TABLE OF CONTENTS

A-3 POTENTIAL FAILURE MODE ANALYSIS

A-3.1 Key Concepts

Identifying, fully describing, and evaluating site-specific potential failure modes are arguably the most important steps in conducting a risk analysis. This forms the basis for risk evaluations and event tree development. If this is not done properly, the remainder of the risk analysis could be of limited value and even misleading.

An adequate job of identifying potential failure modes can only be performed after thoroughly reading ***all*** relevant background information on a dam, levee, or floodwall including geology, design, analysis, construction, flood and seismic loadings, operations, safety evaluations, and performance and monitoring documentation. Photographs, particularly those taken during construction or unusual events, are often key to identifying issues related to potential failure modes. It is essential that the records be ***diligently collected and reviewed***, even if those involved have familiarity with the project, as something might have been missed in previous reviews.

A site examination should also take place if at practicable. The examination team should be looking for clues as to how the dam or levee and associated structures might be vulnerable to uncontrolled release of water. Operations and maintenance personnel should be involved in the examination and queried as to how they handle flood operations and other unusual incidents. They should also be asked their opinion as to where the vulnerabilities lie.

More than one qualified person should take part in the data review and examination activities, as one person might uncover something that another might miss. The interaction of disciplines often reveals vulnerabilities that would otherwise be missed. First hand input from operating personnel is essential to the process of identifying and understanding potential failure modes. This usually occurs at the examination and initial meeting. For team facilitated risk analyses, operating personnel are typically part of the risk analysis team.

It is important to include, but also think beyond, the traditional “standards-based” analyses when identifying potential failure modes. Some of the more critical potential for uncontrolled release of water may be related to malfunction or misoperation issues, or behavior that cannot be analyzed using traditional standards-based engineering analyses.

A-3.1.1 Identifying and Describing Potential Failure Modes

Identifying potential failure modes is done in a facilitated team setting, with a diverse group of qualified people. The facilitator is ideally a senior level registered engineer with many years of experience in dam or levee design, analysis and construction. The facilitator must have participated in several failure mode and risk analysis sessions before facilitating a session. It is important to take a fresh look at the potential failure modes, and not just default to those that may have been previously identified.

The facilitator elicits "candidate" potential failure modes from the team members, based on their understanding of the vulnerabilities of the project from the data review and field conditions. It is often useful to "brainstorm" potential failure modes, then go back and evaluate each one. The first step following the brainstorming session is to identify those potential failure modes that are not expected to contribute significantly to the risk associated with the project. The detailed reasons for excluding these from further evaluation should be clearly documented. The team should discuss and agree on those that potentially contribute the most to the risk. These are often referred to as "risk-driver" potential failure modes. It should not be just one person's opinion, nor should the team just accept the previous failure mode screening.

Once the risk-driver potential failure modes have been identified, it is the facilitator's role to ensure these potential failure modes are completely described. It is important to put scale drawings or sketches up on the wall and sketch the potential failure modes during the discussions. The potential failure modes must be described fully, from initiation through step-by-step progression to breach and uncontrolled release. There are three parts to the description:

- **The initiator.** This could include increases in water levels due to flooding or flood inflows (perhaps exacerbated by a debris-plugged spillway), strong earthquake ground shaking, misoperation or malfunction of a gate or equipment, and degradation or deterioration (e.g., fatigue, scour, alkali-aggregate reaction/alkali-silica reaction).

- **Failure progression.** This includes the step-by-step mechanisms that lead to the breach or uncontrolled release of water. The location where the failure is most likely to occur should be also be highlighted. For example, this might include the path through which materials 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 breach or uncontrolled release of water 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.

The reasons for completely describing the potential failure modes are: (1) to ensure the team has a common understanding for the follow-on discussions, (2) to ensure that someone picking the report up well into the future will have a clear understanding of what the team was thinking, and (3) to enable development of an event tree or other means of estimating risks, if warranted. Examples of potential failure mode descriptions, as initially written and then as fleshed out to meet the requirements of this section, follow.

- **Unedited** (insufficient detail)**:** Sliding of the concrete dam foundation.

- **Edited:** As a result of high reservoir levels, a ***continuing increase in uplift pressure*** on the old shale layer slide plane at about elevation 1135, and a ***decrease in shearing resistance*** due to gradual creep on the slide plane, sliding of the buttresses initiates. Major ***differential movement between two buttresses takes place causing the deck slabs to be unseated*** from their simply supported condition on the corbels. ***Breaching*** failure of the concrete dam ***through two bays rapidly results.*** (Note that each of the basic failure mode components is underlined here for emphasis).

- **Unedited** (insufficient detail**):** Foundation liquefaction.

- **Edited:** Liquefaction of a continuous saturated loose sand layer in the dam foundation, identified in borings between stations 2+50 and 6+50 at about elevation 1664, leads to loss of shear strength in the layer, instability of the downstream slope, and loss of freeboard to the point that the crest drops below the reservoir level. Overtopping erosion ensues, and the embankment is breached to the base of the dam.

- **Unedited** (insufficient detail)**:** Piping through the embankment.

- **Edited:** Internal erosion of the embankment core initiates at the gravel transition interface. The core material is carried through the gravel transition zone and rockfill shell material, and into the waste berm at the toe of the dam. Backward erosion occurs until a “pipe” forms through the core to the upstream gravel transition beneath the reservoir level. At that point, flow through the “pipe” increases, eroding the core material until the gravel transition and upstream shell collapse into the void, forming a sinkhole in the upstream face. Continued increase in flow erodes and enlarges the "pipe" until the crest collapses into the void and the embankment is breached. Erosion continues to the base of the dam, about elevation 2960.

- **Unedited** (insufficient detail)**:** Dam overtopping due to gate failure.

- **Edited:** During a large flood, releases in excess of those that can be passed through the automated spillway gate are required (there are three additional spillway gates that are not automated). The limit switch on the automated gate fails (as occurred in 1994) due to a loss in Supervisory Control and Data Acquisition (SCADA) communications and the gate opens fully wiping out the main access road. An operator is deployed to the site, but cannot make it to the gate operating controls in time. The release capacity of the single automated gate is insufficient, and the dam overtops, eroding down to the stream level.

A-3.1.2 Evaluating and Screening Potential Failure Modes

A-3.1.2.1 Adverse and Favorable Factors

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 table. 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. Consider the internal erosion potential failure mode described above. A list of adverse and favorable factors might look like the following. Regular text shows how they might be captured on the flip chart or table, 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 relatively 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 benches in the excavation profile that could cause cracking.

  - 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).

A-3.1.2.2 Consequence Review

Although a detailed consequence evaluation will be performed as part of the risk analysis (see "chapter C-1, Consequences of Dam or Levee Failure"), an initial review is performed to get a general sense of how significant the downstream hazard is. This is done in two parts. ***The first part*** is the downstream impacts of the given potential failure mode; ***the second part*** relates to factors specific to the potential failure mode in terms of how quickly it might progress, whether a partial or full breach is more likely, or other site-specific attributes. The following paragraphs illustrate these two components.

- If the East Dam were to breach by this mechanism, at risk would be two county roads, several farmhouses, two bridges, a railroad line, an interstate highway, a gas pumping station, an aggregate plant, a barley mill, a transmission line, and the town of Tannerville at about 30 miles downstream. There is little recreation activity downstream of the dam. The total population at risk is estimated at about 90.

- If this potential failure mode were to initiate, it would be difficult to detect due to the coarse rockfill shell and waste berm downstream which would hide the seepage. The downstream weir is affected by precipitation that often masks the true seepage. Therefore, the failure mode could be well developed and in progress by the time it is detected. Once the core of the dam is breached to the reservoir, rapid enlargement and complete loss of the reservoir could occur in less than an hour.

A-3.1.2.3 Risk Screening of Risk-Driver Potential Failure Modes

As the team collects and discusses the adverse and favorable factors, they typically get a sense of which factors are most important and should receive the most weight, as well as the overall risk posed by the potential failure mode under consideration. Once all the adverse and favorable factors that the team can think of have been collected, and the consequences have been reviewed, each potential failure mode is screened to determine its potential contribution to the risk. It is helpful to use the semi-quantitative risk matrix approach (see "chapter A-4, Semi-Quantitative Risk Analysis") to get a sense of the risks associated with each risk-driver potential failure mode. This can be useful in identifying interim risk reduction actions, monitoring improvements, and additional data or analyses that could be useful in better defining the risks. In addition, quantitative risk analyses can be quite expensive and time-consuming, and such a screening exercise will help focus any quantitative risk analyses on only the failure modes potentially critical in terms of risk guidelines (see "chapter A-9, Governance and Guidelines").

A-3.1.3 Potential Failure Mode Considerations

A list of issues related to potential failure modes that have been identified in past potential failure mode analyses is provided below. It is not an exhaustive list, nor have the descriptions been fleshed out to the extent needed in the documentation. This must be done on a **case-by-case** basis. However, the list provides food for thought in conducting a potential failure mode analysis.

- 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 alkali-silica reaction 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 overtopping.

- Opening the gates in accordance with the Water Control Manual or Standing Operating Procedures rule curves would flood people out downstream and there may be reluctance on the part of the operators to do this, which in turn could lead to a delay in releases and premature overtopping of the dam.

- Faulty instrumentation could indicate reservoir levels and flows are within normal ranges, but dangerous inflows, outflows, or water levels are developing.

- Failure to install closure structures in levees or floodwalls can lead to an uncontrolled release into the leveed area. Careful attention must be paid to the most recent experience with operation of closures within the levee system.

- Malfunction or misoperation of gravity outlets or pumps can lead to inundation of the leveed area. However, if the interior drainage system capacity is overwhelmed, it is considered part of the non-breach risk assessment.

- Overtopping of levees is almost always a risk driver due to the height of the levee and frequency of overtopping unless there is a designed overflow or armored section.

- Overtopping of concrete dams may be acceptable and advisable. 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 or levee 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, 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.

- Seepage occurring from an unprotected/unfiltered exit could lead to internal erosion through the embankment 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.

- Vegetation can structurally compromise the performance of the levee system or its foundation, impair or prohibit needed access for inspection or emergency activities, and/or pose other risks.

- Animal burrows, vegetation, and human activity can trigger or exacerbate conditions for internal erosion through the levee embankment or its foundation.

- Scour of a floodside impervious blanket on the outside of a meander can occur due to high velocity river flows providing a direct and shortened seepage path for initiation and progression of backward erosion piping. Scour of the levee toe or channel bank can also undermine the embankment leading to instability.

- Deflection of I-walls can lead to gap formation between the sheet piling and the adjacent soils on the flood side. This gap can then be filled with water and apply full hydrostatic pressures to the I-wall along this gap, which may extend to the pile tip, and lead to global instability and breach.

- The rock foundation beneath the core of an embankment contains open joints that were not treated with slush grout or dental concrete, leading to the possibility of internal erosion of the embankment material 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 seepage paths.

- Internal erosion of material into underdrain 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.

- Metal gravity drainage pipes within levee embankments can deteriorate over time, and corrosion-induced holes the pipe walls can provide unfiltered exits for internal erosion of the surrounding embankment material into the pipe. The location and conditions of pipe penetrations are often unknown or poorly documented.

- Internal erosion can occur along the outside of poorly compacted backfill adjacent to penetrations through embankments, especially gravity drainage pipes through levees.

- 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.

- 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).

- Large spillway gates could release life-threatening flows if they failed under normal operating conditions. Buckling of radial (Tainter) gate arms under operation (trunnion pin friction) or seismic loading may be an important consideration. Deterioration due to lack of maintenance can be a contributing factor.

- Tainter gate trunnions are commonly supported at prestressed concrete piers. Failure of multiple rods in an anchorage could result in failure of the anchorage and one or more spillway gates. The design of the trunnion anchorage should be reviewed to determine if multiple trunnion anchor rods can break before anchorage failure.

- 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 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.

- Fault displacement within the foundation of an embankment dam could crack the core and lead to seepage paths and internal erosion. If fault displacement occurred within the foundation of a concrete dam, severe cracking and structural distress could result, perhaps leading to foundation erosion, differential displacement and rupture of gates, loss of the reservoir through the created gap, or loss of ability to carry load.
- Large landslides may fail quickly into a reservoir creating a wave that overtops and erodes the dam. Landslide movement within the abutment of a dam could lead to cracking of the core and internal erosion of an embankment, or foundation instability or severe structural stress to the point where load carrying capacity is lost if a concrete dam.

- Allision such as barge impacts can cause failure of spillway gates of navigation dams. Careful attention must be paid to the potential for strong outtdraft conditions toward spillways upon approach to the locks. Past records of incidents and rates of occurrence are helpful in evaluating this condition.

A-3.1.4 Summary

Potential failure mode analysis is the vital first step in conducting a risk analysis. A lot can be learned from this step alone. A thorough job of failure mode identification, description, and screening will lead to a more relevant and efficient risk analysis process. It will also help to identify potential interim risk reduction actions, monitoring enhancements, and additional data or analyses that would be helpful in better defining the risks.