VIII-1. Operational Risks

Key Concepts

In recent years, many dam failures and levee incidents have been attributed to operational failures, such as the failure of Taum Sauk Dam in Missouri in 2005 which is summarized later in this section. 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, inundation of the leveed area, or inability to get people out of harm's way. Examples of these types of failure modes (summary descriptions, not a complete list) include:

- Failure of a log boom allows reservoir debris to drift into and plug the spillway, resulting in premature overtopping and erosion of the dam.
- Gates fail to operate as intended resulting in premature overtopping and erosion 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.
- Insufficient pump capacity or inoperable pumping systems prevent evacuation of interior drainage from the leveed area leading to inundation
- Excess seepage overwhelms interior drainage facilities leading to inundation of the leveed area
- Inability or failure to close conduit gates or valves allows backflow into the leveed area leading to inundation
- Inability to warn and evacuate people in advance of life-threatening downstream flows. This could result from inability to detect the flows or a breakdown in the communication process to get people out of harms way; for example power and phone lines may be cut by a large earthquake or flood.
- Loss of access to operate key equipment during a flood leads to overtopping and erosion of the dam or other uncontrolled releases.
- Loss of release capacity leads to overtopping and erosion of the dam. For example, if releases through the powerplant 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, resulting in premature dam overtopping and erosion.
- 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.

- Levee pump stations are insufficient to remove water from the leveed area and the leveed area is flooded with deep water.
- Levee drain valves fail to close under high stage conditions and the leveed area floods with deep water through the drain conduits.
- Levee closure sections cannot be placed in time and the leveed area floods with deep water through the openings.
- Runaway barges inpact spillway sections of lock and dam projects reducing spillway capacity and flooding upstream areas.
- Failure of gates or other components at locks associated with navigation projects result in shutting down river traffic for extended periods and significant economic consequences.

Event Trees or Fault Trees?

Event trees allow the analysts to visualize the progression of events that lead to failure. Since this is how potential failure modes are typically described, most geotechnical, hydraulic, and structural failure modes are evaluated using event trees. Indeed, even relatively simple operational failure modes can be described using event tree logic. However, in some cases there may be an operational failure mode involving complex interaction between mechanical and electrical systems. This could result in an event tree with an unmanageable expanding array of branches. In such cases, a fault tree would be a more manageable tool for estimating risks. A fault tree starts with the assumed failure, and works backwards to look at the causes of the failure. It has the advantage of using "and gates" and "or gates" to link the basic events. For example, failure could result from one basic component "or" another. But each component might require conditions 1, 2, "and" 3 to occur before it fails. This allows the use of "Boolean" algebra for calculating risks. The reader is referred to the section on Mechanical and Electrical Systems and Ang and Tang (1984) for more information on fault trees.

Example Assessment

Consider a concrete arch dam in a remote location with a potentially unstable abutment. There were concerns that the abutment might slide on a low angle fault zone during a large earthquake under the combined loading from the dam, reservoir, and inertia effects, displacing the left side of the dam downstream and resulting in uncontrolled release of the majority of the reservoir.

The primary population at risk consists of people camping in two large U.S. Forest Service campgrounds along the river downstream of the dam, and about 1000 people in three small towns along the river downstream of the campgrounds. The flood wave travel time to the nearest campground is about an hour.

Due to the dam's remote location, an interim early warning system was installed to deal with this potential failure mode until remediation could be completed. The early warning system consisted of the following:

- A reservoir level gauge and downstream flow gauge. These data were collected and transmitted via satellite every 15 minutes.
- Two float triggers at different elevations on the river bank immediately downstream of the dam, two in-place inclinometers and two shear strips placed in

vertical drill holes across the fault zone, and an extensometer installed in an angled hole drilled across a critical contraction joint in the dam. These data were collected by a data logger and transmitted via satellite every 15 minutes.

- A strong motion accelerograph on the left abutment set to trigger at 0.05g, which would then transmit the ground motions via radio transmitter.
- All data were sent to a central power control center manned 24/7 where alarms would be triggered for various combinations of data levels.
- Operators at the power control center would then call the local sheriff and the Forest Service Office (which is adjacent to the upstream campground) to initiate the evacuations.

The question to be answered during the risk analysis was how effective would this warning system be in reducing risk, or put another way, what are the chances the early warning system would fail to operate as intended and/or fail to achieve the desired results? Thus, it is an evaluation of potential operational failure. To assess this, the team developed an event tree to show the steps that must occur for the warning system to be successful. If any of these steps breaks down, the system would be unsuccessful. The event tree is shown in Figure VIII-1-1, and consists of the following steps:

- Failure is detected by the system and the alarms are triggered
- The decision is made to evacuate the population at risk
- The population at risk is notified of the impending failure flood
- The population at risk is successfully evacuated prior to the flood

It was noted that the population at risk would be larger during camping season, and that communications would be enhanced during the daytime hours when people are up than at night when people are asleep. Thus, the event tree contained branches for each of these possibilities. The campgrounds are closed from October through April, and camping season is from May through September.

Since the Early Warning System was intended to save lives, and since the goal is to examine how effectively it would do so, it is necessary to evaluate all aspects of the system as well as the Emergency Action Plan all the way to evacuation of the population. The following factors were noted relative to branches of the event tree (see also the section on Event Trees).

Warning System is Able to Detect Failure

The following factors would make the warning system “more likely” to detect dam failure.

- There are three independent “platforms” to collect and transmit data. One in the valve house for the reservoir level and downstream flows, one in the “cabin” on the left abutment for the abutment instruments and downstream floats, and the radio platform for the strong motion instrument. This provides redundancy in transmitting data.
- There are numerous independent instruments that provide for possible verification of dam failure and alarms are so programmed.

The following factors would make the warning system "less likely" to detect dam failure.

- A false alarm has already occurred due to a faulty downstream float gauge (but there was no secondary verification alarm). The instrumentation is not 100 percent reliable.
- A major seismic event near the site capable of failing the dam could wipe out all communications platforms at the site. While this could be an indication of dam failure, it could also be interpreted as something else.
- Due to the remoteness of the site and lack of cell phone service, visual verification of dam failure would not be possible except by happenstance.

Based on consideration of these factors, the team estimated somewhere between a neutral (0.5) and likely (0.9) chance that the warning system would successfully detect dam failure. The independent platforms and instrumentation should make the chance of detection good. The false alarm tested the software and allowed it to be corrected and verified. However, the team was concerned that there was a reasonable chance that communications would be lost completely, and that this would not be interpreted as dam failure. The overall mean estimate was about 0.8.

Decision is Made to Evacuate the Population at Risk

Given a dam failure and that the early warning system successfully detects the failure through the alarm systems in place, the factors that make the decision to initiate an evacuation "more likely" included the following.

- Operating personnel have taken part in a "Table Top" exercise related to dam failure and the need to evacuate the downstream population. Given this, and having dealt with the false alarm has given them a good idea of what the alarms mean, and what needs to be done if they are triggered.
- Operating personnel have been given the authority to initiate the evacuation. The notice to evacuate can be given directly without going through other offices for approval.

Factors that make initiation of an evacuation "less likely" included the following.

- The decision to evacuate would need to be made without visual confirmation of the dam failure. There might be a reluctance to initiate a panic situation where people could get hurt in just evacuating the area.

The team decided that initiation of evacuation would be likely (0.9) if dam failure was detected, given the current awareness level of the operators, but perhaps not 100% since it would need to happen quickly without visual confirmation.

The Population at Risk is Notified

The ability to notify the population at risk would be dependent on the time of year and the time of day. During camping season, not only would the towns need to be notified, but the campgrounds and recreation areas as well. The logistics of notifying the downstream population might be different during the day than at night. The factors that make successful notification "more likely" included:

- The sheriff's office can be contacted 24 hours a day, 7 days a week.
- The inundation area has reliable phone service under normal conditions (i.e. prior to arrival of the flood wave).

- It might be possible to contact the Forest Service office during normal business hours to begin the evacuation of the campgrounds during camping season.
- The population in the towns is relatively concentrated and easy to access.
- During the day, communications are better facilitated since people are typically up and alert.
- At night, most of the recreationists would be concentrated in the two campgrounds.

Factors making successful notification "less likely" included:

- The Forest Service office is staffed only during normal business hours. With the increased use of voice mail and automated answering systems, it is not certain anyone at the office could be reached.
- The sheriff's office is on the opposite side of the county. If the sheriff or a deputy were not in the area, someone would need to drive up through the eventual inundation area to deliver the evacuation notice, which could take up to 30 minutes.
- During camping season, campers and recreationists would need to be found and notified. During the day, these people are spread out along the river, and may be difficult to warn.
- At night, it might be necessary to wake and warn everyone in the flood plain; it would not be possible to count on "word of mouth" to spread the message.

The team concluded that notification would be likely to very likely (0.9 to 0.99) during the non-camping season, since the towns were easily accessed and the word could be spread quickly, with a little more difficulty at night than during the day. During camping season, it was uncertain (neutral, 0.5) whether the campers could be notified during either daytime or nighttime hours. During the day, there could be a deputy in the area, but it would be difficult to find and warn all the recreationists. During the night, it would be easier to locate the campers, but there may not be anyone in the area to initiate the notifications.

Population Evacuates

Given that the downstream population was notified of the impending flood wave, factors which make a successful evacuation "more likely" included the following.

- About 90 percent of the population at risk could leave the area on paved roads.
- The river valley is fairly narrow. It is fairly obvious which way to climb (uphill away from the river) to get out of harms way.

Factors making a successful evacuation "less likely" included the following.

- The notification may not occur in time to get everyone out.
- Warned people may choose not to leave for various reasons.
- There may be a bit of a traffic jam if everyone tried to leave at once since the lanes of traffic out of the area are somewhat limited.

The team concluded that people would leave if notified by the authorities, and that there was ample capacity to get everyone out if warned in a timely fashion, and thus considered this branch to be likely to very likely under all conditions.

In examining Figure VIII-1-1, it can be seen that based on the team's evaluation, the expected chance of the warning system being fully successful is only a little over 50 percent. The evaluation was instructive to identify areas where the warning system could be improved. In addition, the consequences could be added to the tree, and ranges added to all the branches. Then a Monte-Carlo analysis of the tree would provide a distribution of consequences to use in estimating risks for the failure mode.

Relevant Case Histories

South Fork, PA

South Fork Dam was constructed upstream of Johnstown, Pennsylvania, forming a lake for a fishing club. The dam, as originally constructed between 1840 and 1853, was 72 feet high and over 900 feet long. It was constructed of rolled earth and puddled material, and contained a low-level stone culvert through the dam. In 1862 the stone conduit collapsed and the dam failed through internal erosion. However, there were no significant consequences as the reservoir was low at the time. The low level outlet conduit was plugged and filled in during dam reconstruction. The spillway was 99 feet wide and crossed by a bridge with supports spaced at 6.5 feet. Iron screens were placed across the spillway to prevent fish from escaping. The crest of the dam was lowered 2 feet to widen the roadway on top of the dam to allow carriages to pass. No camber was left in the dam, and the center portion of the dam may have been lower than at the abutments. In May of 1889 a large rainstorm advanced from the west. The large inflows sent debris to the spillway area where it became lodged in the fish screens, plugging the spillway. Overtopping erosion failure of the dam ensued. More than 2,200 people lost their lives. See also Frank (1988). This was the largest catastrophe in the U.S. from a single event until the terrorist attacks of September 11.

Taum Sauk, MO

The 2005 failure of Taum Sauk Dam in Missouri brought renewed attention to operational failure modes. The dam formed the upper reservoir of a pumped-storage project. The dam was a concrete faced earthfill structure, forming a complete "ring" on the top of a large hill. Water was routinely stored on a 10-foot-high parapet wall above the crest of the dam. After a membrane liner was installed in 2004, the instrumentation for measuring the water level in the reservoir was tied to cables in the reservoir because the warranty for the liner would have been void had holes been drilled through it to secure the instruments. The cables, which were installed near the power intake, loosened due to the hydraulic currents. In addition, settlement of the embankment was not taken into account in re-setting the reservoir level sensors. Finally, the reservoir level sensors were re-wired such that both the high level sensor and near overtopping sensor would have to be triggered before an alarm was sent to the control center. The reservoir was overfilled due to pumping, overtopped with no alarm trigger, and failed. The instrumentation installed to detect and prevent such an occurrence did not provide accurate readings or function as originally intended. A house with five people inside was destroyed in the downstream flooding. Miraculously, everyone in the house was thrown upstream when the water hit, and no one died. Additional information can be found in FERC (2006).

Marseilles, IL

In the spring of 2013, six barges broke free while attempting to enter the lock channel at the Marseilles navigation project in Illinois. The spillway was releasing flows to regulate the river stage at the time. Tainter Gates 2 through 6 of the spillway section were impacted. The trunnion anchorage at Pier 2 was destroyed leaving Gates 2 and 3 inoperable. The reduced spillway capacity resulted in raising of the upstream pool to the point where it overtopped the main dam and an upstream embankment dike that protected a large residential area, resulting in erosion of the embankment, deep flooding of the residential area, and significant economic damages.

Note: Some additional examples of levee operational failures are shown in the presentation that goes along with this manual chapter.

Exercise 1 (Dams)

Given the following potential failure mode description develop an event tree to evaluate dam overtopping as a result of operational failure.

During a large flood, releases in excess of those that can be passed through the automated gate are required. The automated gate is opened to buy some time until an operator can get to the site. The limit switch on the automated gate fails (as it did in 1994) due to a loss in 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 before the main access road is wiped out. The operator next must attempt to make it to the site through the back road, but due to bad road conditions does not make it to the dam in time to operate the gates, and the dam breaches by overtopping erosion.

Exercise 2 (Levees)

Given the following potential failure mode description develop an event tree to evaluate inundation as a result of operational failure.

During a large rainfall event related to a severe thunderstorm, the creek experiences a rapid rise in water level in excess of those that can be passed without the installation of a closure along Park Avenue. Post and beam closure structure components are located in a shed in the maintenance yard on the far side of town about a 15 minute drive away. It has been twenty years since the structure was installed and there are no directions stored with the parts. The concrete sill for the closure structure was paved over by the highway department two years ago to smooth the roadway for truckers and improve drainage from the road. The gap between the ends of the floodwall where the closure structure should be installed is 70 feet wide, and flood waters are expected to crest 6 feet above the road surface. There is insufficient time to chip the asphalt, and transport and install the closure structure. The residents under the direction of the fire chief and the public works manager attempt to sand bag the opening. All efforts to close the opening fail and the deep floodwaters enter the town along Park Avenue.

References

Ang, A. and W. Tang (1984), *Probability concepts in Engineering Planning and Design – Vol. II: Decision, Risk, and Reliability*, Wiley, New York

FERC (Federal Energy Regulatory Commission) (2006), "Report on Findings on the Overtopping and Embankment Breach of the Upper Dam – Taum Sauk Pumped Storage Project, FERC No. 2277.

Frank, W.S., "A New Look at the Historic Johnstown Flood of 1889," *Civil Engineering Magazine*, pp. 63-66, May 1988.

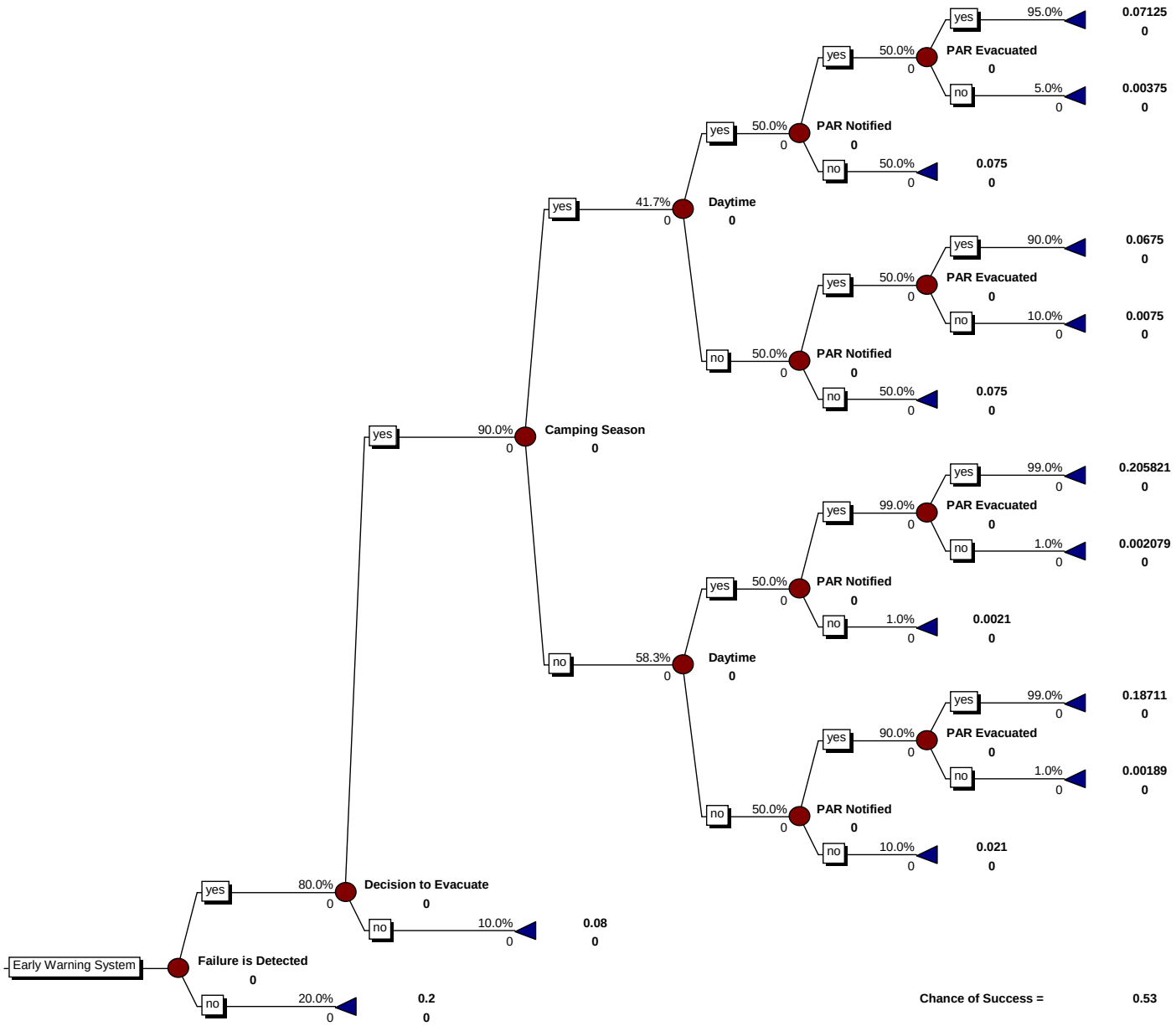

Figure VIII-1-1. Early Warning System Event Tree