conditions make an embankment more susceptible to these potential failure modes.

- Seepage occurring from an unprotected/unfiltered exit could lead to internal erosion through the dam or foundation. In some cases the flows may be measured by flumes, which cannot trap and detect sediments in the seepage flow. In other cases, seepage, if occurring, cannot be observed due to vegetation, tailwater, or an unfiltered blanket at the toe that dried up the area.
- The rock foundation beneath the core of an embankment dam contains open joints that were not treated with slush grout or dental concrete, leading to the possibility of internal erosion of the embankment into the foundation. A similar concern exists if the embankment core material was placed directly against foundation soils that may not be filter compatible.
- In some cases, incidents related to internal erosion and sinkholes have developed in the past, but are buried in the archives. A careful review could identify significant potential internal erosion paths.
- Internal erosion of material into under-drain systems can leave a void adjacent to or beneath a conduit or structure. This provides an unfiltered exit (into the void) closer to the reservoir than would otherwise exist and increases the average gradient. This can be especially problematic in low plasticity soils.
- Internal erosion of material from beneath concrete dams founded on alluvial soils can lead to a rapid draining of the reservoir beneath the dam and life-threatening downstream flows.

The following conditions may lead to an increased likelihood of a flaw existing through the dam (including considerations for conduits through the dam):

- Wide benches or “stair steps” in the upper to middle portion of the abutment profile can lead to transverse cracking from differential settlement.
- Steep abutments near the top of the dam can also lead to transverse cracking from differential settlement.
- Very steep abutments and a narrow valley can lead to “arching” of the soil across the valley leading to a reduction in vertical confining stress within the dam and increased potential for cracking due to hydraulic fracturing (i.e. pore pressures exceed confining stress).
- Differential settlement between the shell and the core (if deformability of the materials differ) can lead to “dragging and transverse shearing” of the core. However, more typically, this type of differential settlement leads to longitudinal cracks at the interface between the two materials.
- Different foundation conditions (deformability) across the profile can lead to differential settlement and cracking of the dam core.
- Low-density fine-grained loess soils or weakly cemented “desert” soils present within the foundation may collapse upon wetting, leading to differential settlement or hydraulic fracturing through the low density material, and transverse cracking through the embankment.
- Desiccation of the embankment material can lead to transverse cracking through the upper part of the core.
- Excessive settlements as a percentage of the dam height (i.e. more than about 4 percent during construction or about 1 percent at 10 years post-construction) increases the chances of transverse cracking.
- An irregular foundation contact surface, possibly with overhanging rock features, or sloppy or loose foundation soil conditions upon embankment placement can lead to inadequate compaction and a pervious channel along the dam-foundation contact.
- Poor core density due to lack of formal compaction, lack of compaction control, or excessively thick compacted layers can result in pervious layers through the core.
- Seasonal shut-downs or placement in freezing weather can lead to a pervious layer through the core if not properly treated (i.e. frozen material and desiccation cracking was not removed and the surface thoroughly scarified with good moisture control upon re-compaction). In the event that post-shutdown construction results in lower modulus material in comparison to the underlying embankment, differential settlement of the overlying embankment can lead to transverse cracking in that portion.

- The presence of a conduit through the core of a dam creates a potential high permeability pathway due to the potential for inadequate density or compaction, especially if one or more of the following conditions are also present:
    - A round conduit with no concrete encasement where it is difficult to get good compaction on the under-side.
    - The presence of seepage cutoff collars which are difficult to get good compaction around and against.
    - Cracks or open joints in the conduit, or corrugated metal pipe which is subject to corrosion deterioration and through-going holes, into which embankment core material can be washed.
    - Steep and narrow trench into which the conduit was placed, which makes compaction difficult and creates the potential for arching of soil across the trench, leaving a low density zone susceptible to hydraulic fracturing.
- If a spillway passes through the embankment such that the core is compacted against the spillway wall, difficulties in compacting against the wall (especially if vertical or counterforted), and settlement away from the wall parallel to the abutment, can potentially lead to a high permeability zone or small gap adjacent to the wall.
- For composite concrete/embankment dams, vertical faces, overhangs, and changes in slopes of the concrete section (against which the embankment core is compacted) can lead to higher permeability seepage paths, especially if post-construction embankment settlements are large.
- Direct observations such as observed transverse cracks in the crest of the dam, or concentrated seepage, or wet areas on the downstream face of the dam adjacent to an outlet works conduit or spillway wall, could be indications that flaw may extend through the dam.
- Evidence of sinkholes or depressions (especially along the alignment of a penetrating outlet works conduit) could be indications that material has moved by means of seepage flows.

The following conditions may indicate an increased likelihood of internal erosion <u>through the foundation, or from the embankment into the foundation</u>:

- A low permeability confining layer at the toe of the dam beneath which high artesian pressures exist, which increases the chance of blowout.
- Sand boils observed in the channel downstream of the dam which could be indications of material movement associated with a foundation seepage path, especially if material is moving out away from the boils.

- Open joints, seams, faults, shears, bedding planes, solution features, or other discontinuities in the rock foundation at the contact with the dam core into which core material can erode, especially if the following also apply:
    - There was no or questionable foundation surface treatment performed during construction in the way of dental concrete or slush grout.
    - The effectiveness of foundation grouting is questionable due to grout holes being parallel to open discontinuities, use of thin grout mixes, widely-spaced holes with uncertain closure, uncaulked surface leaks during grouting, and/or little pore-pressure drop across the grout curtain as measured by piezometers.
    - The discontinuities are open, or perhaps filled with erodible silty or sandy material. Wider discontinuities are more problematic than narrow ones.
    - The discontinuities trend upstream to downstream across the foundation, providing a pathway for reservoir seepage.
- Poor clean-up at the core-foundation rock surface can lead to a low density or erodible pathway at the contact.
- Ridges and valleys formed by excavation along geologic features (e.g. tilted bedding planes forming an irregular surface) that trend upstream to downstream, into which compaction is difficult, can lead to low density pathways near the dam-rock contact.
- Embankment core material placed against the downstream slope of a cutoff trench cut into pervious gravels with no intervening filter leaves an interface through which core material can be eroded.
- A narrow steep-walled cutoff trench forms a location where arching of core material placed into the trench can lead to a low density zone in the core susceptible to transverse hydraulic fracturing. This can be problematic if there is a pathway downstream through which the core material can erode.
- Highly permeable foundation materials exist which can transmit significant flow capable of eroding material at the base of the dam and carrying it downstream.

Page intentionally left blank

APPENDIX 17-F: EXAMPLE CONSIDERATIONS IN DESCRIBING POTENTIAL FAILURE MODES

The following are some brief examples of some considerations in developing and describing potential failure modes. The examples are intended to illustrate the kinds of engineering evaluation and judgment needed to properly identify and develop potential failure modes.

Operational Related Potential Failure Mode

The design flood was routed through Dam A by a hydrologic engineering consulting firm using the traditional means and assumptions and the capacities for the facilities provided by the owner. The dam was found to pass a sizeable portion of the probable maximum flood using the main spillway gates and the emergency spillways, thus there was concern for the hydrologic deficiency but not great concern. However, examination at the site for potential failure modes revealed a significant potential for an overtopping failure mode due to the following factors:

- The emergency spillway bays were fronted by arch rings designed to be blasted away if the emergency spillway was needed. Discussions with the owner revealed that use of the emergency spillway in such a manner was highly improbable. This was due to the potential liability from such an action (a sizeable town is located just a mile or so downstream) and also due to the physical arrangement of the dynamite ports on the top of the spillway bays (it was likely that these would be underwater by the time a decision to use them was made). Further there were no plans or procedures in place to do the blasting.
- The first location for overtopping of the structure was immediately above the transformer yard. Overflow at this location would have resulted in loss of capability to pass flow through the turbines and while this flow was not relied on in the routing, the early shut off would have exacerbated the overtopping situation.
- Drawings were located for the emergency spillway, which was referred to as a "fuse plug" spillway but this fuse plug actually had to be excavated by a dozer before it was functional. Operators at the site did not know the location of the spillway limits and had no procedures or equipment to initiate this spillway.
- Design crest elevations indicated that the concrete structures would be overtopped prior to the embankment structures. However, examination of survey data, settlement records and settlement projections (along with the physical location of the monuments relative to the crests) revealed that the low point for the project was currently an earthen saddle dam.

Internal Erosion Related Potential Failure Mode

The following potential failure mode was highlighted because the specific conditions at Dikes 1 and 2 are such that this potential failure mode is physically possible and is one of the most significant potential failure modes definable at this site. Failure of the dikes poses a high hazard, and diligence in monitoring for development of this potential failure mode is warranted.

Potential Failure Mode 1 - Dikes 1 and 2 – Internal Erosion

During site investigation the foundation of these dikes was found to contain joints much more open than anticipated based on pre-construction investigations. These joints provide a potential path for subsurface erosion of the Zone 1 material leading to an unprotected exit downstream of the dam. Although grouting was performed following construction (during the first filling of the reservoir) and the seepage levels were reduced, the fundamental potential failure mode remains). The presence of 4 to 5 ft^3/s of seepage, which occurred during first filling, from a dike of moderate height and length attests to the possibility of open joints in the foundation capable of carrying adequate flow to result in erosion, and transport of eroded material downstream. The specific potential failure mode paths and the factors relative to the likelihood for the development of this potential failure mode are as follows:

Potential failure mode paths - there are two primary potential paths for internal erosion to take place through the foundation jointing and two of lesser likelihood. These are:

- Flow through the dike embankment across the Zone 1/foundation interface. This could result in the Zone 1 materials eroding and being carried through the open joints to an unprotected exit downstream. (Failure would result if internal erosion through the Zone 1 materials reached the reservoir source. An ever-increasing flow potential could then progressively enlarge the flow channel downstream of the point of erosion initiation in the core to an extent large enough to carry continually increasing flows).
- Flow under the foundation attacking the base of the Zone 1 material and removing it by seepage erosion through the foundation jointing

The other two potential flow paths leading to an internal erosion failure are (1) internal erosion of the Zone 1 through the foundation alluvium, and (2) seepage erosion of the foundation alluvium exiting through the open joints in the rock. These are considered to be of significantly lesser likelihood.

APPENDIX 17-G: PFM TEMPLATE

Dam Name		
PFM Information		
Structure		
Loading Condition		
PFM Failure Type		
Location(s)		
PFM Source		
PFM Source Date		
PFM Description		
PFM No.		
PFM Title		
PFM Description	(include flaw/initiation, continuation, progression, intervention, and failure)	
PFM Classification	☐ Ruled Out ☐ Clearly Negligible ☐ Insufficient Info ☐ Asset Management ☐ Financial/Damage State ☐ Credible ☐ Urgent Credible	
Classification Justification		
PFM Sketch(s)		
Additional Supporting Information (if needed)		
Performance Monitoring Information		
Evaluation Factors		
Step/Node	Adverse (More Likely)	Favorable (Less Likely)
Flaw/Initiation		
Continuation		

Progression		
Intervention		
Failure/Breach		

Consequences	
Life Safety Consequences	
Consequence Description	
Other Consequences	
Consequence Description	
Potential Interim Risk Reduction Measures/ Potential Dam Safety Management Actions	
Potential Risk Reduction Measures	
Inspections and Actions	
Surveillance and Monitoring	
EAP	
Follow up Studies	
Others	
Other Notes/Comments	

APPENDIX 17-H: EXAMPLES OF CLEARLY NEGLIGIBLE POTENTIAL FAILURE MODES

The following sections provide examples of potential failure modes that were considered clearly negligible and were excluded from further consideration because they were deemed so remote to be considered non-credible (adapted from *USACE Periodic Assessment Guidance, Appendix A Excluded Potential Failure Modes, 2014*).

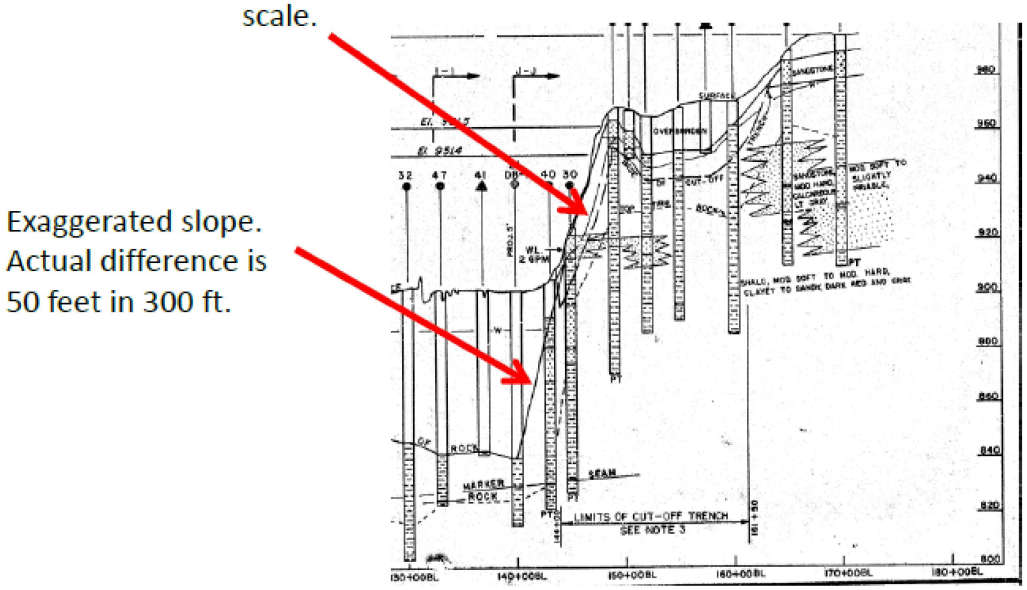
1. Examples of Embankment Potential Failure Modes due to Transverse Cracking

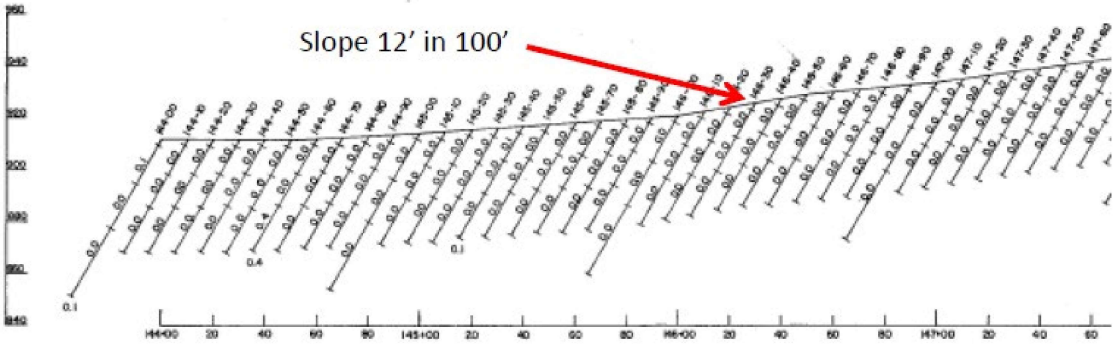
PFM ##: Concentrated leak erosion (scour) in a transverse crack in the embankment near station 587+00

There is an approximately substantial rise in the bedrock surface over about 400 feet in the vicinity of Sta. 580+00 that appears very steep on the section drawn along centerline but the scale on this drawing is very exaggerated. This corresponds to an average angle of about 7.5 degrees from horizontal which is considered to be a relatively gentle slope. See the figures below for more explanation. Therefore, the likelihood of transverse cracking in the embankment due to differential settlement due to a steep abutment profile is considered remote.

Note that this slope which appears steep was a gentle slope in cutoff trench (12' in 100'). See figure below for slope drawn to scale.

Exaggerated slope. Actual difference is 50 feet in 300 ft.





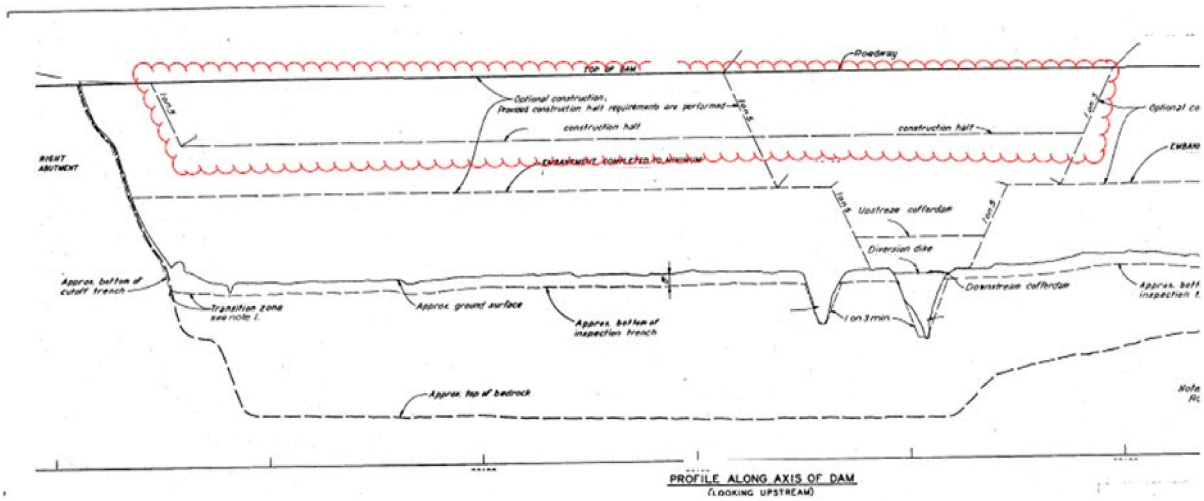
PFM ##: Concentrated leak erosion (scour) in the embankment due to desiccation cracking at the crest

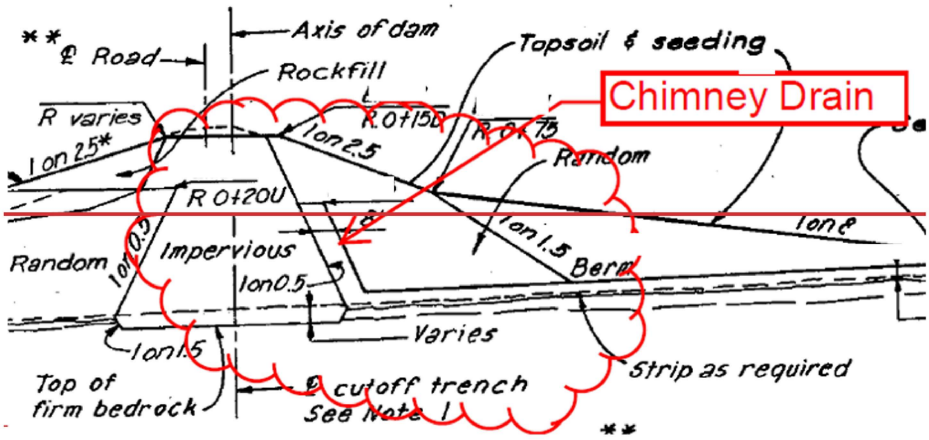
No cracking has been observed in the paved crest. A 20-foot-deep crack would extend to el. 1694 ft NGVD, which corresponds to a reservoir level with an ACE of about 1/2,000. The top of the impervious fill (core) is at el. 1707 ft NGVD. The impervious core is overlain by about 5 feet of random fill which is overlain by a pavement section containing 24 inches of select fill and 6 inches of aggregate base and double-bituminous surfacing. The average liquid limits of the impervious and random fills are about 38 and 31, respectively, which are not susceptible to desiccation cracking.

2. Examples of Embankment Potential Failure Modes due to Staged Construction Interfaces

PFM ##: Concentrated leak erosion (scour) at a staged construction interface (construction halt at el. 3300 ft NGVD)

A 6-month construction halt was enforced when the embankment placement reached el. 3300 ft NGVD. Construction documentation indicates good construction practices and adequate quality control for subgrade preparation prior to fill resumption of fill placement. The likelihood of a continuous, upstream to downstream poor lift bond, disturbed zone, or poorly compacted zone is remote. A 8-foot-thick, inclined pervious drain (filter) extends up to el. 3303 ft NGVD and provides defensive measures against this potential failure mode.





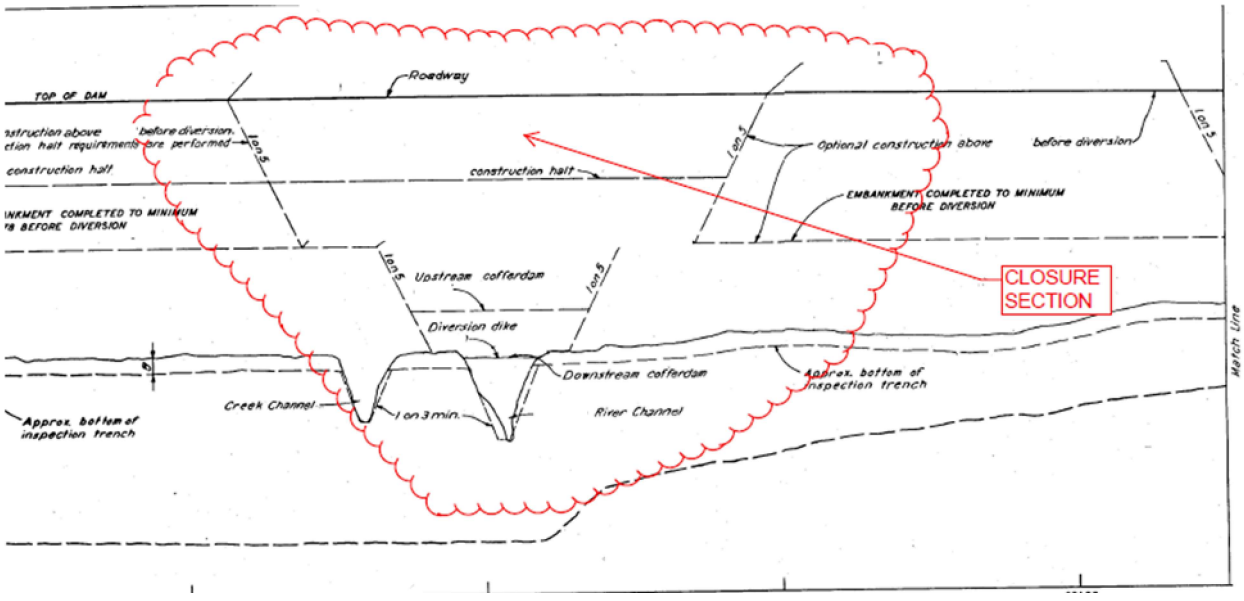
PFM ##: Concentrated leak erosion (scour) at a staged construction interface (unscheduled construction halt at el. 1512 ft NGVD)

A construction halt was ordered when the embankment placement reached el. 1512 ft NGVD due to increasing pore pressures in the lower embankment. Construction

documentation indicates good construction practices and adequate quality control for subgrade preparation prior to fill placement. The likelihood of a continuous, upstream to downstream poor lift bond, disturbed zone, or poorly compacted zone is remote. An unfiltered exit exists at the elevation of the unscheduled construction halt because the top of the inclined pervious drain (filter) is el. 1503 ft NGVD. Since a large flood with an estimated annual chance exceedance less than about 1/18,000 is required to reach the elevation of the unscheduled construction halt and the likelihood of a continuous flaw/defect is remote, this potential failure mode is considered clearly negligible and was excluded from further consideration.

PFM ##: Concentrated leak erosion (scour) at the river closure section (crest stations 1+40 to 9+60)

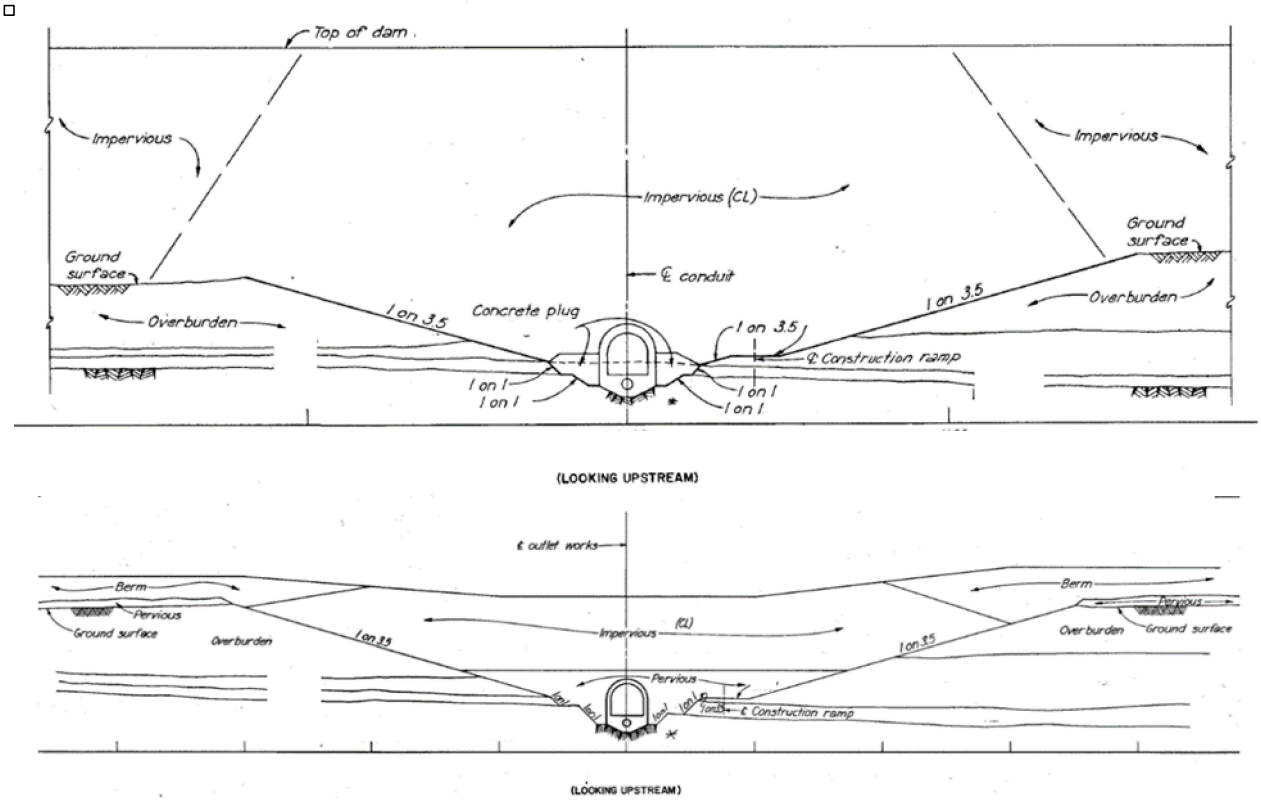
The embankment slopes of the initial phase at the river closure section were 5H:1V. Construction documentation indicates good construction practices and adequate quality control for subgrade preparation prior to fill placement. The likelihood of a continuous, upstream to downstream poor lift bond, disturbed zone, or poorly compacted zone is remote. A 10-foot-thick, inclined pervious drain (filter) provides defensive measures against this potential failure mode below to el. 1503 ft NGVD. The closure section interface daylights on the downstream slope, and no evidence of seepage, leakage, or settlement has been observed in this area.



3. Examples of Embankment Potential Failure Modes Related to a Buried Conduit

PFM ##: Concentrated leak erosion (scour) in the embankment adjacent to the conduit due to poor compaction

The conduit is founded on moderately hard interbedded shale and sandstone. A series of concrete collars are located at the monolith joints upstream of the dam centerline. Defensive measures against internal erosion in the embankment adjacent to the conduit consist of a lean concrete plug placed along conduit between stations 9+47 to 10+74 (dam centerline at station 10+00) and pervious (filter) materials surrounding the conduit from the lean concrete plug to the downstream toe. The lean concrete plug was placed to the top of the Simpson Sandstone (about el. 325 to 330 ft NGVD), and the top of the pervious fill surrounding the conduit is at el. 344 ft NGVD. Therefore, the likelihood of a continuous flaw/defect in the embankment with an unfiltered exit is remote.



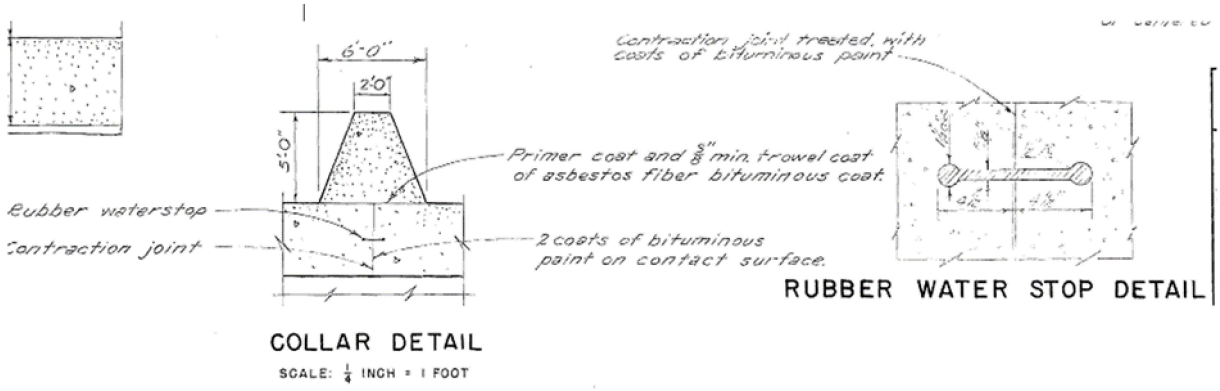
PFM ##: Concentrated leak erosion (scour) in the embankment adjacent to the conduit

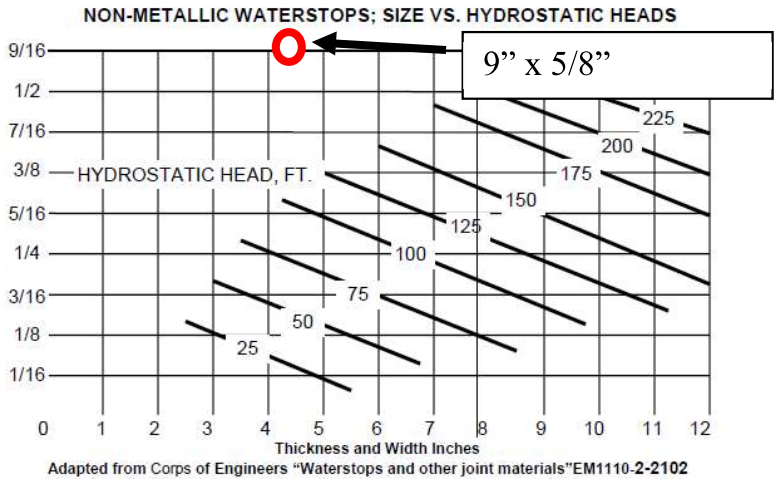
A 6-foot-wide chimney filter is located 20 feet downstream of the axis that extends up to normal pool of el. 1251.1 feet. A 6-foot-thick blanket filter/drain extends from the chimney to filter-compatible bedding material at the embankment's downstream toe alongside the stilling basin. The width of the base of the excavation adjacent to the conduit was a minimum of 6 feet. The firm rock in which the excavation was made was sloped at 1H:2V, and the overlying weathered rock materials were sloped at 1H:1V.

Concrete seep rings are located upstream of the dam centerline (Sta. 190+00) at Sta. 12+37 and 12+93. The details of the filter and general design layout appear to provide adequate defense against this potential failure mode.

PFM ##: Concentrated leak erosion (scour) of the embankment into an open defect in the conduit

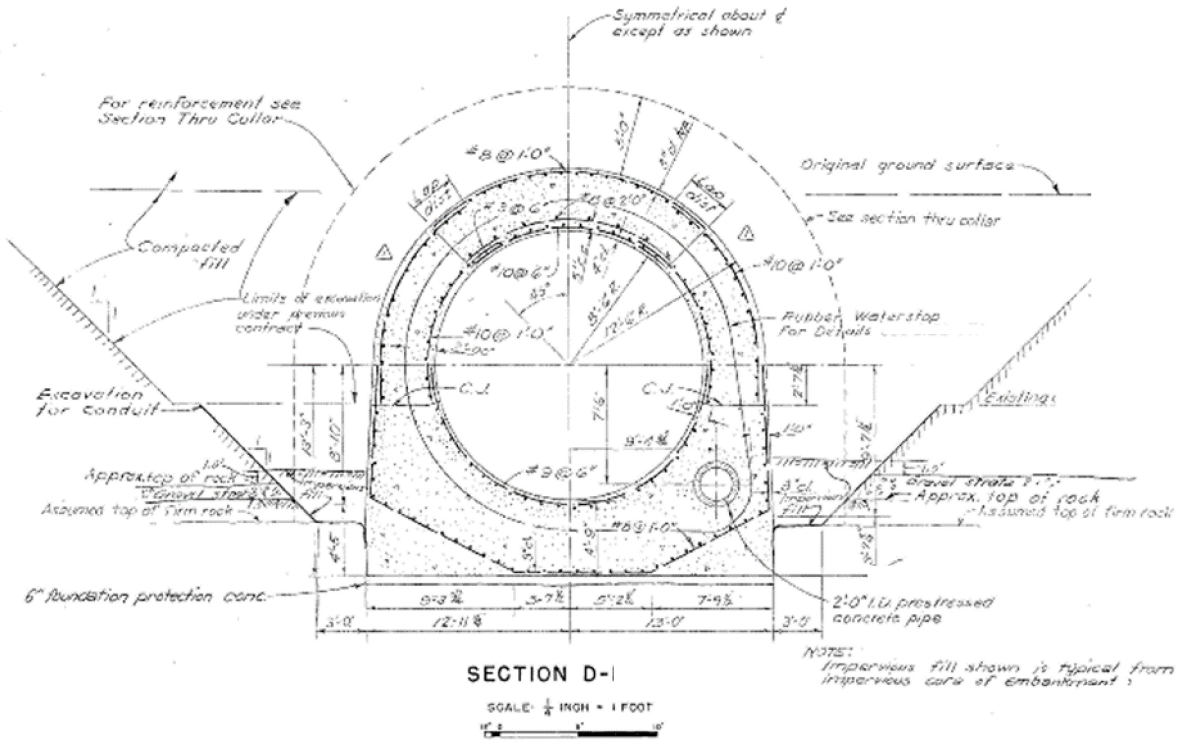
There are no known joint openings in the conduit. A recent inspection report (2006) indicated that there are only leaks near the ends of the conduit where the conduit joins adjacent structures (the intake tower and the stilling basin training walls). These leaks are clear and calcified. The conduit is founded on rock which was protected during construction by a 6-inch-thick concrete protection layer. The conduit does not exhibit any signs of settlement which would allow joints to open. There are 5/8-inch-thick dumbbell waterstops present at each monolith joint as shown below. The 5/8-inch-thick waterstops are capable of withstanding over 200 feet of hydrostatic head as shown below. The head difference on the conduit at the PMF is approximately 63 feet: PMF of el. 1420 ft NGVD minus el. 1357 ft NGVD at the base of the conduit. Therefore, this potential failure mode is considered so remote as to be considered clearly negligible and was excluded from further consideration.





PFM ##: Concentrated leak erosion (scour) of the embankment adjacent to the conduit due to leakage out of a joint resulting from pressurized conduit flow

There are no known joint openings in the conduit. The latest inspection indicates that there are only leaks near the ends of the conduit where the conduit joints adjacent structures (the intake tower and the stilling basin training walls). These leaks are clear and calcified. There are 5/8-thick-thick dumbbell waterstops present at each monolith joint. The 5/8-inch-thick waterstops are capable of withstanding over 200 feet of head as shown above for PFM XX. Tailwater would not be high enough to create pressurized flow in the conduit until flows exceed el. 1411 ft NGVD (an ACE of 1/300) occurred. The conduit would be pressurized for approximately 2 days for the PMF (el. 1420 ft NGVD) event under normal operations. The conduit is 4 feet thick with two layers of reinforcement as shown below. The likelihood of an open defect in the conduit in conjunction with sufficient, sustained pressurized flow to initiate erosion along the conduit is considered so remote.



PFM ##: Concentrated leak erosion (scour) of the embankment into/along the conduit at failed water stops

A 3-foot-wide filter is located 120 feet downstream of the axis that extends up to the normal pool of el. 1956 ft NGVD, or at least 40 feet above the top of the conduit. A 3-foot-thick filter/blanket drain extends to filter-compatible bedding material at the

embankment's downstream toe. During the site visit in August 1998 with the reservoir at el. 1954.32 feet, joint leakage was observed at the joint between Monoliths No. 11 and 12 and some locations upstream. This joint is located approximately 30 feet upstream of the impervious core and 150 feet upstream of the filter than surrounds the conduit. This historical photograph was taken from an older inspection report shows similar minor leakage from a defect further upstream. The filter/drain system appears well-designed and constructed to defend against defects in the core materials adjacent to the conduit.

Photo 21. The minor seepage at monolith joint 4-5 in the conduit appears unchanged.

4. Examples of Embankment Potential Failure Modes due to Slope Instability

PFM ##: Slope instability leading to crest deformation and overtopping erosion

The embankment side slopes are 2.5H:1V above about el. 1306 ft NGVD, while the slope of the berms flanking the impervious and random fill zones is 8H:1V. At the conduit section, the embankment is steeper at 5H:1V upstream and 6H:1V downstream. The steeped section near the conduit is short such that stress arching could be transmitted to the berm sections. Another consideration is that the conduit joints are tight, indicating little to no deep-seated lateral deformation has occurred since construction. Calculated factors of safety for sliding stability using conservative input parameters are over 3.5. Available freeboard during normal pool is 8.5 feet. The likelihood of slope instability with large crest deformations that would result in release of the reservoir is considered so remote as to be considered negligible. This potential failure mode was considered clearly negligible.

5. Examples of Embankment Potential Failure Modes due to an Earthquake

PFM ##: Overtopping due to crest deformation caused by earthquake

With the reservoir at normal pool of el. 351.1 ft NGVD, there is 20 feet of freeboard. Deformations on the order of 40 percent or more of the embankment height which would cause overtopping were judged to be remote. The embankment consists of a homogenous, well-compacted earth fill, and the core has an average liquid limit of 27 and was compacted on average to over 100 percent of the maximum dry density at a 0.8 percent above optimum moisture content. The alluvium in the foundation can be characterized as either CL, SM, or SC soils (i.e., high fines content), and field SPT N-values were typically greater than 15 bf. The dam has many defensive design measures to protect against failure in the event of earthquake shaking including ample freeboard to allow for settlement or slumping, wide-plastic core, chimney and blanket filter to lower pore pressures in the downstream slope, and very flat slopes with high static factors of safety against sliding.

PFM ##: Slope instability due to an earthquake leading to crest deformation and overtopping erosion

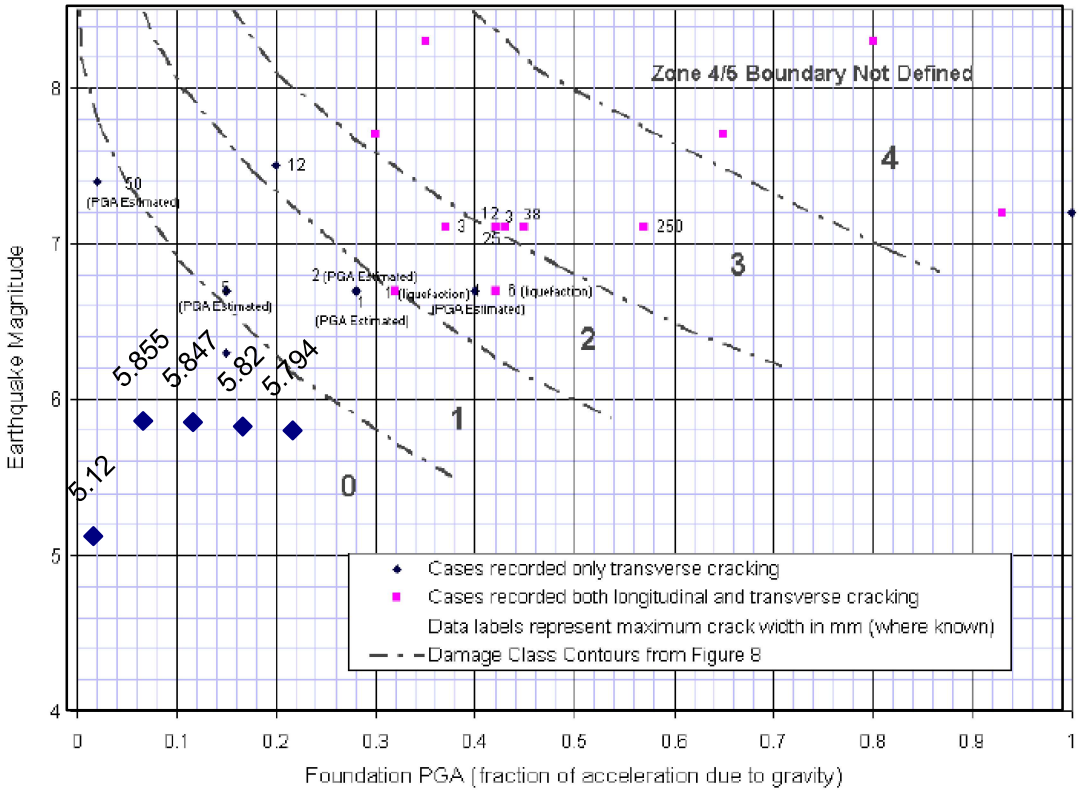
An earthquake case was considered during the original design for embankment stability assuming a pseudostatic coefficient of 0.1. The factors of safety ranged from 1.4 to 1.65. The critical earthquake failure surfaces were sliding on the base of the clay overburden overlying the Shelby Shale (near el. 130 ft NGVD). While the factors of safety approach is a limit state, the shear strength characterization using consolidated-undrained strengths (Q-tests) was very conservative and based on preconstruction testing as applied to load cases for rapid loading during construction. The existing foundation strengths below the completed embankment after dissipation of excess pore pressures would be considerably higher. The foundation clay shear strength, which predominantly impacts the factor of safety, used cohesion of 0.65 tsf. Using a simplified undrained strength approach with a conservative c/p ratio (cohesion/effective stress) of 0.25, the current clay shear strength at el. 130 ft NGVD would vary from about 1.0 tsf near the embankment toe to greater than 2.0 tsf near the centerline.

The peak ground acceleration (PGA) for the Maximum Credible Earthquake (MCE) was estimated to be 0.18g, and the USGS (2008) indicates a PGA of 0.19g corresponds to an earthquake with an AEP of 1/10,000. The normal pool of el. 210.6 ft NGVD provides about 8 feet of freeboard. The dam foundation consists of about 65 feet of lean and fat clays, underlain by a 0 to 6 feet of basal clayey sand and gravel, underlain by clay-shale bedrock. The embankment side slopes are 3.5H:1V above about el. 218.7 ft NGVD, while the slope of the berms flanking the impervious and random fill zones is generally 9H:1V. At the conduit section, the embankment is steeper at 5H:1V upstream and 6H:1V

downstream. The likelihood of a large earthquake and slope instability with large crest deformations in conjunction with a large storm approaching the PMF is remote.

PFM ##: Concentrated leak erosion (scour) in a transverse crack in the embankment due to an earthquake

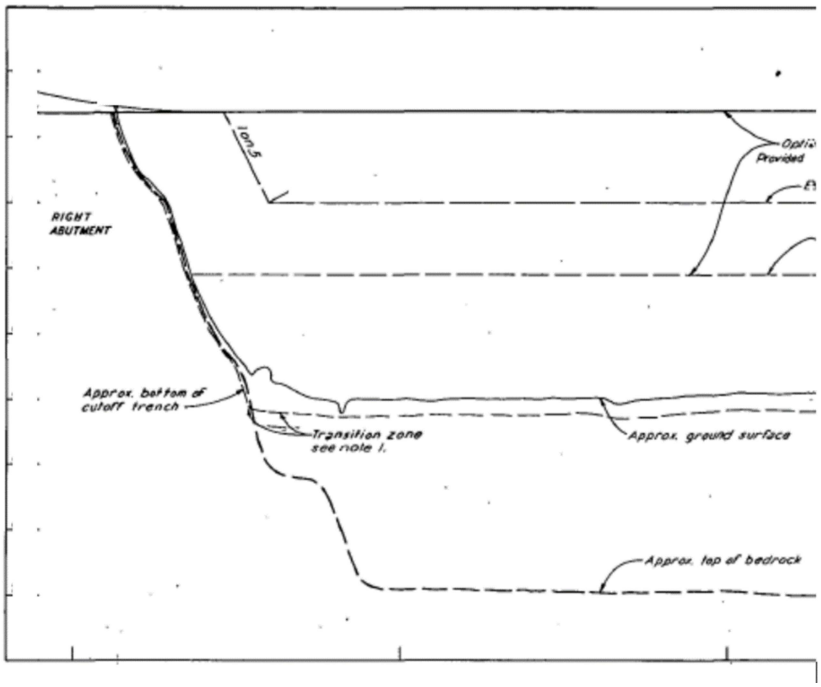
The cross-valley foundation profile is relatively uniform. The slopes of the right and left abutment rock are relatively flat at about 17 degrees and 18 degrees, respectively. The ground motions at this site are very low. The peak ground acceleration (PGA) for an earthquake with an AEP of 1/ 10,000 is approximately 0.18g. Based on incidences of transverse cracking in earthfill dams compiled by Pells and Fell (2002, 2003), the likelihood of cracking is remote (Damage Class 0 – no or slight) for PGA values less than 0.3g and the expected M_w of less than 5.9 from the USGS 2002 Banded Deaggregation tool, as shown below.



PFM ##: Concentrated leak erosion (scour) in a transverse crack in the embankment due to an earthquake between stations 6+00 and 8+00 (bench in right abutment profile)

The peak ground acceleration (PGA) for the Maximum Credible Earthquake (MCE) was estimated to be 0.15g, and the USGS (2008) indicates a PGA of 0.17g corresponds to an earthquake with an AEP of 1/10,000. The dam foundation consists of about 25 feet of

lean and fat clays, underlain by a 0 to 6 feet of basal clayey sand and gravel, underlain by clay-shale bedrock. The measured settlement is discussed under PFM XX. The embankment materials consist of similar deformability characteristics with a plasticity index generally greater than 15. An approximately 50-foot-long bench is located in the right abutment at about el. 1345 ft NGVD, or about 44 feet below the design crest elevation. A 6-foot-thick, inclined pervious drain (filter) provides defensive measures against this potential failure mode up to el. 1403 ft NGVD (ACE of about 1/1,600). The normal pool of el. 1395 ft NGVD provides about 9 feet of freeboard. The likelihood of a large earthquake in conjunction with a large storm approaching the PMF is remote.



PFM ##: Seiche caused by earthquake

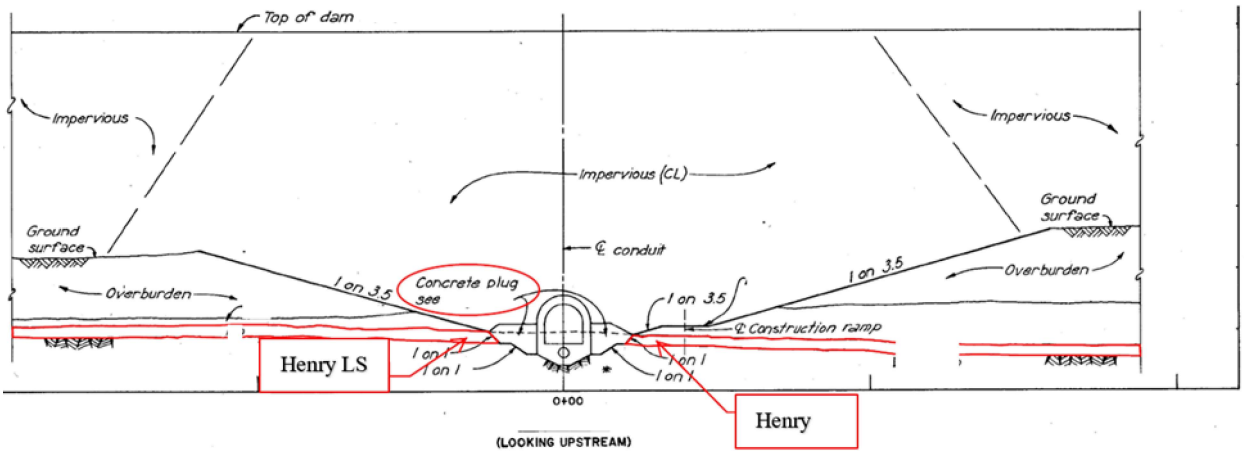
Significant instability to cause a seiche due to an earthquake was judged to be remote because the topography around the reservoir rim is relatively flat, and the foundation bedding is typically horizontal.

6. Example of Foundation Potential Failure Modes

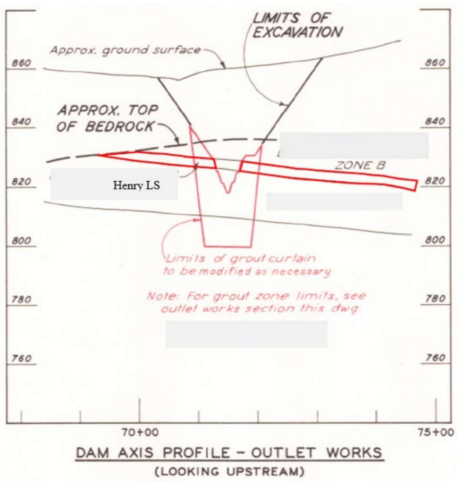
PFM ##: Internal erosion into or along an open rock defect in the Henry Limestone in the outlet works foundation

The Henry Limestone was exposed in the outlet works excavation. The outlet works foundation was grouted at the dam centerline with the relatively small grout takes in the Henry Limestone. The 2.5- to 5-foot-thick formation is not known to have widened joints

or solution features capable of accepting large quantities of material. A lean concrete plug was placed along conduit between stations 9+83 to 10+97 (dam centerline at station 120+00) to the top of the Henry Limestone (about el. 1326 to 1345 ft NGVD). Therefore, the limestone it is not in contact with the embankment at the right abutment so erosion of the embankment into any open rock defects is not possible.



Portion of concrete plug along conduit



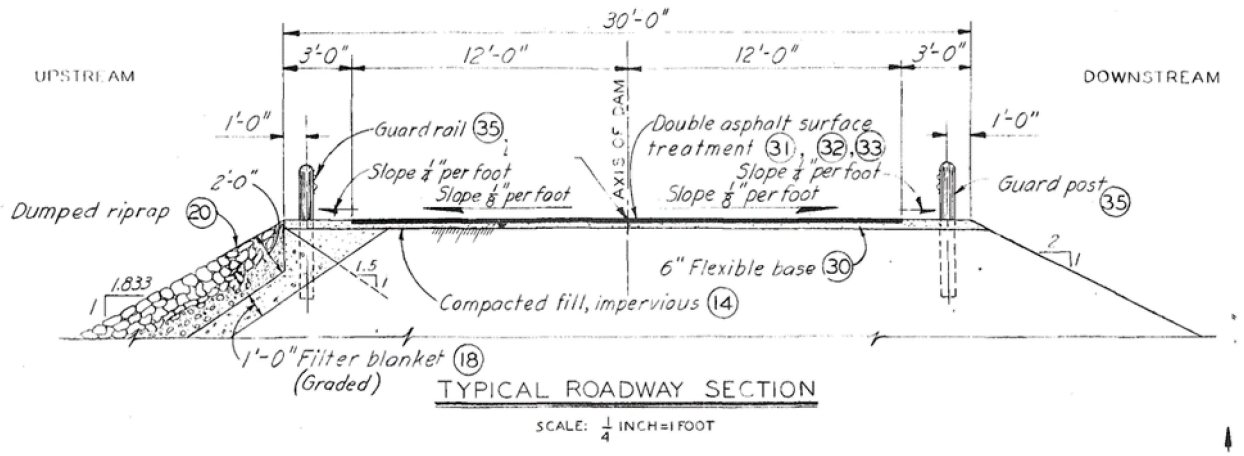
7. Overtopping and Overwash Erosion Potential Failure Modes

PFM ##: Overtopping erosion of the embankment

The lowest actual crest elevation of el. 1043.04 ft-NAVD88, and the estimated PMF elevation is el. 1038.58 ft-NAVD88. According to a 1987 study, the estimated all-direction wind setup is 0.09 foot resulting in 4.37 feet of freeboard. The combined maximum water surface elevation and wind setup do not overtop the dam. Therefore, this potential failure mode is clearly negligible.

PFM ##: Overwash erosion of the embankment

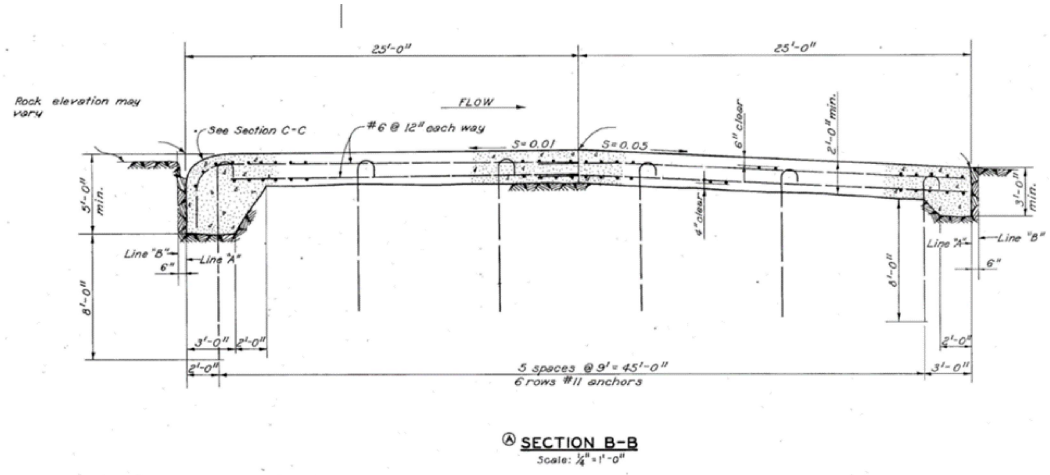
The lowest actual crest elevation of el. 1043.04 ft-NAVD88, and the estimated PMF elevation is el. 1038.58 ft-NAVD88. According to a 1987 study, the total increase in maximum water surface elevation is 4.71 feet based on an estimated all-direction wind setup of 0.09-foot and wave run-up of 4.62 feet. At the PMF with an AEP of approximately 1/100,000, sustained wind/wave action intermittently overtops the dam by 0.25-foot for approximately 6 hours. Only waves exceeding 4.37 feet will overtop the dam. The embankment consists of impervious fill, primarily classified as CL type soil (lean clay) with some CH type soil (fat clay). The downstream slope consists of mowed grass, and the asphalt-paved HR Road 192 runs along the crest of the dam. Guard rails and posts are located on both sides of the road. The likelihood of overwash erosion leading to dam breach is considered remote because of the very shallow overtopping depth and relatively short duration of overtopping of the paved crest and grassed downstream slope. Therefore, the potential failure mode was considered clearly negligible and excluded from further consideration.



8. Examples of Spillway Erosion Potential Failure Modes

PFM ##: Spillway erosion

The uncontrolled spillway was excavated in dolomite and is not lined. The crest elevation of the spillway is el. 386 ft NGVD, which corresponds to an ACE of about 1/150. The exit chute is approximately 580 feet long at a 5 percent slope. It terminates near the head of an existing ravine. The spillway has a 2-foot-thick, reinforced-concrete control sill with a turndown thickness of 5 feet upstream and 3 feet downstream that is anchored 7 feet into bedrock. The spillway channel is excavated in durable rock with approximately 7-foot joint sets. It is expected that the weathered rock would be scoured quickly, but erosion would then slow once the more durable underlying rock was exposed. The erosion mechanism would likely consist of plucking; however, headcut migration to the control sill is considered very unlikely due to the size of the joint sets and the length of the erosion path. The expected duration of flow through the spillway is about 4 days, and the maximum water depth over the spillway channel is about 3.6 feet. The likelihood of eroding approximately 600 feet of competent rock and removing a portion of the control sill during the relatively short duration of the PMF is so remote and is considered to be clearly negligible.

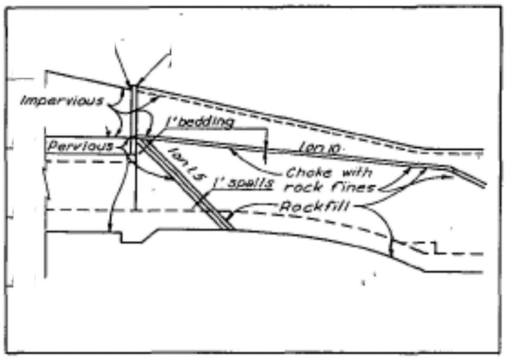


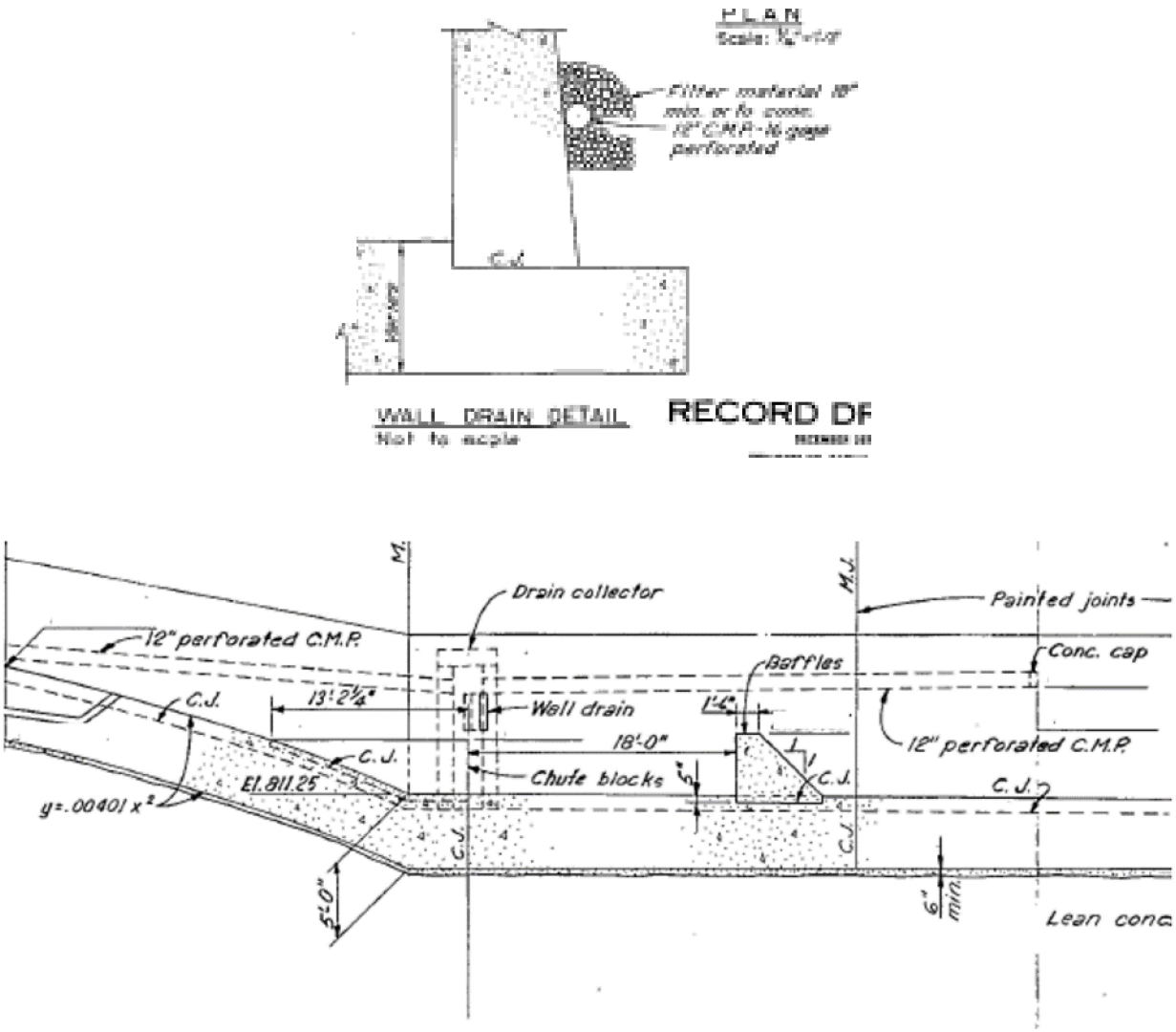
Spillway Control Sill Detail (As-Built Drawings)

9. Examples of Stilling Basin Potential Failure Modes

PFM ##: Failure of the stilling basin stilling basin walls leading that progressively erodes the toe leading to overtopping erosion

The stilling basin walls are backfilled with rockfill from the bottom of the stilling basin floor (el. 1856.25 ft NGVD) up to the top of the stilling basin wall el. (1891 ft NGVD). The rockfill is drained by a 12-inch-diameter, perforated CMP near the base of the wall. This CMP connects to a wall drain in the stilling basin. The CMP has not been inspected since installation. During a flood, it is very likely that there will be water in the stilling basin and behind the stilling basin which would result in equalized pressures on the wall. Instability of the stilling basin walls is very unlikely. Progressive erosion of the embankment toe leading to overtopping erosion would take considerable time given the relatively flat embankment slopes and the plasticity of the embankment materials. Therefore, several events must occur in series to cause failure, and the likelihood of those events is so remote and is considered clearly negligible.





PFM ##: Overtopping of the stilling basin stilling basin walls that progressively erodes the toe leading to overtopping erosion

The training walls of the stilling basin are backfilled with rockfill from the bottom of the stilling basin floor (el. 1856.25 ft NGVD) up to the top of the stilling basin wall (el. 1891 ft NGVD). Progressive erosion of the embankment toe leading to overtopping erosion would take considerable time given the relatively flat embankment slopes and the plasticity of the embankment materials. Therefore, several events must occur in series to cause failure, and the likelihood of those events is so remote and considered clearly negligible.

10. Example of Intake Tower Potential Failure Modes due to an Earthquake

PFM ##: Failure of intake tower during earthquake leading to internal erosion of the embankment into conduit

Seismic loading was not considered in the design of any of the structural features. According to the USGS (2008), peak ground acceleration (PGA) for the Maximum Credible Earthquake (MCE) was estimated to be 0.185g, and the USGS (2008) indicates a PGA of 0.19g corresponds to an earthquake with an AEP of 1/10,000. According to the foundation report, the intake tower is founded on moderately hard sandstone. Several events must occur in series to cause failure due to internal erosion, and the likelihood of those events is so remote. This potential failure mode was considered clearly negligible.

11. Examples of Gate-related Potential Failure Modes

PFM ##: Uncontrolled release from the service gates due to stainless steel roller chain binding in the slot with the gate in the open position

Inspection reports indicated that roller chains have experienced cracking of the rollers and failure of the roller keeper rings. Failure of a roller or keeper ring could result in failure of the roller chain. Failure of the roller chain has been reported to result in jammed gates at other projects. Recent inspection reports indicated that the roller chains and gates have been rehabilitated. The project has two service gates and one emergency gate that is designed to close under flow. The downstream channel capacity is 7,500 cfs, and the maximum release from one gate exceeds the channel capacity. According to the reservoir control manual, the gates are either closed or releasing minimum flow up to a pool elevation 659 NGVD. Operation permits the increase of flows beyond minimum flow up to a pool elevation of 660 ft NGVD. At el. 660 ft NGVD, releases are required to increase above 8000 cfs. If the pool rises above el. 665 ft NGVD, the operation manual requires the gates to open to full open. The gates are designed to be full open with spillway release. In order for this failure mode to result in significant consequences, the roller chains would need to break in the full open position during a high pool event. The gates are either not opened for lower pool events or are fully open during major flooding events already.

PFM ##: Overtopping erosion of the embankment due to the service gates failing to open to pass flow

Inspection reports indicate that roller chains have experienced cracking of the rollers and failure of the roller keeper rings. Failure of a roller or keeper ring could result in failure of the roller chain. Failure of the roller chain has been reported to result in jammed gates at other projects. Recent inspection reports indicated that the roller chains and gates have

been rehabilitated. The project has two service gates and one emergency gate that are designed to close under flow. According to the reservoir operations manual, the gates are either closed or releasing minimum flow up to a pool elevation of 659 ft NGVD. Operation permits the increase of flows beyond minimum flow up to a pool elevation of el. 660 ft NGVD. At el. 660 ft NGVD, releases are required to increase above 8000 cfs. Conduit capacity is 15,800 cfs total with both gates open. If the pool rises above el. 665 ft NGVD, the operation manual requires the gates to open to full open in order to release the required 15,000 cfs. With one gate closed, the conduit could still release approximately 7,000 cfs from the open gate. This would permit the system to function between el. 660 and 665 ft NGVD. The gates are designed to be full open with spillway release. The gates are either not opened for lower pool events, or full open during major flooding events already. With limited release capacity of 7,500 cfs due to a jammed closed gate, overtopping would still not occur, therefore this potential failure mode was considered clearly negligible.

PFM ##: Uncontrolled release from the service gates due to loss of a hoist and inability to prevent flow caused by an earthquake

While it is possible that release from a single gate could exceed downstream channel capacity, the gates are closed or only minimally open at pool elevations below 659 feet NVGD 29. Releases at this elevation will exceed the downstream channel capacity. However, prescribed gate operations do not require additional opening (from minimal) of the gates until reaching this elevation and therefore the non-breach consequences will have already occurred at that point. The ground motions are relatively low (i.e., PGA of 0.19g for an AEP of 1/10,000), and the likelihood of ground motions large enough to cause the loss of a hoist is also low.

APPENDIX 17-I: MAJOR FINDINGS AND UNDERSTANDINGS – EXAMPLE WRITE UP

Given below is an example write up of the Major Findings and Understandings gained from a Potential Failure Mode Analysis for a project consisting of a main concrete dam incorporating a power station and two auxiliary embankment dams. Although this was an actual study and presents the actual findings, the names of the dams and the river in the example are not the real names.

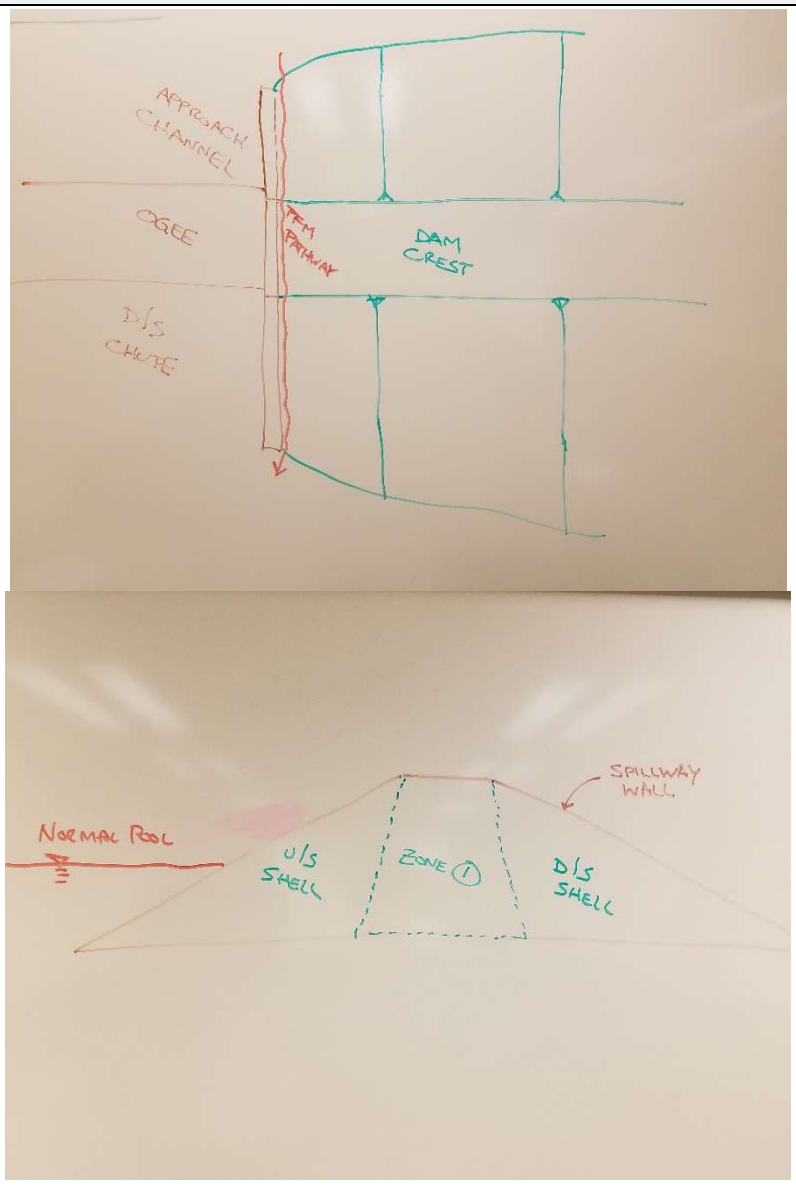
- Currently in the event of a very large flood on the Blue River, approaching the PMF, overtopping failure of Auxiliary Dam 1 is the main point of vulnerability at the project. This is because the crest of Auxiliary Dam 1 it is at a lower elevation than is the crest of Auxiliary Dam 2. In the event of Auxiliary Dam 1 failure, peak discharges downstream would nearly triple (from about 1900 m^3/s at failure to 5700 m^3/s at breach) and the consequences of failure of Auxiliary Dam 1 would be high (life loss potential and large economic losses). On the other hand if Auxiliary Dam 2 were to be established at a lower elevation than Auxiliary Dam 1 and thus allowed to fail from overtopping the effects and consequences of overtopping failure would be significantly less. Auxiliary Dam 2 failure peak discharges downstream are estimated to only be slightly larger than flows resulting from the PMF (from about 2100 m^3/s at PMF to 2400 m^3/s at breach). Several measures to achieve overtopping failure risk reduction are identified in the report and the best alternative should be selected after an appropriate risk management evaluation. However, the Potential Failure Mode Analysis team emphatically concluded that it is essential that as long as the potential for overtopping failure of the earthfill dams exists, Auxiliary Dam 2 should be established at a lower elevation than Auxiliary Dam 1.
- Dam failure as a result of internal erosion is a physically possibility at Auxiliary Dam 1 as the result of one or more potential flow paths. Although there is no unequivocal physical evidence that internal erosion has occurred or will occur in the future, the nature and relationship of the materials in the dam and foundation, the water level and piezometric observations, and the performance of the structure (observation of surface seepage and a depression at the toe) allow for this possibility. Further the surveillance and instrumentation have not been extensive enough to rule out the possibility that internal erosion episodes (turbid water or particle transport) have occurred, and even if there had been transport of material could occur subsurface and thus not be amenable to observation. The consequences of a “sunny day” internal erosion failure of Auxiliary Dam 1 would be high with a greater life loss potential due to the possible lack of advance warning. From the standpoint of the Potential Failure Mode Analysis Team, awareness of this potential internal erosion condition is a key finding of the study as this potential failure mode is the most significant structural vulnerability found at the project. Several risk reduction measures, both structural and non-structural

were identified and should be considered in the risk management evaluation of the project.

- A potential foundation failure mode identified for the Main Dam was the only PFM of significance identified for this structure. Although, this foundation potential failure mode is considered physically possible it is highly probable that a foundation stability analysis would show that the factor of safety against failure is quite high and thus risk reduction measures would not be required. Thus, the Potential Failure Mode Analysis team considers that analysis rather than consideration of remedial work is the appropriate initial course of action relative to this potential failure mode.

APPENDIX 17-J: EXAMPLE COMPLETED PFM TEMPLATE

Thisis Notur Dam	
PFM Information	
Structure	Main Dam
Loading Condition	Normal
PFM Failure Type	Internal Erosion
Location(s)	Right abutment along left spillway training wall
PFM Source	2016 PFMA
PFM Source Date	December 2016
PFM Description	
PFM No.	TND-MD-N-IE-03
PFM Title	Concentrated leak erosion along left spillway training wall
PFM Description	With the reservoir at normal pool, concentrated leak erosion initiates along a crack between the zone 1 embankment and the left concrete spillway training wall. Hydraulic gradients are sufficient to initiate erosion of the finer zone 1 materials and transport them along the crack to the downstream toe of the embankment. No filter exists downstream along the flow path and erosion continues. Sufficient fines in the zone 1 hold the crack and sufficient fines in the upstream and downstream shells do not provide flow limiting and the erosion progresses. Detection of the increasing flows are obscured by the large downstream rockfill materials and the erosion progresses undetected. Intervention is unsuccessful and the flows erode an increasingly large channel along the contact and uncontrolled release of the reservoir results.
PFM Classification	☐ Ruled Out ☐ Clearly Negligible ☐ Insufficient Info ☐ Asset Management ☒ Financial/Damage State ☒ Credible ☐ Urgent Credible
Classification Justification	This potential failure mode is considered credible. The presence of erodible materials within the embankment core, lack of a suitable downstream filter, and questionable construction control at this critical location all factor into this potential failure mode being credible.

PFM Sketch(s)

Additional Supporting Information (if needed)
This PFM is also considered during flood loading conditions. See PFM No. TND-MD-F-IE-03.
Performance Monitoring Information
Little to no seepage is reported at this location. Typically the reservoir spends only a few weeks a year at the normal pool elevation. It is unclear from the records if any seepage or flow occurs at this location when the reservoir is high. No instrumentation is installed at this location to measure flows, settlements, or pressures.

Evaluation Factors	
Adverse (More Likely)	Favorable (Less Likely)
No downstream filter	
Zone 1 core is considered moderately erodible due to lower plasticity	Core is considered not dispersive.
Hydraulic gradients are not high, but considered high enough to initiate erosion	Reservoir head is only about 10 feet
Presence of large nested rocks in rockfill downstream make detection very difficult	
Vegetation at contact can also obscure observations	
Limited to no information is available about how materials were place and compacted at this location.	
It does not appear that the concrete spillway wall is battered at this location, therefore making compaction a bit more difficult.	

Consequences	
Life Safety Consequences	
Consequence Description	Breach dimensions would likely be limited and breach formation time could be longer, both of which could limit outflows from a breach at this location. Given that, limited inundation studies indicate that flow depths and velocities would be high enough in downstream population centers and dispersed populations downstream of the dam to result in some loss of human life.
Other Consequences	
Consequence Description	A number of residences, commercial structures, industrial structures, and agricultural facilities (livestock and crops) would be impacted. Critical infrastructure, including a regionally-important state highway bridge would likely be significantly damaged or destroyed.
Potential Interim Risk Reduction Measures/ Potential Dam Safety Management Actions	
Potential Risk Reduction Measures	Remove and keep vegetation along contact cut back to facilitate observation. Stockpile filter sand and sandy gravel that could act as a crack stopper or flow limiter should this PFM activate. Install a filter downstream of the zone 1 at this location.
Inspections Actions	Routinely inspect contact for the presence of a gap or crack between the spillway wall and the embankment. Provide photographic evidence. During higher reservoir levels, this area should be inspected at least daily to see if this PFM occurs.
Surveillance and Monitoring	Consider finding a way to install a weir to measure any seepage along the pathway.

EAP	Initial flows would likely be limited due to at least some plasticity within the zone 1 and shell materials. Breach formation time should be many hours to fully develop.
Follow up Studies	Consider a focused trenching investigation to evaluate if a gap is present at this location and how deep the crack(s) go. Limited information indicates that the zone material is likely not dispersive; however, no dispersive testing has been performed. Obtain samples of the core material to investigate if the material is dispersive.
Others	
Other Notes/Comments	

APPENDIX 17-K: GENERAL FORMAT FOR POTENTIAL FAILURE MODE ANALYSIS REPORTS

I. Introduction and Background

Purpose / description of study

List key members of the PFMA team including the facilitator(s), subject matter experts, and other participants. Provide dates and location(s) of the PFMA session.

List key reference documents.

II. Description of Dam and other Key Features

Provide a general description of the dam and project features. The description does not need to be to the same level of detail as the project description included in the Part 12D Report.

III. Major Findings and Understandings

List the Major Findings and Understandings (MFU) from the PFMA. Highlight important MFU's identified and discussed by the team.

IV. Potential Failure Modes Identified

A list of candidate potential failure modes should be provided.

Provide a discussion of the screening of the potential failure modes, including justifications for why potential failure modes were considered 'ruled out', 'clearly negligible', and 'insufficient information'.

For each credible potential failure mode identified there needs to be:

- A detailed description of the Potential Failure Mode and potential adverse consequence (scenario developed by the team [**including a sketch where applicable**] and a discussion of the potential adverse consequences of the formulated scenario.)
- A listing of factors that indicate the PFM is more likely or less likely to occur.

The potential dam safety management activities identified during the discussion of each potential failure mode should also be documented in the report.

V. Summary and Conclusions

This section should include a review of the number of potential failure modes identified, any study-specific comments related to the potential modes of failure, and a summary of potential actions identified in the PFMA with respect to potential dam safety management activities.

Appendix to Report

Key supporting data and information and references, figures, sketches, photos made during field review showing key elements of dam and auxiliary features should be included along with any photos that show conditions leading to potential failure modes.

Note 1: The report of the PFMA session, although it will reside in and be appended to the STID, should be prepared as a standalone document.

Note 2: Use of tables to present Potential Failure Modes information

Tables may be an effective way to present the information related to each potential failure mode identified. However, it may not be possible to fully describe the potential failure mode in a table format. It is important to remember that the description of the potential failure mode must provide a complete understanding of the intent of the team to reviewers 5 to 25 years in the future. Thus, if tables are to be used then extra care must be taken by complete description in Section IV text to ensure that future reviewers obtain a full understanding of the team's meaning and intent. Tables may be used as a means to summarize or supplement a more complete written description of potential failure modes.