Current State-of-Practice in Dam Safety Risk Assessment

Scott T. DeNeale
Gregory B. Baecher
Kevin M. Stewart
Ellen D. Smith
David B. Watson

December 2019

**Approved for public release.
Distribution is unlimited.**

OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

Environmental Sciences Division

CURRENT STATE-OF-PRACTICE IN DAM SAFETY RISK ASSESSMENT

Scott T. DeNeale, Oak Ridge National Laboratory
Gregory B. Baecher, University of Maryland, College Park
Kevin M. Stewart, Oak Ridge National Laboratory
Ellen D. Smith, Oak Ridge National Laboratory *(retired)*
David B. Watson, Oak Ridge National Laboratory *(retired)*

December 2019

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

AEP	annual exceedance probability
ALARP	as low as reasonably practicable
ANCOLD	Australian National Committee on Large Dams
ANS	American Nuclear Society
ANSI	American National Standards Institute
ARS	Agricultural Research Service
ASCE	American Society of Civil Engineers
ASDSO	Association of State Dam Safety Officials
BC Hydro	British Columbia Hydro and Power Authority
BIA	Bureau of Indian Affairs
BLM	Bureau of Land Management
CDA	Canadian Dam Association
CDF	cumulative distribution function
CEATI	Centre for Energy Advancement through Technological Innovation
CFR	Code of Federal Regulation
CNSC	Canadian Nuclear Safety Commission
CONUS	contiguous United States
DEFRA	(UK) Department for Environment, Food, & Rural Affairs
DOE	Department of Energy
DSIG	Dam Safety Interest Group
DWR	(California) Department of Water Resources
EAP	emergency action plan
EPRI	Electric Power Research Institute
FDSS	Federal Dam Supervisory Section (Austria)
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FMAF	Federal Ministry of Agriculture and Forestry (Austria)
FMEA	failure modes and effects analysis
FN (curve)	frequency-severity (curve)
GDC	General Design Criterion
HEC	Hydrologic Engineering Center
HEC-RAS	Hydrologic Engineering Center River Analysis System
HHA	hydrologic hazard analysis
HHC	hydrologic hazard curve
HRA	human reliability analysis
IBWC	International Boundary and Water Commission
ICODS	Interagency Committee on Dam Safety
ICOLD	International Committee on Large Dams
IDF	inflow design flood
IFT	Independent Forensic Team
MC	Monte Carlo
MSHA	Mine Safety and Health Administration
MWR	(Chinese) Ministry of Water Resources
NCDC	National Climatic Data Center, now National Centers for Environmental Information (NCEI)
NDSP	National Dam Safety Program
NDSRB	National Dam Safety Review Board
NID	National Inventory of Dams

NOAA	National Oceanic and Atmospheric Association
NPDP	National Performance of Dam Project
NPP	nuclear power plant
NPS	National Park Service
NRC	US Nuclear Regulatory Commission
NRCS	National Resources Conservation Service
OBE	operating basis earthquake
OPG	Ontario Power Generation
PAR	Population at Risk
PFHA	probabilistic flood hazard assessment
PFM	potential failure mode
PFMA	Potential Failure Modes Analysis
PLC	programmable logic controller
PMF	probable maximum flood
PMP	probable maximum precipitation
PRA	probabilistic risk assessment
PSHA	Probabilistic Seismic Hazard analysis
RCC	roller-compacted concrete
RG	Regulatory Guide
RIDM	risk-informed decision-making
SCADA	supervisory control and data acquisition (system)
SIMBA	Simplified Breach Analysis
SME	subject matter expert
SSC	structures, systems, and components
SSE	safe shutdown earthquake
SSHAC	Senior Seismic Hazard Analysis Committee
TVA	Tennessee Valley Authority
UK	United Kingdom
US	United States
USACE	United States Army Corps of Engineers
USBR	Unites States Bureau of Reclamation
USDA	United States Department of Agriculture
USFS	United States Forest Service
USFWS	United States Fish and Wildlife Service
USGS	United Stated Geological Survey
USSD	United States Society on Dams

ACKNOWLEDGMENTS

EXECUTIVE SUMMARY

Dams provide significant benefits to the nation, serving as critical infrastructure to deliver water retention and control throughout the United States (US). Major cities could not function without the fresh water supply stored in dammed reservoirs, and many electrical systems rely on dependable hydroelectric power supply. Dams on rivers across the country protect communities against destructive flood impacts while providing navigable waters for transportation, irrigation for agriculture, and various opportunities for recreation. While dams provide many essential services, dam failure flooding can present significant risks to property and life. Over decades of experience, dam safety practices, including risk assessment, have evolved as engineering knowledge, scientific understanding, and technological advancements grow. This project summarizes the current state-of-practice in dam safety risk assessment.

The US government instituted dam safety programs following the failures of Buffalo Creek (1972), Teton (1976), and Kelly Barnes (1977); and today, all states but one have adopted state dam safety programs. The current state-of-practice in US dam safety risk assessment has been used by the dam safety community for over 20 years and was adopted by the Federal Energy Regulatory Commission under the term, *risk-informed decision making*. Risk-informed decision making enables structured, engineered approaches to identifying, classifying, and quantifying potential dam failures and provides a mechanism for dam owners, designers, operators, and regulators to communicate dam safety risk and mitigate concerns. More comprehensive *probabilistic risk assessment* is practiced by the US Army Corps of Engineers, the Bureau of Reclamation, and many private sector dam owners. Yet its implementation may be challenging because of gaps in knowledge, uncertainty associated with the physics of dam failure, and difficulty in communicating results with stakeholders. Together, federal and state dam safety frameworks have helped prevent major calamities, and risk prioritization tools have been leveraged with success.

Given the risk that dam failure flooding can pose to nuclear power plant safety, this project supports the US Nuclear Regulatory Commission (NRC) in surveying the current state-of-practice in dam safety risk assessment to support risk-informed operating and new reactor licensing and oversight. The information assembled in this report is intended to aid the NRC in developing guidance on the use of *probabilistic flood hazard assessment* methods and support the provision of dam failure flooding risk information to NRC's licensing framework.

This literature survey report highlights the history and importance of dam safety in the US, describes the primary federal and state organizations engaged in dam safety, describes the primary physical and operational considerations in dam engineering, summarizes the principal features of dam safety risk assessment and modeling, summarizes the critical aspects of operational risk, documents the relevant software tools for dam safety risk analysis, catalogues historical dam failures, and provides insights from recent dam incidents and failures. The information assembled provides an assessment of key aspects of dam safety risk assessment, including the following (among others):

- Probabilistic engineering analysis methods for assessing dam stability and integrity
- Reliability of key components such as gates, gate hoists, valves, and so forth
- Systems analysis approaches
- Reliability of operational and emergency procedures
- Methods for estimating breach initiation and the progression and propagation of uncertainties

1. INTRODUCTION

Dams are important infrastructure elements. Many cities and regions could not function without the fresh water supply stored in their reservoirs, and many regions rely on hydroelectric generation to supply reliable power. Mainstem dams on the Missouri, Columbia, and other rivers protect great inland valleys against the ravages of floods, provide navigable waters for commercial traffic, supply irrigation water needed for agriculture, and support numerous recreational activities. However, dams can also be dangerous. If a dam loses containment, downstream property damage can be catastrophic with the potential for loss of life. In some cases, "the failure of the dam could produce flood rates and damages greater than would have been experienced if the dam had not been built" (National Research Council 1985). Dam projects can also initiate political conflicts, which may relate to the equitable distribution of benefits, environmental impacts, and failure risks, among other considerations. In the shadow of the protection provided by a dam, land use and environmental issues arise in the altered flood plain.

To help mitigate risks posed by potential dam failure, several US federal agencies and almost every state maintain dam safety programs. These programs are designed to inspect and monitor the structural, hydraulic, and geotechnical integrity of dams and dam components. Such inspections may include periodic technical inspections, periodic maintenance inspections, and informal observations that use checklists and inspection forms (National Research Council 1983). In many jurisdictions, dam safety programs are also involved in reviewing and approving emergency action plans (EAPs).

To estimate the risks posed by potential dam failure, qualitative or quantitative assessments may be performed. Dam safety and risk assessment are important to owners and operators liable for safe operation, upkeep, upgrade, and repair; regulators charged with evaluating conditions and plans; communities benefitting from various services; and populations at risk from potential dam failure consequences.

This report provides a review of the current state-of-practice in dam safety risk assessment. It is organized into the following sections:

- Section 2—highlights the history and importance of dam safety in the United States (US).
- Section 3—describes the primary federal and state organizations engaged in dam safety.
- Section 4—describes the primary physical and operational considerations in dam engineering.
- Section 5—summarizes the principal features of dam safety risk assessment and modeling.
- Section 6—summarizes the critical aspects of operational risk.
- Section 7—documents the relevant software tools[1] for dam safety risk analysis.
- Section 8—provides an overall report summary.
- Appendix A and B—catalogue historical dam failures and provide insights from recent dam incidents and failures, respectively.

The information contained in this report is intended to aid the US Nuclear Regulatory Commission (NRC) in developing guidance on the use of probabilistic flood hazard assessment (PFHA) methods and support the provision of risk information to NRC's licensing framework in the context of flooding hazards due to dam failure. This information will support and enhance NRC's capacity to perform thorough and efficient reviews of license applications and license amendment requests. It will also support risk-informed determination of the significance of inspection findings, unusual events, and other oversight activities.

---

[1] The mention of specific software tools in this report does not constitute endorsement or approval for any specific use by the NRC or ORNL.

2. HISTORY AND IMPORTANCE OF DAM SAFETY IN THE UNITED STATES

The first known dam was constructed by ancient Egyptians nearly 5,000 years ago, and the first known concrete dam was built by Romans nearly 2,000 years ago (Yang et al. 1999). Over time, dam construction evolved and gave way to engineered design. While many dams endure for decades and even centuries (the oldest standing dams are roughly 1,800 years old), poor design and/or structural degradation has yielded many historical dam failures.

The deadliest US dam failure resulted from the 1889 failure of the South Fork Dam on the Little Conemaugh River in Pennsylvania, which occurred as a result of flood-induced overtopping[2] and caused the Johnstown Flood in which more than 2,200 people died. Over the ensuing 80+ years, many other disastrous dam failures occurred, and hundreds of lives were lost. It was not until after the 1972 Buffalo Creek Dam failure that Congress authorized the US Army Corps of Engineers (USACE) to inventory and inspect non-federal dams.[3] Following the 1976 failure of Teton Dam and 1977 failure of Kelly Barnes Dam, additional action was taken to bolster dam inspections. In 1978, the US Bureau of Reclamation's (USBR) Dam Safety Program was established in response to the Teton Dam failure. In 1979, the Federal Emergency Management Agency (FEMA) was established and was given responsibility for coordinating federal efforts to promote dam safety.[4] Current dam safety programs and authorities are covered in more detail in Section 3.

Ensuring the safety of a dam is no small task, and with over 90,000 dams in the US, the responsibility for ensuring dam safety is widely distributed. Figure 1 shows the locations of major dams, the classification of which is defined in Section 2.2, in the contiguous US (CONUS).

The remainder of this section focuses on the relevance of dam safety to the US nuclear fleet (Section 2.1), dam classifications (Section 2.2), dam purposes (Section 2.3), dam owners and operators (Section 2.4), dam failure causes (Section 2.5), dam failure consequences (Section 2.6), dam hazard potential classification (Section 2.7), and dam infrastructure condition (Section 2.8).

---

[2] Although overtopping was the immediate failure mechanism, significant structural alterations made by the dam owners (e.g., lowering the dam crest to allow construction of a road, removing a system of relief pipes and valves, installing a fish screen in the spillway) are thought to have increased the vulnerability of the dam.
[3] National Dam Safety Inspection Act (PL 92-367).
[4] Executive Order 12148 (Federal Emergency Management); July 20, 1979.
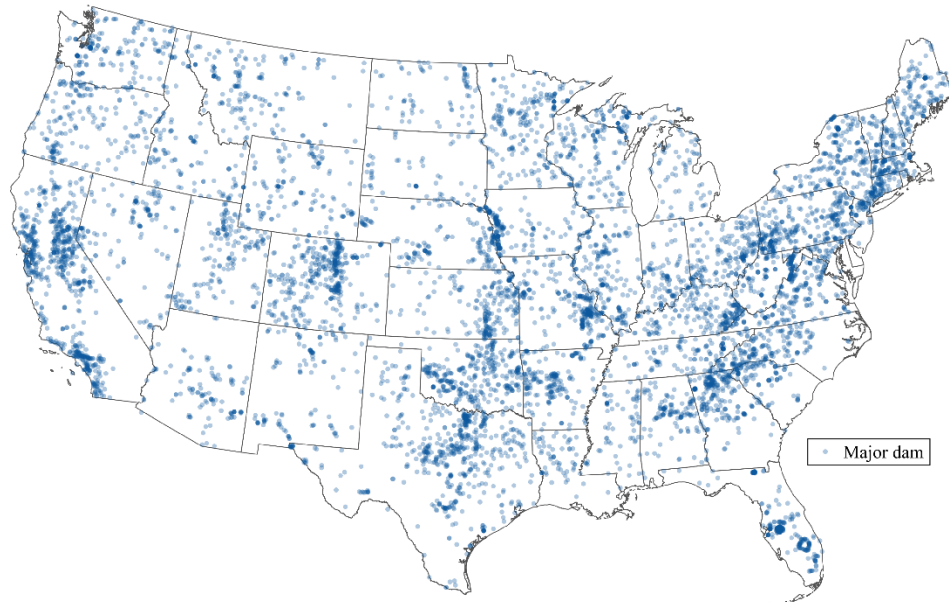
Figure 1. Major dams in CONUS. (Data from USGS[5]).

2.1 RELEVANCE TO THE US NUCLEAR FLEET

Consideration of potential floods due to dam failures is integral to evaluating flooding hazards (and thereby, risk) for nuclear power plants (NPPs). Traditionally, dam failure flooding has meant flooding due to the uncontrolled release of water from any dam upstream from the plant site that threatens to impact structures, systems and components (SSCs) important to safety at the NPP site. However, there are instances in which controlled releases could also lead to inundation at the NPP site. Examples include, but are not limited to, (1) releases performed to prevent incipient failure during flood conditions; (2) releases performed to rapidly draw down a reservoir to prevent incipient failure after a seismic event; and (3) releases performed to rapidly draw down a reservoir to prevent incipient sunny day failure. (NRC 2013). In addition, dams that are not upstream from the plant, but whose failure would affect the NPP site because of backwater effects, may present potential flooding hazards. Finally, failures of dikes or levees in the watershed surrounding the site may contribute to or ameliorate flooding hazards, depending on the location of the levee and the circumstances under which it fails. Failures of onsite water-storage or water-control structures (such as onsite cooling or auxiliary water reservoirs and onsite levees) that are located at or above the grade of safety-related equipment are also potential flooding mechanisms. Flood-induced failure of a dam or levee that impounds the ultimate heat sink (i.e., a cooling water system for use in normal and emergency operating conditions) constitutes a hazard to the plant. Therefore, dam failure flooding hazard assessments include all water-impounding structures that can affect the NPP site, whether or not they are defined as dams in the traditional sense.

To date, dam failures have not directly affected US NPPs. However, the Fukushima Daiichi incident in Japan (the magnitude 9.0 earthquake associated with the event also failed the Fujinuma Dam) heightened awareness of water and flooding issues in nuclear safety. NRC staff released a report in 2011 summarizing the current understanding of the flooding issue at NPPs related to upstream dam failures

---

[5] https://nationalmap.gov/small_scale/mld/dams00x.html (accessed November 2019)

(Perkins et al. 2011). Public interest groups, such as the Union of Concerned Scientists,[6] have also become concerned.

NRC has estimated the likelihood of failure of Jocassee dam, upstream of the Oconee Nuclear Station in South Carolina, at approximately 2.8×10^{-4} per year (Vail et al. 2010). This estimate aligns with historical dam failure rates found in literature (see Table 3 in Section 2.5). Other recent incidents related to water control infrastructure have also raised concerns, including the 2012 flooding at Fort Calhoun Nuclear Generating Station and NPP shutdowns during Hurricane Sandy.

2.2   DAM CLASSIFICATIONS

Various classification systems are used to categorize dams bases on size, hazard potential, and construction material, among others. Types of classifications include:

- **By size:** Major dams (shown in Figure 1) are defined by the US Geological Survey (USGS)[5] as those 50 ft (15 m) or more in height with a normal storage capacity greater than 5,000 acre-ft (~6 million m^3), or a maximum storage capacity of 25,000 acre-ft (~31 million m^3) or more.

   The International Committee on Large Dams (ICOLD) defines a large dam as one with a height of at least 15 m (from lowest foundation to crest) or a dam between 5 and 15 m impounding at least 3 million m^3 of water (interpreted as maximum storage).

   Despite these differing definitions, analysis of the 2016 data from the National Inventory of Dams[7] (NID), maintained by the USACE, reveals that nearly the same number of US dams fall into each of these two categories—around 8,300 large dams (per USGS definition) and around 8,700 major dams (per ICOLD definition). Additional information on the NID is provided in Appendix A.

- **By hazard potential:** US federal agencies classify dams by hazard using a three-level approach (FEMA 2004b). Failure or misoperation of low-hazard dams is expected to result in no human life loss and low economic and/or environmental losses. Similar failure or misoperation of significant hazard dams is expected to result in no human life loss but may cause economic and/or environmental losses, disruption of lifeline facilities, or other impacts. High-hazard dam failure or misoperation is likely to cause at least one human life loss. In this classification system, a dam that may result in loss of one human life is classified in the same way as a dam that may result in loss of thousands of lives. Additional information on hazard potential classification is provided in Section 2.7.

- **By construction material:** From a construction standpoint, dams generally fall into a few categories, including earthfill, rockfill, concrete gravity, concrete arch, concrete buttress, and timber dams. Most dams in the US are earthfill; however, many of the larger dams, including those posing flood hazards to NPPs, are of rockfill or concrete construction. More information on concrete gravity, concrete arch, earthfill, and rockfill dams is provided in Section 4.1.

- **Other classifications:** Dams are also classified into different categories based on use and hydraulic design, as described in USBR (1987). They can serve as storage, diversion, or detention structures, which may serve one or multiple purposes (covered in more detail in Section 2.3). A dam may also

---

[6] Available at http://www.ucsusa.org/nuclear-power/nuclear-power-accidents/flood-risk-at-nuclear-power-plants (accessed November 2019)

[7] Available at https://catalog.data.gov/dataset/national-inventory-of-dams (accessed November 2019)

include multiple structures with varying hydraulic designs meant to operate as either overflow or non-overflow structures.

2.3 DAM PURPOSES

FEMA and USACE identify recreation, flood control, water supply (including fire protection), and irrigation as leading benefits of dams (Figure 2). Although most dams were originally constructed for a single purpose (Figure 3), some provide multiple beneficial services (especially large dams, as shown in Figure 4). For example, Bonnet et al. (2015) indicates that roughly 94% of all federal hydropower reservoirs serve more than one purpose. Table 1 provides descriptions of the various common benefits of dams.

Table 1. Common benefits of dams.

Use	Description
Multipurpose	Provide multiple benefits. Many dams in the US are multipurpose
Recreation	Offer numerous recreation opportunities, including boating, fishing, skiing, camping, picnicking, and so on
Flood control	Impound water bodies and may be designed to store significant flood volumes or operated to reduce flood impacts
Water supply (including fire and farm ponds in Figure 2)	Supply water for various industrial, municipal, and agricultural purposes
Irrigation	Divert water to provide approximately 10% of the water supplied to croplands in the US.
Tailings and debris control[8]	Retain mine tailings (e.g., coal slurry, minerals, uranium mills) and control debris.
Hydropower	Include power production facilities to generate electricity as water flows from upstream to downstream.
Navigation	Provide infrastructure for inland river navigation.

---

[8] Debris control dams are often associated with the containment of hazardous materials and detrimental sedimentation resulting from mining activities and are not to be confused with natural debris dams that are formed by landslides or volcanic activity.

Dams by Primary Purpose

Purpose	Count
Recreation	25,394
Flood Control	16,179
Fire Protection, Stock, or Small Farm Pond	10,781
Other	8,462
Irrigation	7,706
Water Supply	5,628
Fish and Wildlife Pond	4,930
Hydroelectric	2,114
Tailings	1,172
Grade Stabilization	906
Debris Control	575
Navigation	207
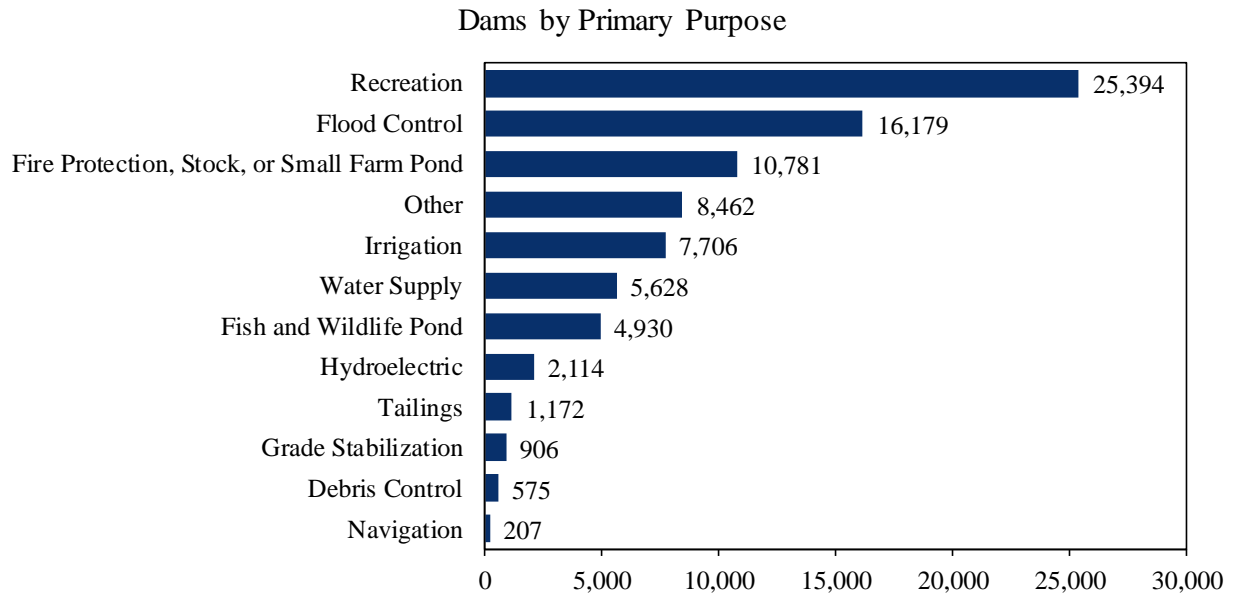
Figure 2. Number of US dams by primary purpose based on 2016 NID data.[7]

Dams by Number of Listed Purposes

Number	Count
1	66,025
2	13,484
3	3,364
4 or more	1,181
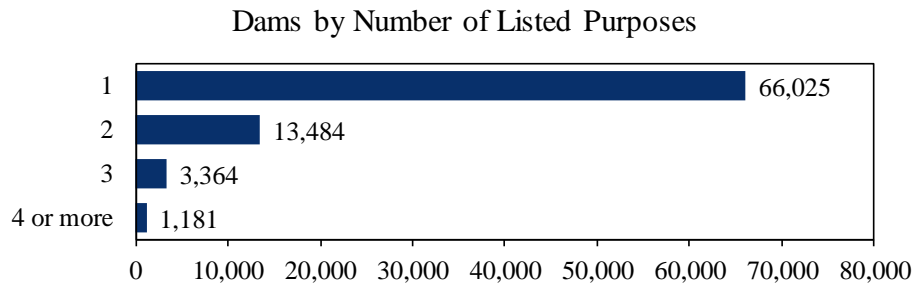
Figure 3**. US dams by number of listed purposes based on 2016 NID data.**[7]
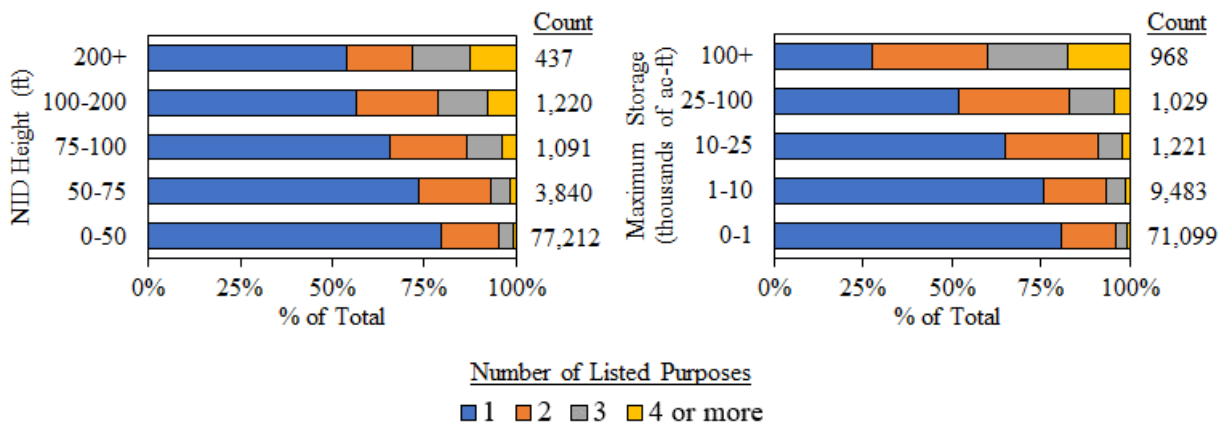
Figure 4. Number of listed purposes by NID height (left) and maximum storage (right) based on 2016 NID data.[7]

6

2.4   OWNERS AND OPERATORS OF US DAMS

Dam ownership in the US is widely distributed. Based on 2016 USACE NID data,[7] most of the dams in the US are privately owned (Figure 5). About 64% are privately owned, 27% are owned by state or local authorities, 4% are owned by public utilities (e.g., cooperative and municipal utilities), and 4% are owned by federal agencies. Although federal, state, or local authorities own only about one-fourth of low-hazard dams, they own nearly half of the high-hazard dams in the US. Federal dam owners and operators include the US Department of Agriculture (USDA), Tennessee Valley Authority (TVA), USACE, and USBR, among others. More discussion of these agencies is included in Section 3.2.1.2.

a) **Categories of Ownership for Low Hazard Dams** (2016 NID, count: 60,705)

b) **Categories of Ownership for Significant Hazard Dams** (2016 NID, count: 11,882)

c) **Categories of Ownership for High Hazard Dams** (2016 NID, count: 15,498)

■ Federal ■ Local Government ■ Not Listed ■ Private ■ Public Utility ■ State
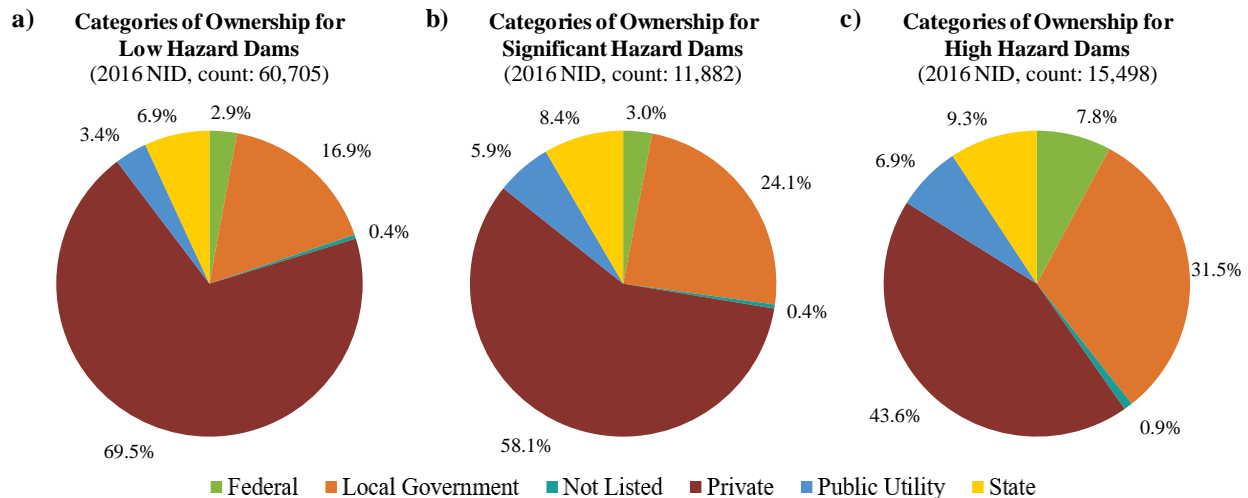
Figure 5. US dam ownership by hazard classification based on 2016 NID data.[7]

Using data from the 2016 USACE NID,[7] major dam ownership in the US (per the USGS definition provided in Section 2.2) was analyzed based on dam height and maximum storage (Figure 6). Federal, state, and local authorities account for 53% of the 8,661 major dams in the US. Although federal owners account for only 14% of major dams in the US, they account for 30% of the major dams with heights of at least 100 ft and 53% of major dams with maximum storage capacities of at least 100,000 ac-ft. Federal owners also account for a higher proportion of the high-hazard dams in the US.

a) Major Dam Ownership

984, 11%
922, 11%
1215, 14%
3070, 35%
42, 1%
2428, 28%

- Federal
- Local Government
- Not Listed
- Private
- Public Utility
- State

b) Major Dam Ownership, by NID Height

NID Height (ft): 200+, 100-200, 75-100, 50-75, 0-50
Number of Major Dams: 0 – 5,000

c) Major Dam Ownership, by Maximum Storage

Maximum Storage (thousands of ac-ft): 100+, 25-100, 10-25, 1-10, 0-1
Number of Major Dams: 0 – 3,000
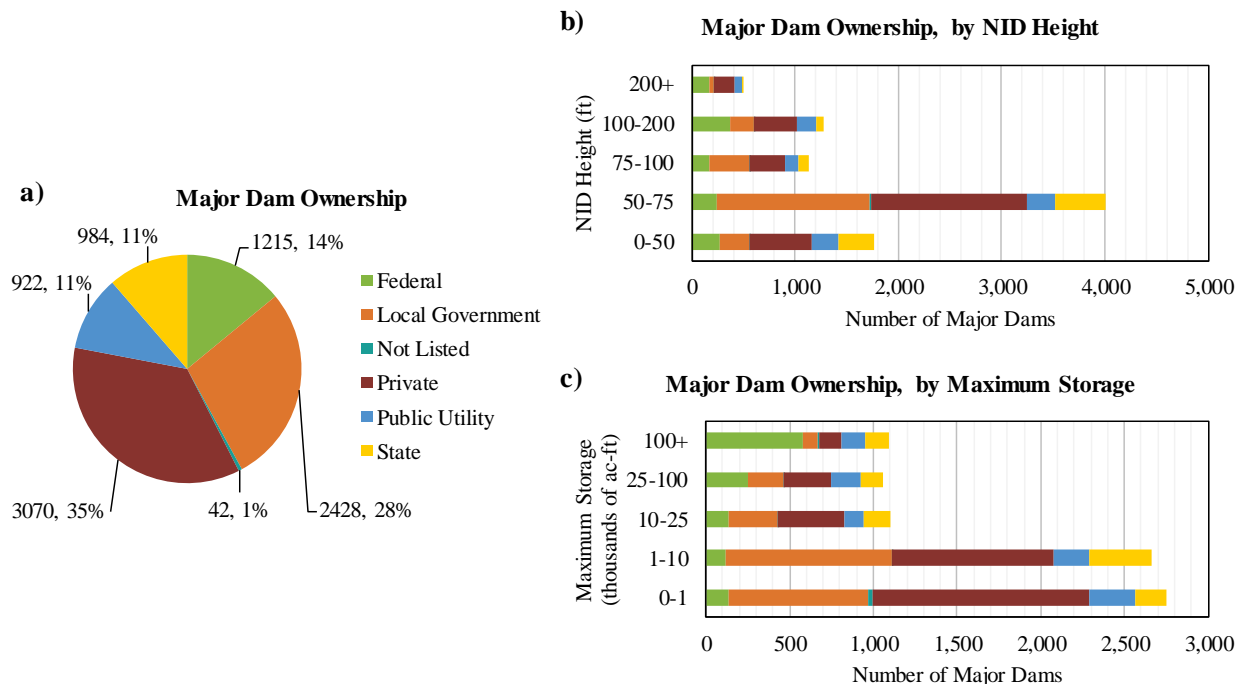
Figure 6. US major dam ownership characteristics based on 2016 NID data.[7]

2.5 DAM FAILURE CAUSES

What constitutes a dam failure can prove somewhat subjective. FEMA (2015) defines *dam failure* as

> the sudden rapid and uncontrolled release of impounded water or liquid-borne solids. It is recognized that there are lesser degrees of failure and that any malfunction or abnormality outside the design assumptions and parameters that adversely affect a dam's primary function of impounding water could be considered a failure.

While a sudden uncontrolled dam release can pose a significant flood hazard to downstream populations and facilities, the NRC's Interim Staff Guidance JLD-ISG-13-01, *Interim Staff Guidance for Assessment of Flooding due to Dam Failure* (NRC 2013) notes

> there may be instances where a controlled release of water from a dam can also lead to the inundation of an NPP site. Examples include, but are not limited to: (a) releases performed in order to prevent dam failure during flood conditions; (b) releases performed to rapidly drawdown a reservoir to prevent incipient failure after a seismic event; and (c) releases performed to rapidly drawdown a reservoir to prevent incipient sunny day failure.

Dams may fail for various reasons, including high reservoir inflows (hydrological), earthquake faulting or ground shaking (seismological), internal erosion, mechanical failures of gates and electrical systems, maloperation, and combinations of these causes. Severe natural hazards such as strong earthquakes and large floods have a relatively low annual probability of occurrence; and many incidents, and sometimes failures, are attributable to operating issues. Failures due to internal erosion and mechanical or electrical failures (e.g., supervisory control and data acquisition, or SCADA) can occur absent a natural hazard initiator and are sometimes termed "sunny day" failures (Ferrante et al. 2011, 2012). Section 4.2 contains more detail on dam failure mechanisms. Appendix A contains additional information on historical dam

8

failures, including relevant inventories. The following are some of the most common causes of dam failure (Table 2 and Figure 7):

Overtopping and inadequate spillway design
- Overtopping caused by floods that exceed the capacity of the dam (including the spillway, powerhouse, and other outlet works)
- Overtopping caused by operational issues (e.g., gates, human factors, SCADA systems)

Piping or seepage
- Internal erosion of soil in embankment dams

Slides
- Movement or failure of the foundation or abutments

Miscellaneous
- Structural failure of materials used in dam construction
- Settlement and cracking of concrete or embankment dams
- Inadequate maintenance and upkeep

Baecher et al. (1980) reports that about half of all dam failures occur within the first 5 years following initial impoundment. Most of these failures are of smaller dams, operated by private owners or local authorities. These summary numbers have changed little since they were first compiled in the 1950s.

Figure 8 shows the geographic distribution of dam incidents reported in Stanford University's National Performance of Dams Program (NPDP),[9] a database of self-reported dam incidents and failures. A category was assigned to each incident for which the type was known. The analysis reveals no significant trend over time and supports the consensus that overtopping, inadequate spillways, piping, and seepage historically represented the primary causes for failure. Structural or foundation issues are also common. The total number of historically recorded dam failures is too few to confidently parse out the effects of age, construction type, and geographic region.

The NPDP data are not comprehensive and may be biased because the data are self-reported (i.e., certain events may not be included) and because the available data are derived from certain regional events that have occurred more recently (e.g., the NPDP contains data on numerous dams that were overtopped following extensive flooding in south-central Georgia in July 1994). The publicly available incident data are only available through 2006, though data collection efforts are ongoing. More information regarding the NPDP is provided in Appendix A.

The historical rate of dam failures is reasonably low compared with other technogenic risks faced by society (Baecher and Christian 2003).With 90,580 dams in the US and 173 state-reported dam failures from January 2005 to June 2013, US dams have an approximate annual failure rate of around 2×10^{-4} per dam-year[10] according to the Association of State Dam Safety Officials[11] (ASDSO). Other literature indicates a similar annual failure rate (Table 3). The frequency of failure of large, modern dams operated by competent authorities is between 1×10^{-5} to 1×10^{-4} per dam-year (Baecher et al. 1980; Regan 2009).

---

[9] Available at http://npdp.stanford.edu (accessed November 2019).
[10] This value is computed as 173 failures divided by 769,930 dam-years (90,580 dams $\times$ 8.5 years), so there is a 0.02% chance of a single dam failing in a single year based on the historical failure rate.
[11] https://damsafety.org/dam-failures (accessed November 2019)

Based on the number of dams in the US, this implies an annual rate of dam failure in the US of about ten per year.

Table 2. Dam failure causes (as percentage of total reported failures) from historical data.

Reference	Principal failure mechanism			
	Overtopping or inadequate spillway	Piping or seepage	Slides	Miscellaneous
Middlebrooks 1953	30%	38%	15%	17%
Gruner 1967	23%	40%	2%	35%
Takase 1967	28%	44%	10%	18%
Babb and Mermel 1968	36%	30%	15%	19%
USCOLD 1975	38%	44%	9%	9%
Foster et al. 2000	46%	48%	6%	—
Zhang et al. 2007	39%	53%	—	8%
Regan 2009	49%	20%	31%	—
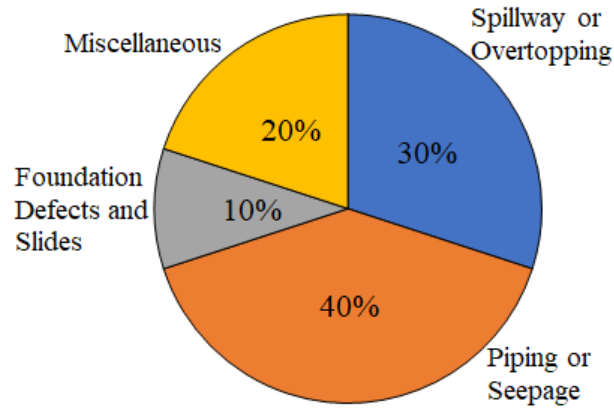
Figure 7. Approximate fraction of international dam failures by proximate cause. (Modified from Baecher et al. 1980)

10
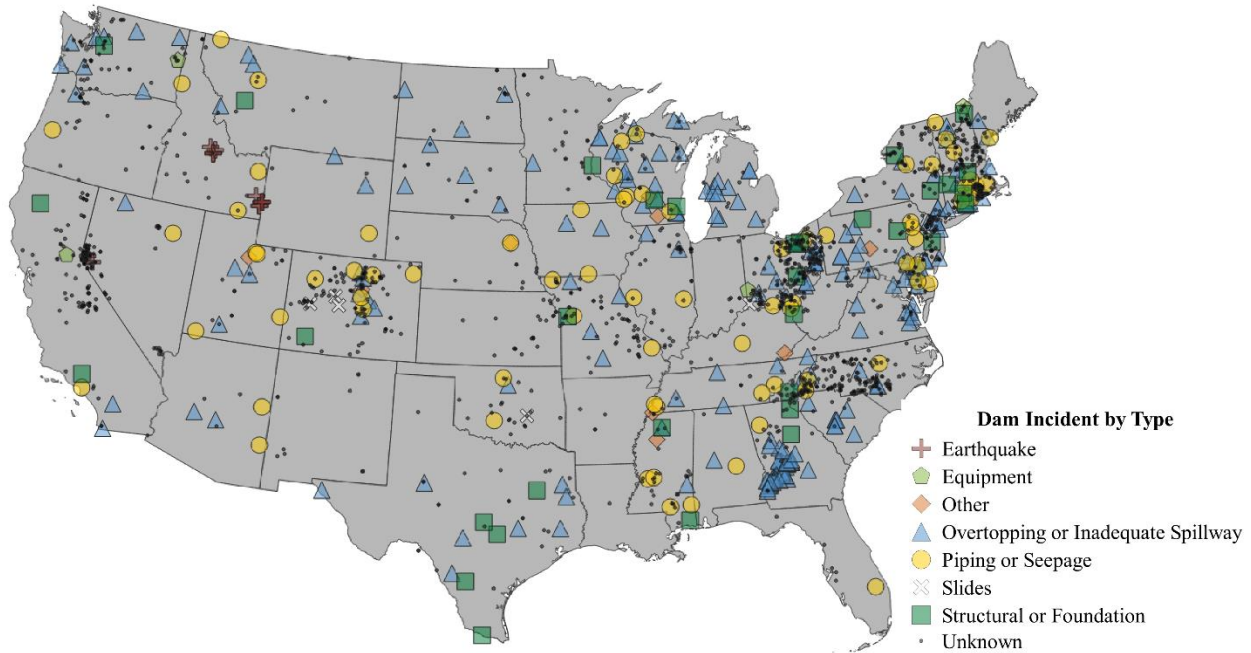
Figure 8. Dam incidents in CONUS by type based on NPDP data.[9]

Table 3. Frequency of historical data failures as reported in the literature.

Region	Reference	Number of failures	Dam-years (in thousands)	Failure rate
US	Gruner 1963, 1967	33	71	5×10^{-4}
	Babb and Mermel 1968	12	43	3×10^{-4}
	USCOLD 1975	74	113	7×10^{-4}
	Mark and Stuart-Alexander 1977	1	4.5	2×10^{-4}
World	Mark and Stuart-Alexander 1977	125	300	4×10^{-4}
	Middlebrooks 1953	9	47	2×10^{-4}
Japan	Takase 1967	1046	30,000	4×10^{-5}
Spain	Gruner 1967	150	235	6×10^{-4}
Average				4×10^{-4}

2.6 DAM FAILURE CONSEQUENCES

Dam failures can pose significant risk to human life and can have significant environmental and financial impacts. According to NPDP,[9] the 1976 failure of Teton Dam resulted in 11 fatalities and a total economic loss of $900 million. In addition to other notable failure events, the Teton Dam failure spurred the US federal government to enact measures to bolster dam safety. To quantitatively assess dam failure consequences and portray risk, some organizations use an FN (frequency-severity) chart (Figure 9), which plots risk exceedance probability against consequences (typically life loss or economic cost). The use of FN charts was popularized in *WASH-1400 The Reactor Safety Study* (NRC 1975), although they were used beforehand in the UK (Bedford and Cooke 2001).

Figure 10 shows the geographic distribution of uncontrolled reservoir releases in the NPDP database, including the year of failure and number of total fatalities. The relatively higher number of incidents

involving fatalities since the 1960s (Figure 11) could be attributed to the increased number of dams constructed from the 1950s through the 1970s (see Figure 16 in Section 2.8), shifts in populations, or increased self-reporting to NPDP. Historical rates of fatalities for international and US dam failures are shown in Figure 9. Since 1900 there have been fewer than six fatalities per year, on average, in the US due to dam failures (see Table A-2 in 0APPENDIX A). Note that the historical failures resulting in large losses of life mostly occurred many decades ago.
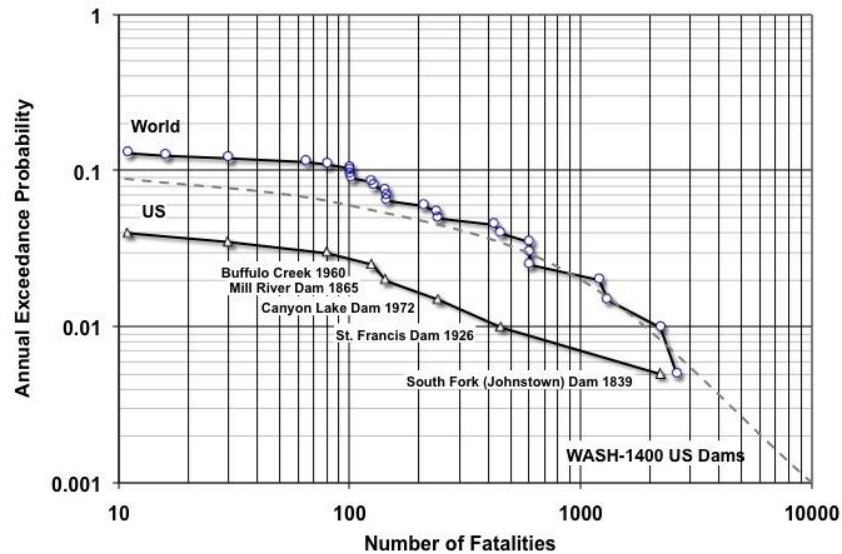
Figure 9. FN chart for fatalities due to historical dam failures in the US and internationally. (Source: Baecher and Christian 2003). Dashed line is the "US Dams" FN curve from *The Reactor Safety Study* [NRC 1975]).
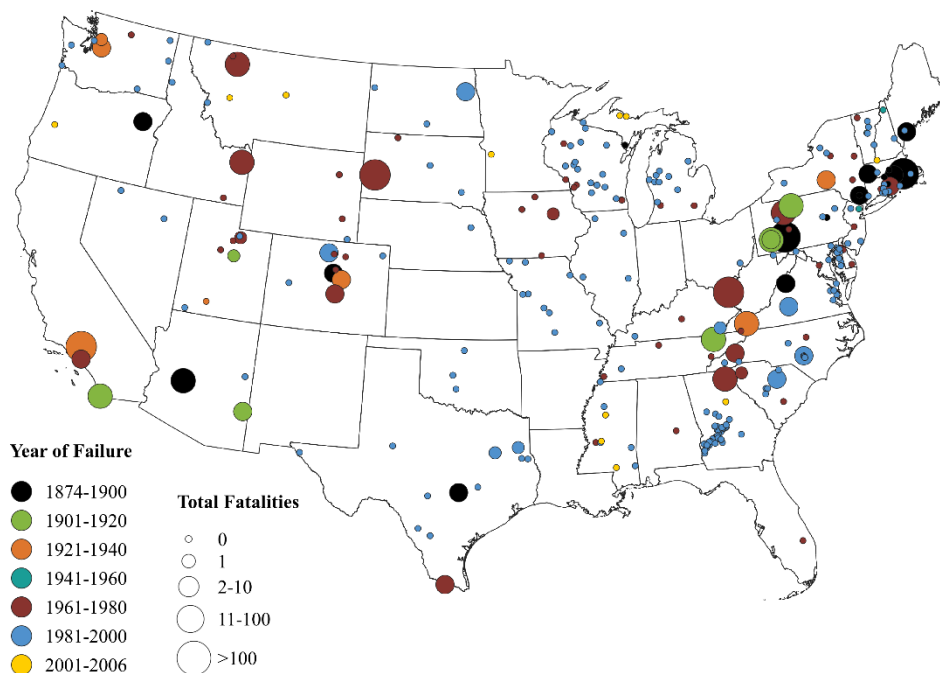
Figure 10. Uncontrolled reservoir releases in CONUS based on NPDP data.[9]
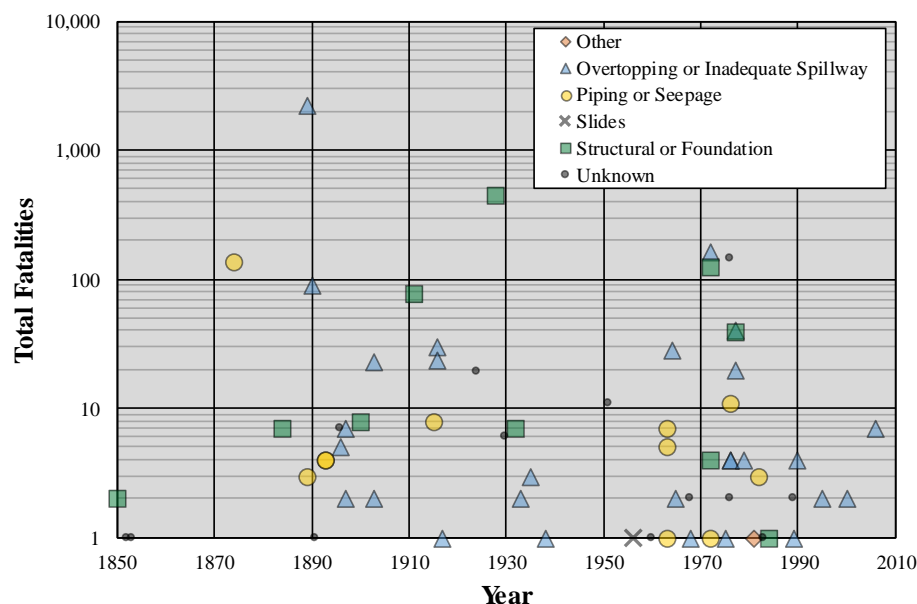
Figure 11. US dam incident fatalities by year and incident type based on NPDP data.[9]

2.7 HAZARD POTENTIAL CLASSIFICATION

US federal agencies have adopted a hazard potential classification system for dams, which was published in the FEMA guidelines for dam safety (FEMA 2004b). This system assigns a high hazard potential to any dam for which failure is expected to lead to one or more fatalities (Table 4). It forces many dams into the high-hazard potential classification even if the probability of failure is low, and even if only one individual is exposed downstream. A dam that was originally constructed in an isolated drainage area may become a high hazard potential if one home is constructed in its floodplain. Figure 12 shows that most dams in the US are classified as having low hazard potential, although more than 15,000 fall into the high–hazard potential category. Figure 13 shows the high-hazard dam count by state, Figure 14 shows the geographic distribution of high-hazard dams across the CONUS based on dam height, and Figure 15 shows the distribution of major dams in the CONUS based on storage.

Table 4. Hazard potential classification system for dams. (Source: FEMA 2004a)

Hazard potential	Loss of human life	Economic, environmental, lifeline losses
Low	None expected	Low and generally limited to owner
Significant	None expected	Yes
High	One or more expected	Yes (but not necessary)
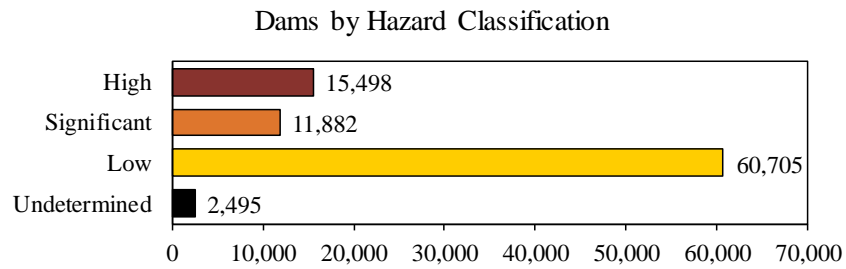
Figure 12. Distribution of US dams by hazard potential based on 2016 NID data.[7]

State	Count
AK*	28
AL	227
AR	191
AZ	171
CA	833
CO	426
CT	443
DE	63
FL	76
GA	597
HI*	124
IA	102
ID	114
IL	231
IN	263
KS	276
KY	275
LA	48
MA	333
MD	79
ME	69
MI	170
MN	55
MO	1,457
MS	298

State	Count
MT	195
NC	1,448
ND	49
NE	143
NH	137
NJ	225
NM	255
NV	154
NY	422
OH	414
OK	431
OR	159
PA	809
RI	96
SC	207
SD	91
TN	274
TX	1,237
UT	242
VA	468
VT	58
WA	240
WI	224
WV	435
WY	97

*not pictured
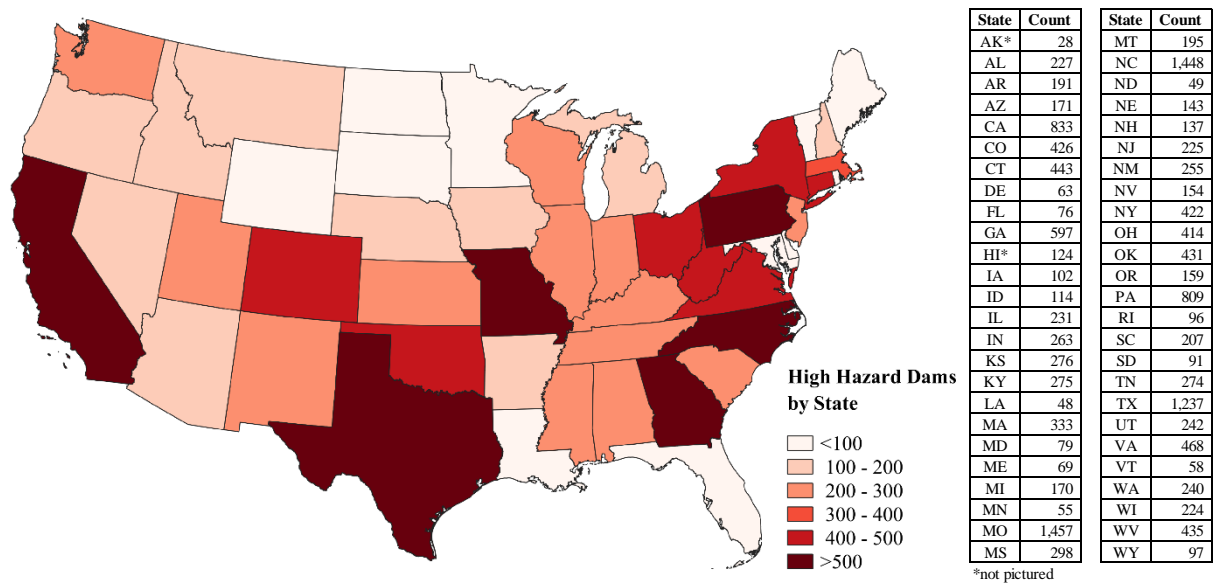
Figure 13. High-hazard dam count in CONUS by state based on 2016 NID data[7].

14
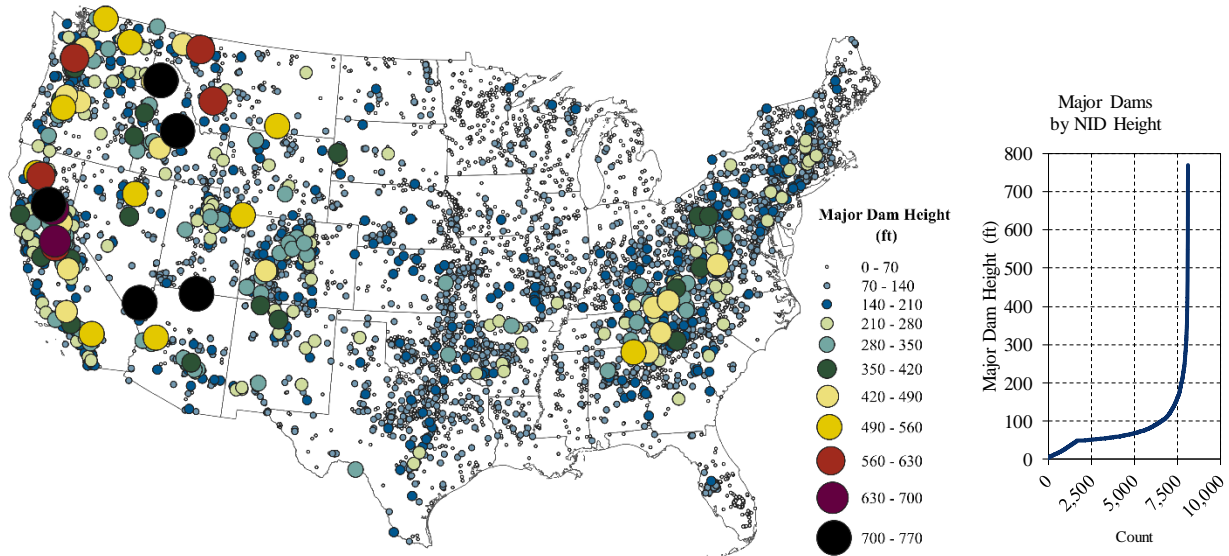
Figure 14. Major dam distribution in CONUS by NID height. (Data from USGS[5])
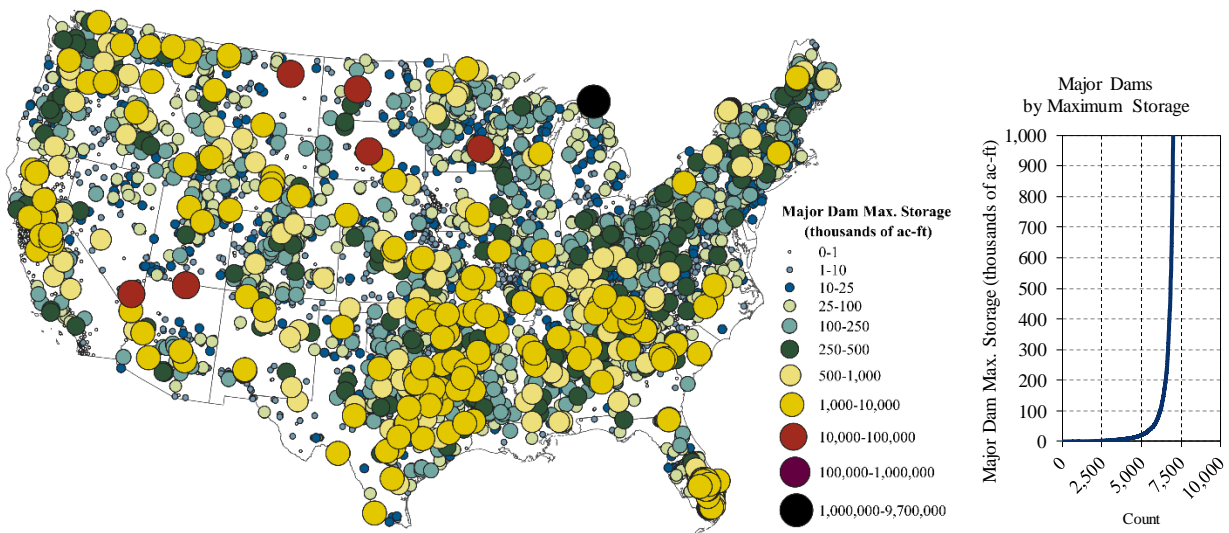
Figure 15. Major dam distribution in CONUS by maximum storage. Note: the distribution curve does not display 243 dams with maximum storage greater than 1 million ac-ft. Dams with a maximum storage value of zero are excluded (893 total). (Data from USGS[5]).[12]

2.8   CONDITION OF US DAMS

Since few single-event hazards (e.g., nuclear disasters and war activities) have the potential for causing more fatalities than dam failures, it is highly important that dams be designed, inspected, and maintained safely (National Research Council 1985). Most of the 90,000+ dams in the US are at least 50 years old; more than 10,000 pre-date World War II and roughly half were built between 1950 and 1979 (Figure 16). Figure 17 shows the average dam age by state; overall, it shows the oldest dams are in the Northeast and

---

[12] Major dams with maximum storage above 1 million ac-ft are not shown in the right-hand plot in Figure 15; they represent about 3% of all major dams in the US.

along the Great Lakes. FEMA (2011) notes that "because the dam infrastructure in the United States is aging, dam failures may increase."
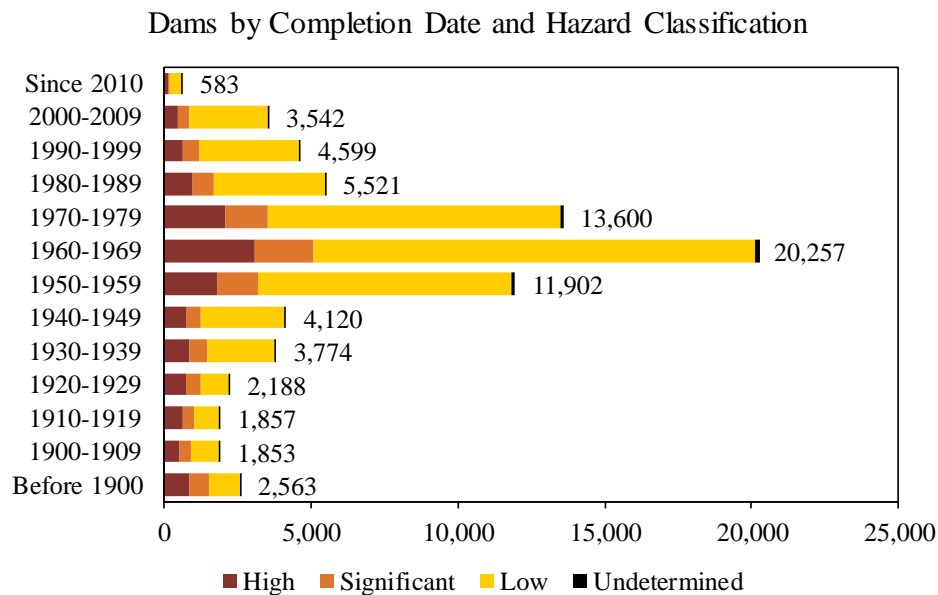
Figure 16. Distribution of US dams by completion date and hazard classification based on 2016 NID data.[7]

State	Count		State	Count
AK*	51		MT	66
AL	52		NC	58
AR	55		ND	51
AZ	62		NE	45
CA	70		NH	88
CO	75		NJ	86
CT	107		NM	54
DE	79		NV	65
FL	49		NY	81
GA	55		OH	58
HI*	85		OK	53
IA	39		OR	60
ID	67		PA	72
IL	54		RI	119
IN	57		SC	61
KS	49		SD	61
KY	52		TN	50
LA	55		TX	60
MA	96		UT	60
MD	54		VA	63
ME	104		VT	83
MI	74		WA	54
MN	57		WI	81
MO	43		WV	53
MS	45		WY	56

*not pictured

Average Dam Age by State (years)
- 30 - 40
- 40 - 50
- 50 - 60
- 60 - 70
- 70 - 80
- 80 - 90
- 90 - 100
- 100 - 110
- 110 - 120
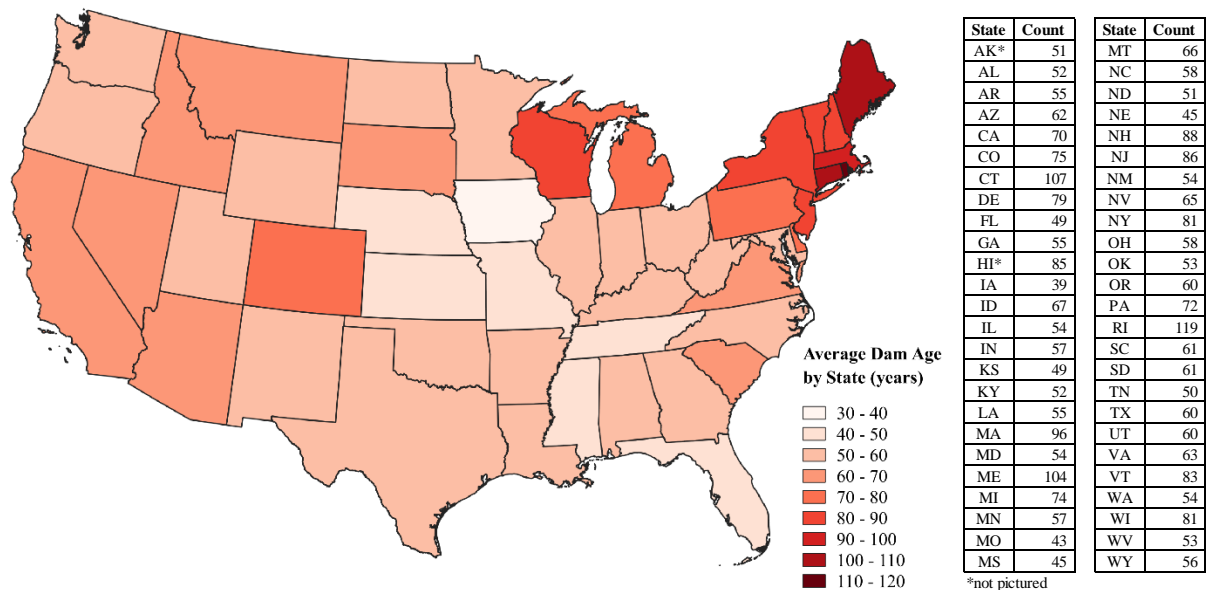
Figure 17. Distribution of dam age in CONUS by state based on 2016 NID data.[7]

Lane (2008) states that "with the exception of seismic or weather events, age is a leading indicator of dam failure." As dams age, material degradation occurs, requiring restoration, retrofits, replacement, repair, or removal of various components and equipment. A dam's structural integrity and operational effectiveness may also deteriorate with age. Human factors, such as delayed or avoided maintenance, outdated or nonexistent EAPs, and a loss of original dam construction knowledge, can contribute to increased dam incident risk. While many dams have been safely operated for well over 100 years, the fact that many

aged dams "are the products of a different generation of design standards and construction practices is generally of greater concern than the aging process itself" (Bowles et al. 1999).

In its *2017 Infrastructure Report Card*,[13] the American Society of Civil Engineers (ASCE) gave US dams a "D" grade.[14] The report indicates that with an average dam age of 56 years, increasing population and development trends, and a lack of investment, the number of high-hazard-potential dams and deficient high-hazard-potential dams continues to climb.

One of the key issues highlighted in the Report Card is that

> many dams are not expected to safely withstand current predictions regarding large floods and earthquakes. For concrete dams, a typical design life is about 50 years. The design life of an earth or rockfill dam is less easily appraised. In addition, many of these dams were initially constructed using less-stringent design criteria for low-hazard potential dams due to the lack of development.

The ASCE estimates that $45 billion in investments would be required to repair aging, high-hazard-potential dams in the US, and ASDSO estimates that $64 billion is needed to rehabilitate the nation's non-federal and federal dams. According to the ASCE infrastructure report,[13] the USACE estimates that more than $25 billion will be required to address dam deficiencies for Corps-owned dams and USBR has estimated that $2 billion is needed to upgrade or repair its high- and significant-hazard dams.

---

[13] Available at https://www.infrastructurereportcard.org/wp-content/uploads/2017/01/Dams-Final.pdf (accessed November 2019)

[14] According to the ASCE *Infrastructure Report Card*, a "D" grade indicates that "The infrastructure is in poor to fair condition and mostly below standard, with many elements approaching the end of their service life. A large portion of the system exhibits significant deterioration. Condition and capacity are of serious concern with strong risk of failure."

3. DAM SAFETY PROGRAMS AND AUTHORITIES

Dam safety programs are mandated at the country level, with guidance provided by international bodies.

After beginning with the NRC regulatory context, Section 3 provides information on federal dam safety coordination (led by FEMA), federal dam owners and operators, federal regulation (by the Federal Energy Regulatory Commission [FERC]), state regulation, international organizations, and international dam safety and regulation.

3.1 NRC REGULATORY CONTEXT

The Nuclear Regulatory Commission has developed regulations regarding the siting and design of NPPs aimed at providing safety from various natural hazards, including flooding. Code of Federal Regulations (CFR) 10 Part 100 addresses siting criteria. CFR 10 Parts 50 and Part 52 address design criteria for NPPs with respect to natural hazards. NRC also has responsibilities related to the safety of uranium milling operations, including impoundments used for management of uranium mill tailings. NRC's regulations address activities in which technical enhancement is achieved (e.g., uranium milling, in situ uranium recovery), whereas uranium mining falls under the purview of state regulators. NRC regulations in 10 CFR 40, Domestic Licensing of Source Material, address the safety of tailings impoundments, which may include dams or embankments.

Nuclear Power Plants

CFR 10 Part 50, Appendix A, General Design Criterion (GDC) 2, "Design bases for protection against natural phenomena," provides the regulatory criterion for protection of (SSCs important to safety against natural phenomena. GDC-2 states that SSCs important to safety must be designed to withstand the effects of natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated. The regulation also states that the design bases shall reflect appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena.

CFR 10 Part 52—more specifically CFR 10 Part 52.17(a)(1)(vi) for early site permits and CFR 10 Part 52.79 (a)(1)(iii) for combined licenses—provides the requirements for new reactor applications as they relate to the hydrologic characteristics of the proposed site. These regulations require consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated.

The requirements to consider physical site characteristics (including hydrologic features) in site evaluations are specified in CFR 10 Part 100.10(c) for applications before January 10, 1997, and CFR 10 Part 100.20(c) for applications on or after January 10, 1997.

Currently, comprehensive and consistent guidance that supports risk-informed decision-making with respect to site-specific assessment of dam failure flooding is lacking. NRC's current regulatory guidance for new reactors for estimating design basis flooding hazards, including those due to dam failure, is contained in Regulatory Guide (RG) 1.59 "Design Basis Floods for Nuclear Power Plants" (NRC 1977, RG-1.59). The standard American National Standards Institute (ANSI) American Nuclear Society (ANS) ANSI/ANS-2.8, *Determining Design Basis Flooding at Nuclear Power Plant Sites* (ANS 1992), has also been used by licensees and NRC for design basis flood estimation at new NPPs. These documents adopt a deterministic, standards-based approach to dam failures and subsequent flooding, employing concepts such as the probable maximum flood (PMF), maximum credible earthquake, and so on. They do not

provide quantitative information useful for risk-informed decision-making, and many of the analytical techniques discussed are outdated.

Although methods used for estimating flooding hazards due to dam failure in new reactor license applications have been largely deterministic, assessments of dam failure likelihood have been used to screen dam failure as a flood-causing mechanism and to assign initiating event frequencies in external event probabilistic risk assessments (PRAs) for operating NPPs. Analyses conducted by the Electric Power Research Institute and NRC in the 1980s developed generic dam failure probabilities based on statistical analyses of reported failures (EPRI 1984; NRC 1987). These were subsequently used by some licensees in their submittals of "Individual Plant Examination of External Events" responses to Supplement 4 to NRC Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities," (NRC 1988).

Subsequent analysis by NRC staff concluded that, although historical dam failure information can provide useful qualitative insight into the generic performance and common failure mechanisms for certain dam types, its applicability to site-specific dam failures must be assessed to establish sufficient technical bases. The reason for this conclusion is the variability in site-specific characteristics (i.e., hydrologic, geologic, structural, and operational) and the potential contributions of site-specific failure mechanisms not considered in generic failure studies (Ferrante et al. 2011; Ferrante et al. 2012). An information notice was issued to licensees summarizing the potential nonconservatism in overreliance on or inappropriate application of generic dam failure probabilities (NRC 2012a).

The NRC-directed post-Fukushima reevaluation of flooding hazards at operating NPPs (NRC 2011; NRC 2012c) generally relies on more recent guidance. NUREG/CR-7046, *Design-Basis Flood Estimation for Site Characterization at Nuclear Power Plants in the United States of America* (NRC 2011), developed to support an update of RG 1.59, discusses modern data sources and analytical techniques for flood hazard assessment but continues to use deterministic approaches. It lacks detailed guidance on assessment of flooding hazards due to dam failure. Interim Staff Guidance JLD-ISG-13-01, *Estimating Flooding Hazards* (NRC 2013), developed to support the post-Fukushima flooding hazards reevaluation, provided more detailed guidance for dam-failure flood-hazard assessment. However, except for estimation of seismic ground motions, it does not adopt probabilistic, risk-informed approaches and methods.

For dams co-located or upstream of NPPs, breach flooding could pose a safety concern. NUREG-0965 (NRC 1983) lists 51 dams associated with NPP sites and 14 uranium mill tailings dams licensed in the US. Although the information contained therein is likely still accurate for co-located and tailings dams, it did not thoroughly evaluate upstream dams for potential cascading failure effects and may have missed some potentially critical upstream dams. NRC work and reviews subsequent to NUREG-0965 (e.g., various non-public post-Fukushima flood hazard assessments) have investigated the broad array of potentially critical dams upstream of NPPs.

Uranium Mill Tailings Impoundments

CFR 10 Part 40, Appendix A," Criteria Relating to the Operation of Uranium Mills and the Disposition of Tailings or Wastes Produced by the Extraction or Concentration of Source Material from Ores Processed Primarily for Their Source Material Content," establishes criteria relating to siting, operation, and long-term performance of surface impoundments and embankments used to manage uranium mill tailings. Regulatory Guide 3.11, *Design, Construction, and Inspection of Embankment Retention Systems at Uranium Recovery Facilities* (NRC 2008), provides more detailed guidance. It asserts that "embankments, foundation, and any abutments need to be stable under all conditions to prevent the uncontrolled release of the retained liquid or semifluid wastes." It recommends using the "latest advances in geotechnical engineering, together with engineering experience and knowledge in the field of water storage dams and retention structures" to inform the design and construction of tailings facilities.

The main function of tailings impoundments is to contain solid material; but water is also present, and the NRC regulatory guidance anticipates that some catchment area (sometimes only the area of the surface impoundment itself) will contribute runoff to a uranium tailings retention system. For tailings retention systems that have some external drainage area and that require hydraulic structures such as diversion channels to safely divert the PMF, the RG states that NUREG-1623, *Design of Erosion Protection for Long-Term Stabilization* (NRC 2002), should be used to determine flood design criteria.

Regulatory Guide-3.11 calls for frequent inspection of tailings retention systems during active operation, with special inspections after the occurrence of significant earthquakes, tornadoes, floods, intense local rainfalls, or other unusual events. Annual technical evaluations, to include assessment of hydraulic and hydrologic capacities, water quality, and structural stability, are also recommended. These inspection and evaluation requirements do not appear to apply to closed tailings impoundments, many of which fall under the jurisdiction of the Department of Energy (DOE) Office of Legacy Management according to the Uranium Mill Tailings Radiation Control Act. However, RG-3.11 notes that NRC implementation of the National Dam Safety Program and its associated guidelines may require special inspections of any uranium recovery site embankments that fall within the scope of the program.

3.2   DAM SAFETY IN THE US

The responsibility for dam safety in the United States resides principally at the state level. Federally owned and operated dams fall under the authorities of the respective federal agencies (i.e., self-regulated). Hydropower dams, including those owned and operated by state governments, are regulated by FERC. According to ASDSO,[15] approximately 70% of US dams are state-regulated, 14% are federally regulated, and the remainder are self-regulated because of state or federal exemptions.

3.2.1   US FEDERAL DAM SAFETY PROGRAMS AND AUTHORITIES

3.2.1.1   National Dam Safety Coordination by FEMA

FEMA, an agency of the US Department of Homeland Security, has lead responsibility for coordinating the federal effort in dam safety and assisting states in improving their dam safety regulatory programs. At the federal level, dam safety programs are organized under the National Dam Safety Program (NDSP). The National Dam Safety Program Act was signed into law on October 12, 1996 as part of the Water Resources Development Act of 1996. The program was established to improve safety around dams by providing assistance grants to state dam safety agencies to assist them in improving their regulatory programs; funding research to enhance technical expertise as dams are built and rehabilitated; establishing training programs for dam safety inspectors; and creating an NID. The act calls for FEMA to provide education to the public, to dam owners, and to others about the need for strong dam safety programs, nationally and locally, and to coordinate partnerships among all players within the dam safety community to enhance dam safety.

Background information on this program is available at the FEMA website.[16] The NDSP is a partnership of the states, federal agencies, and other stakeholders that encourages and promotes the establishment and maintenance of effective federal and state dam safety programs to reduce the risks to human life, property, and the environment from dam related hazards. The NDSP works with its partners to help improve dam safety. It provides financial assistance to state dam safety programs under authority of the biennial Water Resources Reform and Development Act. This includes state assistance grants, training, research, and public safety awareness. Components of the NDSP include the ICODS, which comprises

---

[15] https://damsafety.org/media/faq (accessed November 2019)
[16] https://www.fema.gov/national-dam-safety-program-information (accessed November 2019)

federal agencies having involvement with dams; and the NDSRB, which comprises federal, state, and private sector partners. ICODS is the forum for coordinating federal government activities in dam safety. The NDSRB also monitors the state dam safety programs.

To support dam safety nationally, FEMA coordinates with federal, state and private sector partners through two advisory committees: the National Dam Safety Review Board (NDSRB) and the Inter-agency Committee on Dam Safety (ICODS).

National Dam Safety Review Board

The NDRSB advises the FEMA administrator in setting national dam safety priorities and considers the effects of national policy issues affecting dam safety. It is chaired by FEMA and consists of members representing various federal agencies, state dam safety officials, and the private sector. Table 5 lists the NDSRB member organizations.

Interagency Committee on Dam Safety

The ICODS was founded in 1980 to encourage the establishment and maintenance of effective federal programs, policies and guidelines to enhance dam safety and security. ICODS serves as the permanent forum for the coordination of federal activities in dam safety and security. It is chaired by FEMA and consists of members representing various federal agencies, which are listed in Table 5. Each representative to ICODS has one vote. Each federal agency that serves on ICODS is responsible for reporting biennially to the Congress on its progress in implementing the Federal Guidelines for Dam Safety, as required by Section 11 of the Dam Safety Act of 2006.

Table 5. Member organizations of ICODS and NDSRB.

Interagency Committee on Dam Safety members	National Dam Safety Review Board members
Army Corp of Engineers	Army Corp of Engineers
Bureau of Reclamation	Bureau of Reclamation
Environmental Protection Agency	Federal Emergency Management Agency
Federal Emergency Management Agency	Federal Energy Regulatory Commission
Federal Energy Regulatory Commission	Fish and Wildlife Service
Mine Safety, and Health Administration	Forest Service
Natural Resources Conservation Service	National Park Service
Nuclear Regulatory Commission	National Weather Service
Office of Worker Safety and Health Policy	Natural Resources Conservation Service
Tennessee Valley Authority	Office of Worker Safety and Health Policy
International Boundary and Water Commission	Private sector representatives (3)
	State agencies (2)
	Tennessee Valley Authority

Under FEMA's leadership, state assistance funds have enabled all participating states to better their programs through increased inspections, emergency action planning, and the purchase of needed equipment.

FEMA generates national guidance on dam safety, which was most recently updated in 2015 (FEMA 2004a, 2015). These NDSP guidelines apply to dams that meet the program's definition of a dam (FEMA 2004a) as

> […] any artificial barrier, including appurtenant works, which impounds or diverts water, and which (1) is 25 feet or more in height from the natural bed of the stream or watercourse measured at the downstream toe of the barrier or from the lowest elevation of the outside limit of the barrier if it is not across a stream channel or watercourse, to the

maximum water storage elevation or (2) has an impounding capacity at maximum water storage elevation of 50 acre-feet or more.

Exceptions are made for dams less than 6 ft in height, regardless of storage capacity, and dams with storage capacity of less than 15 ac-ft at maximum water storage elevation, unless there is a "potentially significant downstream hazard" (FEMA 2004a). Treatment of tailings dams differs across agencies. FEMA dam safety guidelines (FEMA 2004a) specifically include tailings dams in their scope. DOE and NRC also include tailings dams in their policies.

The FEMA dam safety program provides many technical guidance documents related to particular dam safety issues. These are accessible online.[17]

FEMA-supported research on dam safety

A national research program in dam safety supported by FEMA[18] focuses on priorities and produces products for both the layperson and the expert and develops technological tools that drive data collection and analysis toward a better understanding of risk and remediation needs. The following are the program components:
- State assistance grants to support state dam safety program
- Training for dam owners and professionals
- Research to address a cross-section of issues in support of dam safety
- Public safety and awareness programs to assist in preparing for, mitigating against, responding to and recovering from incidents

3.2.1.2   Federal Dam Owners and Operators

Eighteen federal agencies or affiliated organizations share responsibility for water resources development, management, regulation, and safety. Several of these either own and operate dams and reservoirs or regulate water and power generation associated with dams. The descriptions that follow are primarily based on information contained in the documents FEMA (2016a) or FEMA (2003).

Department of Agriculture

Dams owned or operated by the USDA are mostly small in height and storage capacity.

The US Forest Service (USFS): USFS hosts 1,745 dams on USFS lands. It owns and operates 499 of these, and the remainder are owned and operated by entities under special use permits or other authorities. Of the dams located on USFS lands, 90% are lower than 50 ft in height, and about 80% have normal reservoir storage of less than 500 ac-ft (FEMA 2016a). These are primarily wildlife, recreation, and fire protection dams.

Natural Resources Conservation Service (NRCS): NRCS is responsible for designing and providing design guidance for water supply and water retention structures across the country. The number of dams designed under NRCS guidance is about 2,480 high-hazard dams, 2,178 significant-hazard potential dams, and 24,497 low-hazard dams, for a total of 29,155 dams (Table 6) (FEMA 2016a). These are mostly privately owned and operated irrigation dams. The NRCS also undertakes research programs in water resources management including dam design.

---

[17] https://www.fema.gov/federal-guidelines-dam-safety (accessed November 2019)
[18] https://www.fema.gov/dam-safety-research (accessed November 2019)

Table 6. Number of dams owned or operated by US federal agencies (FEMA 2003, 2016a).[19]

Department	Agency	Hazard category			
		High	Significant	Low	Total
Agriculture	Agricultural Research Service	1	0	0	1
	NRCS	2,480	2,178	24,497	29,155
	USFS	406	524	884	1,814
Defense	Air Force	0	6	18	24
	Army Installations	33	27	150	210
	Marines	3	2	4	7
	Navy	3	2	12	17
	USACE	511	151	47	709
Energy		2	1	9	12
Interior	Bureau of Indian Affairs	93	43	744	910
	Bureau of Land Management	11	178	700	910
	National Park Service	17	38	450	505
	Office of Surface Mining Reclamation and Enforcement	10	11	48	69
	USBR	239	11	64	314
	US Fish and Wildlife Service	15	2	323	340
	USGS	0	0	1	1
State	International Boundary and Water Commission	3	2	2	7
TVA		75	31	22	128

Department of Defense

USACE owns and operates approximately 709 dams in the CONUS, Alaska, and Puerto Rico; most of these dams are classified as large, of which 511 are high-hazard (Table 6). These structures provide a variety of benefits, including flood risk management, navigation, hydropower, water supply, environmental management, and recreation. USACE has a mature and extensive dam safety program to manage these structures. Along with the USBR, it has pioneered a number of innovative dam safety approaches, including probabilistic risk management.

The uniformed branches of the Department of Defense also control dams on military installations. FEMA (2016a) reports these to consist of 240 Army, 40 Air Force, 17 Navy, and seven Marine Corps dams (Table 6).

Department of Energy

DOE has jurisdiction over 12 water impoundments classified as dams. They are located in Tennessee, Colorado, Georgia, and South Carolina, with two dams rated as high-hazard.

Department of the Interior

Most Department of the Interior agencies own, operate, or have dams and dam safety in their organizational charters.

US Bureau of Reclamation: Through the Reclamation Act of 1902 and subsequent legislation, USBR is authorized to operate as a federal water resource management and development agency in the 17 western states. The USBR inventory currently consists of 474 dams located throughout the West.

---

[19] The numbers provided change over time and are from the cited FEMA references. They are intended to provide an overall picture of dam ownership distribution, rather than an exact measure.

USBR owns and operates 474 dams in those 17 western states with 366 rated as high- or significant-hazard. USBR principally provides irrigation water for agricultural purposes in the western US. Some of the largest hydropower dams in the country (e.g., Hoover Dam, Glen Canyon) are under USBR authority. The USBR was the first of the major federal agencies to develop risk-informed techniques for dam safety studies. USACE has adopted most of the USBR dam safety practices, as have FEMA and FERC. FEMA guidance on dam safety risk management is mostly an evolution of techniques originally developed by USBR in the 1990s (FEMA 2004a).

Bureau of Indian Affairs: The Bureau of Indian Affairs (BIA) is responsible for 910 dams on Indian reservations (of which 136 are high- or significant-hazard). The BIA is responsible for all dams on Indian lands in accordance with the Indian Dam Safety Act of 1994 (Public Law 103-302), but it works with the tribes to maintain dams.

Bureau of Land Management: The Bureau of Land Management (BLM) owns approximately 700 dams on its lands (of which 11 are high-hazard). BLM also maintains an inventory of approximately 544 private dams owned by others but located on BLM lands.

Fish and Wildlife Service: The Fish and Wildlife Service Coordination Act of 1934 (U.S.C. 661-666) grants authority to US Fish and Wildlife Service (USFWS) to operate facilities associated with fish and wildlife conservation. USFWS dams are located on national wildlife refuges, waterfowl production areas, national fish hatcheries and, in some cases, on private land through easement agreements.

National Park Service. The National Park Service (NPS) Dam and Levee Safety Program is responsible for the management of the risks of all dams, levees, and canals that could affect NPS parks.

Department of State

The Department of State, through the International Boundary and Water Commission (IBWC), is responsible for a number of treaties between the US and Mexico. IBWC has jurisdiction over two large international dams on the Rio Grande and Colorado Rivers and four international diversion dams.

The U.S. section of the IBWC is also responsible for the annual maintenance of the American Diversion Dam and five sediment control and flood control dams owned by the Caballo Soil and Water Conservation District., which are not international dams.

Tennessee Valley Authority

TVA is a federally owned corporation organized under the TVA act of 1933, as amended. TVA's mission includes navigation, flood control, electricity generation, and economic development in the Tennessee Valley of KY, TN, GA, AL, and MS. TVA has an inventory of 128 dams, which includes 75 high-hazard dams, 31 significant-hazard dams and 22 low-hazard dams. In addition to flood control dams, TVA operates 30 hydropower dams, some of which date to its earliest years.

3.2.1.3   Federal Regulation

Federal Energy Regulatory Commission

FERC is the principal federal entity responsible for regulating non-federal hydropower dams. It is an outgrowth of the former Federal Power Commission, which became FERC with the DOE Organization Act of 1977. In addition to many other interstate energy transmission responsibilities, FERC is responsible for licensing and inspecting private, municipal, and state hydroelectric projects, including hydropower dams and associated facilities. Thus, dam safety is an essential part of FERC's mission, regulating the planning, construction, and operation of non-federal hydropower dams.

FERC manages the largest dam safety program in the US, regulating 2,525 dams (FEMA 2016a). Of these, 815 are high-hazard, 178 are significant-hazard, and 1,532 are low-hazard. The majority of these are more than 50 years old. Every 5 years, FERC, usually through the agency of an independent consulting engineer, inspects dams higher than 32.8 ft (10 m) or with a storage capacity greater than 2,000 ac-ft (2.5 million m^3). It publishes and maintains the Engineering Guidelines for the Evaluation of Hydropower Projects as guidance for owners and operators. FERC also cooperates with other federal and state agencies to ensure dam safety. Since FERC-regulated project dams are located in seismically active areas, the Commission monitors research activities in the seismic engineering community.

FERC also conducts real-time surveillance and post-event inspections of incidents or events to evaluate the impact on dam safety. For example, during and following large floods, FERC staff visit licensed projects, determine the extent of damage, and make decisions on necessary studies or remedial measures.

FERC requires licensees to prepare EAPs and to conduct training. EAPs include operational procedures, such as reducing reservoir levels and reducing downstream flows, and procedures for notifying affected residents and agencies responsible for emergency management. These plans are periodically updated to ensure that, in emergency situations, cognizant parties know what to do to save lives and minimize damage.

Mine Safety and Health Administration (Department of Labor)

The Mine Safety and Health Administration (MSHA) regulates approximately 1640 dams associated with mining operations, many of which are tailings dams and impoundments.[20] More than 400 of these are high-hazard, meaning that at least one fatality could result from a failure.

Although all dams are inspected for hazards, not every dam at a coal mine requires an approved design plan. Title 30 CFR §77.216[21] states that plans for the design, construction, and maintenance of structures that impound water, sediment, or slurry shall be required if such an existing or proposed impounding structure can impound water, sediment, or slurry to an elevation of 5 ft or more above the upstream toe of the structure and can have a storage volume of 20 ac-feet or more; or impound water, sediment, or slurry to an elevation of 20 ft or more above the upstream toe of the structure.

All impoundments and dams at metal and nonmetal mines are inspected by MSHA for hazardous conditions. Title 30 CFR §56.20010 and §57.20010 state the following: if failure of a water or silt retaining dam will create a hazard, it shall be of substantial construction and inspected at regular intervals. A "hazard" is not restricted to a fatality. Injuries and property damage resulting from a dam failure may constitute a hazard. In addition, flooding resulting from dam failure that could block mine escape could constitute a hazard.

Office of Surface Mining Reclamation and Enforcement (Department of the Interior)

The Office of Surface Mining Reclamation and Enforcement, through a nationwide regulatory program, ensures that coal mining activities are being conducted in a manner that protects citizens and the environment, restores the land to beneficial use following mining, and mitigates the effects of past mining by pursuing reclamation of abandoned mine lands. These duties are performed under the Surface Mining Control and Reclamation Act.

---

[20] https://www.msha.gov/training-education/safety-and-health-materials/safety-topic-impoundments-and-dams (accessed November 2019)

[21] https://arlweb.msha.gov/regs/30cfr/ (accessed November 2019)

3.2.2 US STATE DAM SAFETY PROGRAMS AND AUTHORITIES

Non-federal dams not associated with hydroelectric or mining projects are regulated by state authorities. These include water supply dams, irrigation dams, flood control dams, recreational dams, and others. As discussed in Section 2.4, this represents the majority of dams in the US. All but one of the states have dam safety offices or agencies, the only exception being Alabama. However, except for certain populous western states (e.g., CA, WA, CO, TX) most state dam safety offices are relatively small.

ASDSO[22] is an important nonprofit organization representing state dam safety programs across the US and serves

> state dam safety programs and the broader dam safety community, which includes federal dam safety professionals, dam owners and operators, engineering consultants, emergency managers, manufacturers, suppliers, academia, contractors, and others interested in improving dam safety.[23]

In furtherance of its goal of expanding the technical expertise of dam safety practitioners, ASDSO holds an annual technical meeting, develops guidance documents, provides training workshops, and represents its members in Washington DC. ASDSO maintains a Dam Safety Resource Database with more than 12,000 dam safety-related works representative of "federal and state departments, professional societies, research groups, industry news outlets, international organizations and universities."[24]

FEMA provides model state dam safety program guidance for the states through the NDSP (FEMA 2007), as discussed in Section 3.2.1. This guidance includes information on model legislation, permitting, inspections and enforcement, emergency response, staffing, and public relations planning. FEMA also provides a broad selection of technical and policy guidance documents to support state offices of dam safety. The guidance is not intended to establish technical standards to supplant or to conflict with state and local government responsibilities for the safety of dams under their respective jurisdictions. The FEMA federal guidelines for dam safety are summarized in FEMA (2004a).

3.3 INTERNATIONAL DAM SAFETY

The international dam safety community is highly active and cooperative. At the international level, the principal coordinating entity is ICOLD. Each member nation of ICOLD has a national member committee. The member committee in the US is the United States Society on Dams (USSD) and in Canada is the Canadian Dam Association (CDA). There is no intergovernmental organization, other than the private sector ICOLD, which has dam safety as part of its portfolio.

3.3.1 International Dam Safety Organizations

International Committee on Large Dams

The main platform for interaction among national dam safety organizations is ICOLD, an international organization with the explicit purpose of sharing technical information on the design and operation of large dams; it has no regulatory authority or governmental responsibilities. Its original founding in 1928 in Paris had the goal of fostering dam safety, and that remains its principal purpose. It consists of 100

---

[22] https://damsafety.org (accessed November 2019)
[23] https://damsafety.org/about (accessed November 2019)
[24] https://damsafety.org/references/search?_zs=q0q2g1&_zl=D8Qe5 (accessed November 2019)

national member organizations, of which the USSD[25] is the US national member society. Like ASDSO, USSD holds annual technical meetings, provides guidance and training to its members, and serves as an important clearinghouse for dam safety technology. USSD is purely a private professional organization and has no regulatory authority or governmental responsibilities. The CDA and the British Dam Society are the corresponding national members for Canada and the United Kingdom (UK), respectively.

ICOLD develops and communicates technical bulletins on a variety of engineering and management subjects. It also maintains a World Register of [large] Dams, cataloging all international dams greater than 15 m in height and 500 m in crest length. Among the important bulletins of ICOLD with respect to dam safety risk are its inventory of dam failures:

- Lessons from Dam Incidents
- Bulletin 59 Dam Safety—Guidelines (ICOLD 1987)
- Bulletin 74 Tailings Dams Safety—Guidelines
- Bulletin 99 Dam Failures—Statistical Analysis
- Bulletin 130 Risk Assessment in Dam Safety Management (now in revision) (ICOLD 2005)
- Bulletin 154 Dam Safety Management: Operational phase of the dam life cycle
- Bulletin 170 Flood Evaluation and Dam Safety

The ICOLD European Club (ICOLD European Club 2012) has provided a report on dam safety across Europe. This group does not have regulatory standing but is instead a trade organization intending to improve communication and cooperation among its participating European ICOLD national member organizations (Italy, Norway, Portugal, Slovenia, Spain, and Sweden). The working group has also provided a survey of European dam safety legislation (ICOLD European Club 2007).

Centre for Energy Advancement through Technological Innovation

The Centre for Energy Advancement through Technological Innovation (CEATI) is a private, not-for-profit professional and research entity that operates a number of technical interest groups for the hydropower industry. Relevant among these is the Dam Safety Interest Group (DSIG). The DSIG comprises dam owners who jointly sponsor research and development projects designed to assess and improve the safety of dams. The DSIG includes participants from Canada, the US, Australia, New Zealand, Sweden, France, the UK, and Germany.

3.3.2   International Dam Safety and Regulation

Most nations have dam safety regulations. Surveys of these are in part provided by Bradlow et al. (2002), ICOLD European Club (2007), and ICOLD European Club (2017). The following material is a selection of the more prominent national regulatory frameworks and enabling legislation.

Australia-New Zealand

The Australia-New Zealand Committee on Large Dams (ANCOLD) has been particularly active and progressive in the use of quantitative risk analysis for dam safety and in the development of tolerable risk guidelines (McDonald 1995). Much of the technical thinking behind these guidelines was developed in reaction to the work of the UK Health and Safety Executive (HSE 2001), which led to the development of comprehensive provincial guidelines on dam safety risk and its regulation (ANCOLD 2003). The ANCOLD guidance was a strong influencing factor on the later development of risk guidelines by USBR and USACE (2017).

---

[25] https://www.ussdams.org/ (accessed November 2019)

Austria

Under the Austrian Federal Water Law, the dam owner has responsibility for dam safety. The dam owner must appoint qualified civil engineers with sufficient authority to oversee dam safety.

Dams taller than 30 m or retaining a volume of water greater than 500,000 m^3, dams on the Danube River, and dams that affect water affairs in other countries are subject to the jurisdiction of the Supreme Water Authority of the Federal Ministry of Agriculture and Forestry (FMAF). Other dams are subject to provincial regulation. The FMAF has a Federal Dam Supervisory Section (FDSS), which examines the dam owner's annual safety reports and carries out inspections. The FDSS is assisted by the Austrian Commission on Dams (the national member organization of ICOLD), which provides background information to the FDSS and passes judgment on the safety of dams.

Canada

There are more than 14,000 dams in Canada, with approximately 1,000 categorized as "large" dams and registered with ICOLD. Dams in Canada are owned by federal or provincial governments, utilities, municipalities, industrial and mining companies, irrigation districts, non-government organizations and private individuals. Detailed lists of links to the Canadian regulatory framework are available online.[26]

Canada has no federal regulatory agency, such as FERC, or overarching dam safety program analogous to that coordinated by FEMA in the US. Instead, dam safety regulation is mainly a provincial (or territorial) responsibility. Specific dam safety regulations exist in British Columbia, Alberta, Ontario, and Quebec. Other provinces and territories rely on water resources legislation. However, the federal government does regulate some aspects of dam safety, such as dams constructed in navigable waters and dams located on boundary waters with the US. The federal government manages its own dams (e.g. Parks Canada, Public Works Canada), which are exempt from provincial regulation. Dams associated with nuclear power facilities and uranium mines are regulated by the Canadian Nuclear Safety Commission (CNSC).

The CNSC, the Canadian equivalent of the US NRC, regulates and licenses all operating and future uranium mining and milling operations in Canada (CNSC 2015). CNSC also regulates dams associated with NPPs. Thus, it plays a larger role in uranium mining operations in Canada than the NRC plays in the US. Surface exploration for uranium is exempt from Nuclear Safety and Control Act requirements because the risks are low; instead, each province or territory is responsible for regulating and monitoring exploration activities. The CNSC regulates uranium tailings dams, with a total of 17 aboveground tailings pond dams located at operating and decommissioned sites in Saskatchewan and Ontario. The CNSC reviewed tailing dams at these sites following the 2014 breach of the Mount Polley copper/gold mine tailings dam, which released 25 million m^3 of contaminated water and tailings into nearby waterbodies. During the review, CNSC staff confirmed the safe design of their regulated dams based on the following activities:

• Directed licensees to reevaluate hazards based on present day guidance and methods defining the design basis; licensees concluded that their tailings management areas are operating as designed and that their dams are safe.

• Performed a detailed technical review of the Mount Polley report and confirmed that uranium tailings dams are protected from similar modes of dam failure.

---

[26] Available at https://www.cda.ca/EN/Dams_in_Canada/Regulation/EN/Dams_In_Canada_Pages/Regulation.aspx (accessed November 2019).

- Reviewed all dam safety assessments and confirmed that all uranium mine tailings dams and their associated structures are in good condition and are safe.

- Carried out focused geotechnical inspections of all dam structures and confirmed site conditions, in addition to carrying out baseline compliance geotechnical inspections.

- Carried out a systematic review of CNSC regulations and guidance on dam safety and identified no immediate regulatory actions necessary to provide additional protection.

Like the USSD, the CDA represents dam owners and operators across Canada. The largest and most active of these member organizations are the provincial hydropower authorities. The most active of these with respect to risk analysis for dam safety are British Columbia Hydro and Power Authority (BC Hydro), Ontario Power Generation (OPG), Hydro-Québec, Newfoundland and Labrador Hydro, and Manitoba Hydro. The provinces of Alberta and Saskatchewan are less dependent on hydropower than the other provinces and therefore are less active in risk analysis for dam safety.

European Union

There is no European Union regulatory guidance on dam safety.

Spain

Spain has an active dam safety interest. The pertinent regulation is the "Basic Guideline for Civil Protection Against Risk of Flooding," established in 1994. Under this guidance, dams are classified into three risk categories and the need for EAPs is specified. Spain has three dam safety regulations:

- In 1967, the "Instruction for the Project, Construction and Operation of Large Dams" was established, which applies to large dams of private owners, higher than 15 m or between 10 and 15 m if the stored volume is greater than 100,000 m^3.

- In 1996, the "Technical Regulation About Safety of Dams and Reservoirs" was established, which applies to large state-owned dams.

- The Amendment of the Public Water Regulation, which includes the need for developing Safety Technical Standards that, once approved, will be the only applicable regulations on dam safety.

In all cases, the dam owner is responsible for dam safety. As complements, eight Technical Guidelines have been developed by the Spanish National Committee on Large Dams (the ICOLD national member organization).

Switzerland

The pertinent regulations in Switzerland fall under the Federal Law Regarding the Supervision of Hydraulic Structures (June 22, 1877, as amended), and the more recent Executive Decree on the Regulation of the Safety of Dams (December 7, 1998; it went into effect January 1, 1999). The latter decree assigns supervisory authority between federal and cantonal authorities. It is applicable to all dams taller than 10 m or dams with a height of at least 5 m and a minimum storage capacity of 50,000 m^3. Other dams that present specific safety concerns can also be subjected to this decree and thereby made subject to its jurisdiction.

The 1998 decree specifies that dam safety decisions be based on structural safety, monitoring, and emergency planning. The construction of new dams and the alteration of existing dams must be approved by the canton. The 1998 decree provides opportunity for public comment in the licensing process. Licenses are granted for a fixed period and renewals depend on a new analysis of the operating and environmental conditions.

United Kingdom

The pertinent regulation in the UK falls under the Reservoirs Act of 1975, which entered into effect on December 1, 1991. This Act applies to raised reservoirs for water with dams holding more than 25,000 m^3 that do not fall under the Mines and Quarries (Tips) Act of 1969. Article 2 of the Act requires each local authority to keep a register of raised reservoirs in its jurisdiction. Local authorities must submit regular reports to the Secretary of State detailing the steps taken to ensure that owners and operators comply with the requirements of the Reservoirs Act.

Pursuant to Article 10 of the Reservoirs Act, owners and operators of a dam must have an independent qualified engineer conduct periodic inspections. Large reservoirs not under the supervision of a construction engineer must be under the supervision of a qualified civil engineer employed to supervise the reservoir and advise the undertakers on safety-related issues.

4. DAM ENGINEERING

Dam construction represents one of humanity's most significant engineering accomplishments. While they range widely in size and structure, dams all serve the same primary purpose of controlling water resources for human and/or environmental benefit. Primary uses and categories of dams may differ (see Section 2.1), yet common themes are found among dam structures, operations, and failures.

- Section 4.1 describes dam structures, highlighting the primary types of dam construction and sub-system structures that affect dam safety.

- Section 4.2 describes common dam failure mechanisms, including overtopping, sliding, overturning, overstressing, internal erosion, and spillway and energy dissipation failures.

4.1 DAM STRUCTURE

Typical dam structures fall into several categories, depending on the engineering material used in construction. Common structures include concrete gravity dams, concrete arch dams, and embankment dams (e.g., earthfill or rockfill). An understanding of the engineering makeup of these structures is important for informing dam safety risk assessment, and an overview of these dam structure types is provided in Sections 4.1.1 through 4.1.3. Additional information on the various types of dams can be found on the USSD website.[27] Figure 18 shows the breakdown of US dams by primary construction type. The overwhelming majority of US dams are of embankment construction (i.e., earthfill or rockfill).

Dams by Primary Construction

Construction	Count
Earthfill	68,627
Concrete	2,780
Other	1,696
Unknown	1,466
Rockfill	1,032
Masonry	758
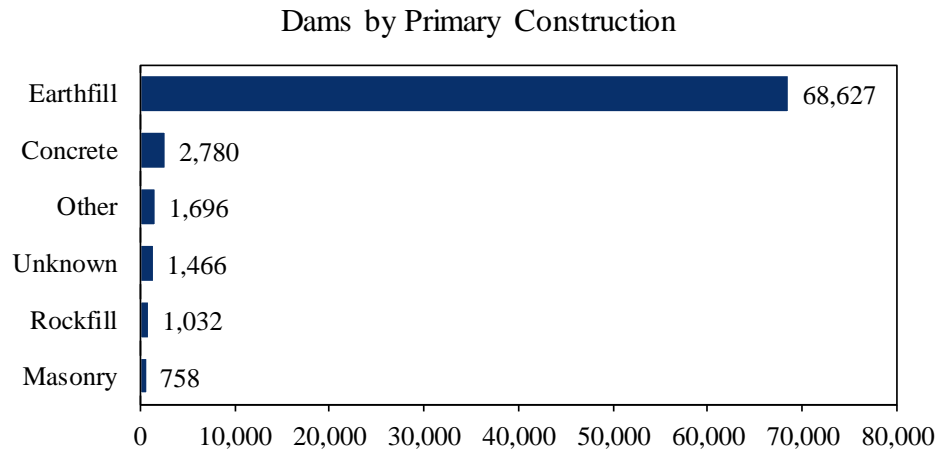
Figure 18. US dam primary construction based on 2016 NID data[7].

In addition to the dam structure itself, specific co-located structures play an important role in dam safety. Among the sub-system structures that most commonly influence dam safety are the powerhouse, spillways, sluiceways, and other outlet works. The components that interact with and comprise these structures require careful design, operation, maintenance, and monitoring. An overview of powerhouse and spillway engineering is provided in Sections 4.1.4 and 4.1.5.

---

[27] https://www.ussdams.org/dam-levee-education/overview/types-of-dams/ (accessed November 2019)

4.1.1 Concrete Gravity Dams

Concrete gravity dams consist of solid concrete. They are often constructed along a straight line or may be slightly curved or angled, depending on site-specific considerations. Gravity dams are well-suited for sites with a reasonably sound rock foundation and offer suitable performance as overflow spillways. Construction of a concrete gravity dam is typically completed using either conventionally placed mass concrete techniques or using roller-compacted concrete (RCC). Compared with conventional methods, RCC construction often permits the use of lower cement content with less heat generation and results in time and cost savings. Once hardened, RCC and conventional concrete exhibit similar properties. (USBR 1987; USACE 1995; FERC 2016)

The loading conditions acting on a concrete gravity dam are maintained through the structure's geometric shape and mass and through material properties of the dam and foundation (USACE 1995). Figure 19 illustrates common loading conditions that impact a concrete dam and foundation.

H1: upstream lateral water pressures
H2: pressure from soil or deposited sediments
H3: ice pressure
H4: loads from floating objects and debris
H5: downstream lateral water pressure
V1: self-weight of dam
V2: weight of water on upstream surface
V3: uplift pressure
V4: weight of water on downstream surface
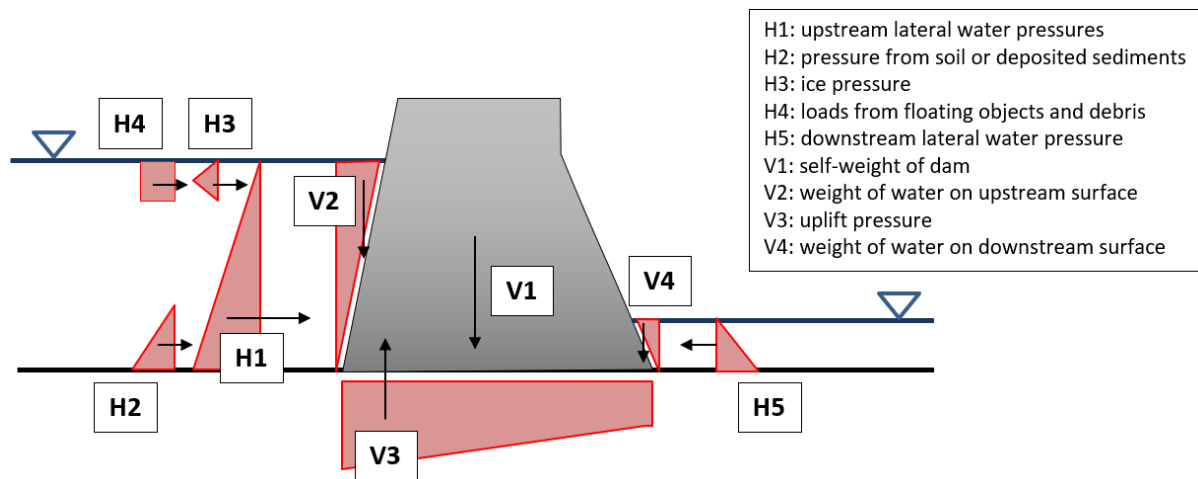
Figure 19. Common vertical and horizontal loads on a concrete gravity dam and foundation. Red triangles represent vertical and horizontal load distributions impacting the dam. [*Source:* Smith et al. (2017); adapted from (ESHA 2004)]

Additional information on design and engineering considerations for concrete gravity dams can be found in USBR (1976), Varshney (1978), USBR (1987), USACE (1995), and FERC (2016), among other references.

4.1.2 Concrete Arch Dams

Concrete arch dams differ from concrete gravity dams primarily in their geometric shape and load transfer characteristics. Unlike gravity dams, which translate loading forces to the foundation gravitationally downward through the base, an arch dam gains extra load transfer through arch action and the resulting outward thrust along the abutments (see Figure 20). Consequently, concrete arch dams are most suitable at sites where abutments have small width-to-height ratios and where the abutment foundation is solid rock capable of resisting the arch thrust. Typical single concrete arch dams have a crest width-to-height ratio of 10:1 or lower; multiple-arch dam designs are also used. (USBR 1987)

Additional information on design and engineering considerations for concrete arch dams can be found in USBR (1977), Varshney (1978), USACE (1994), and FERC (1999), among other references.
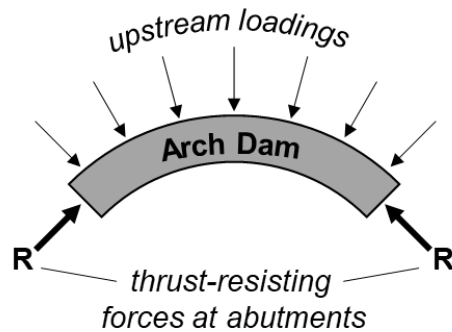
Figure 20. Plan view of arch dam loads and resulting thrust-resistant forces at abutments.

4.1.3   Earthfill and Rockfill Dams

Embankment dams can be either earthfill or rockfill dams or a combination of both (see Figure 21 and Figure 22 for common designs). Earthfill dams represent the most common type of dam in the US (Figure 18), since the use of excavated and locally available natural materials reduces the overall acquisition and construction effort, offering numerous cost savings. Most earthfill dams are (roller) compacted fill, and construction is typically either homogenous, zoned, or zoned with impervious core. Since overflow of earthfill dams quickly leads to erosion and eventual failure, they require appurtenant structures to serve as spillways and outlet works. Filters are often used to safely transmit water through or past the dam while reducing the risk of internal piping erosion. (USBR 1987)

A rockfill dam is a type of embankment dam that comprises primarily compacted rock materials. Watertightness is provided by an impervious zone (i.e., impervious core or membrane on the upstream face; see Figure 22). Impervious cores are usually impervious soils, while impervious membranes may be impervious soil, concrete, asphalt-concrete, metal, or other impervious material. Like earthfill dams, rockfill dams are typically designed to preclude overtopping and subsequent erosion. Foundations must avoid significant settlement to maintain the membrane integrity. Rockfill dams are often found where rock supply is good, high rainfall may complicate earthfill dam construction, or concrete dam construction is too costly. (USBR 1987)

Additional information on design and engineering considerations for earthfill and rockfill dams can be found in USBR (1987), USACE (2004), FERC (2006), and USBR (2012), among other references.

EARTHFILL DAM SECTIONS

a. Homogenous dam with internal drain on impervious foundation

b. Central core, zoned dam on impervious foundation

c. Inclined core, zoned dam on impervious foundation

d. Homogenous dam with internal drainage on pervious foundation

e. Central core, zoned dam on pervious foundation

f. Zoned dam with upstream impervious zone on pervious foundation
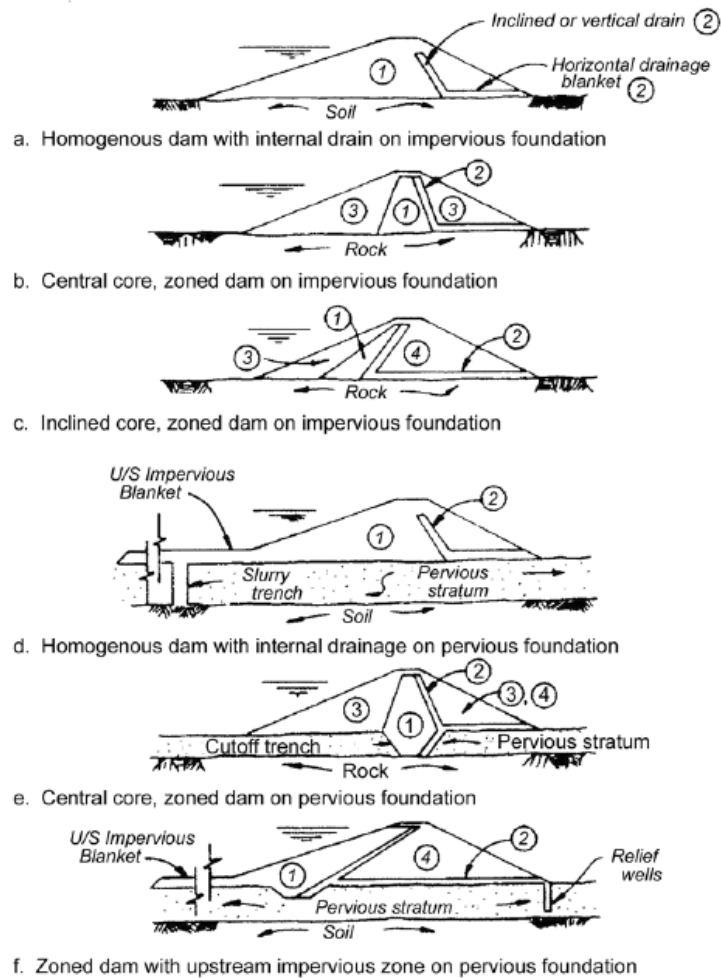
Note: Sections are modified from those presented in Fig. 1-1, EM 1110-2-2300,
Dept. of the Army, Corps of Engineers, May 10, 1982

LEGEND:

① - Zone 1, impervious soil

② - Zone 2, filter drain material (may require a two-stage system
- usually processed sands and gravels)

③ - Zone 3, pervious soil (sands and gravels)

④ - Zone 4, random soil (requires adequate engineering properties,
but plasticity and gradation are less critical considerations)

Figure 21. Common types of earthfill dams. (*Source:* USBR 2012)

34

ROCKFILL DAM SECTIONS

a. Dam with inclined impervious zone

b. Dam with central core

c. Dam with upstream membrane

Note: Sections a. and b. are modified from those presented in Fig. 1-2, EM 1110-2-2300, Dept. of the Army, Corps of Engineers, May 10, 1982. Section c. is modified from Fig. 202, Design of Small Dams, USBR, 1977.

①- Impervious earth fill
②- Filter zone
③- Well graded, selected compacted rock used to provide drainage and bearing support for membrane, and/or transition
④- Smaller sized rock from quarry and rock of lesser quality from foundation excavations, compacted to reduce membrane settlement, and/or provide transition
⑤- Best quality, higher strength rock, compacted to provide section stability

Figure 22. Common types of rockfill dams. (*Source:* USBR 2012)

4.1.4 Powerhouse

For hydropower dams, powerhouses (used to house the hydroelectric machinery and accessory equipment) are typically located at the toe of the dam or at the downstream end of a diversion structure. To prevent large debris or other foreign objects from entering the water conveyance system and potentially damaging flow control or mechanical equipment, a trash rack and control gate are typically placed at the intake. Figure 23 shows a typical layout for a hydropower project co-located with a dam. Many variations of this layout can be found across the US, with arrangements deviating according to site-specific conditions, dam makeup, and project objectives. (USBR 1987)
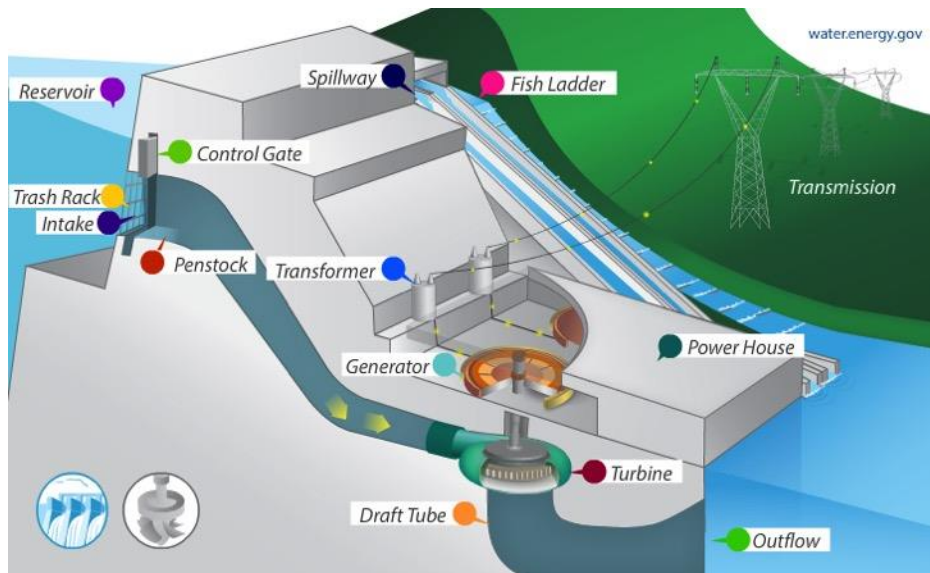
Figure 23. Major components of a hydropower plant. (*Source:* US DOE)

The operation and integrity of the powerhouse equipment and water conveyance system are essential for dam safety and reservoir management. During flood periods, powerhouses are often used to capacity, with additional water often spilled via a spillway or other bypass. In the case of a power outage, hydropower units equipped with induction generators must be shut down to prevent "freewheel" (i.e., excessive and potentially damaging high rotational speed), thus eliminating flow availability through the turbines. Units equipped with synchronous generators may be designed to continue operating even when grid connection is unavailable.

If flooding occurs during equipment maintenance periods or if operability is limited (e.g., from unplanned outages or equipment malfunction), adverse flow conditions and flow control may result. In addition, rapid drawdown of the headwater through hydropower operations or through flood prevention procedures can alter structural loading conditions on the dam. Thus, clearly defined hydropower and extreme event operational procedures are needed to ensure safe and reliable energy production without jeopardizing dam safety.

4.1.5   Spillways

For many dam applications, a spillway is used to safely transport non-generating flows over, around, or through a dam. Operationally, spillways and other flow control devices are used to alter flow conditions to meet desired current and future hydraulic characteristics. A desire to meet these operational conditions may be motivated by various purposes, including flood control, hydropower, navigation, recreation, and water supply. To safely pass excess flows, many dams are equipped with gated or non-gated spillways that can safely pass a sizable volume of water; and they are often constructed of concrete or another non-erosive material (Shams-Ghahfarokhi 2014). Such spillways and gates are also subject to failure or misoperation and may incur flow rates exceeding design conditions, as some devices were originally designed based on rare but not extreme flood conditions.

Spillways may be uncontrolled or controlled depending on whether gates or temporary structures are used. Controlled spillways are equipped with various control structures, which may include gates, bulkheads, or stoplogs and their associated operating equipment. Water conveyance via the spillway may be accomplished using a chute, conduit, or tunnel or a combination of multiple features, with the

arrangement largely determined based on geologic, topographic, or operational considerations (FERC 2015). Figure 24 shows a typical spillway layout.

Spillways are broadly classified as either service, auxiliary, or emergency spillways (USBR 2014).

- *Service spillways* provide continuous or frequent controlled or uncontrolled releases from a reservoir. Most service spillways are made from cast-in-place reinforced concrete and may include riprap channels to prevent erosion. Since they are used on a regular basis, service spillways are designed as erosion- and damage-resistant structures and may come in various forms, including gated, morning glory, or stepped spillways.

- *Auxiliary spillways* are used infrequently and may and may serve as secondary spillways to increase spilling discharge capacity. Since they are economically designed to be used infrequently, auxiliary spillways may incur some structural or erosion damage from discharges up to and including the maximum design discharge. Typical designs include cast-in-place reinforced concrete, riprap channel protection, or unarmored excavated channels.

- *Emergency spillways* offer additional dam-overtopping protection and are designed for use under extreme or unusual conditions such as service spillway or outlet work misoperation or malfunction, flooding, or other emergency situations. Like service spillways, emergency spillways may incur some structural or erosion damage from releases and may be constructed from concrete, riprap, or unarmored material. Emergency spillways are the least robust and erosion-resistant spillway structure.
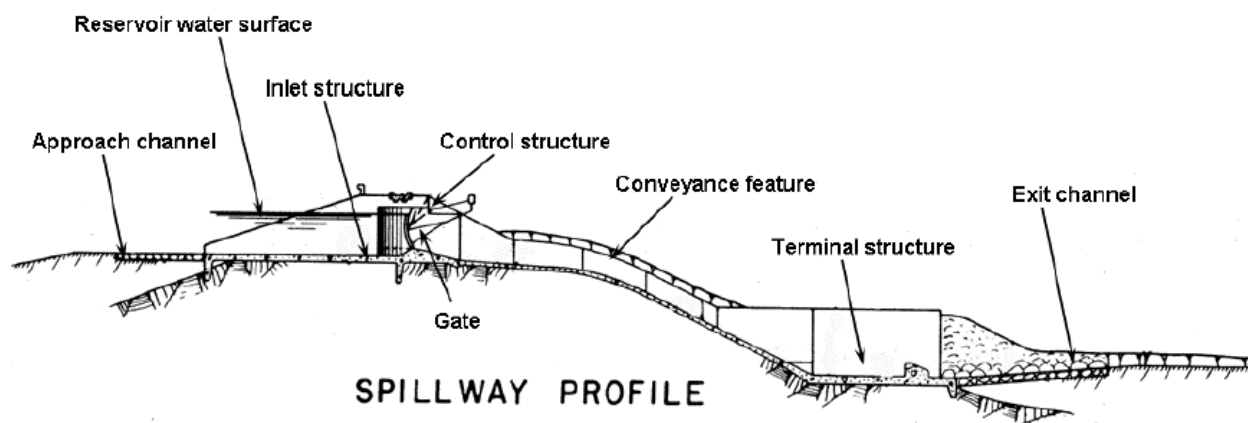
Figure 24. Common spillway design features. (*Source:* USBR 2014)

The hydraulic design requirements specified for a spillway reflect the inflow design flood (IDF). Depending on a dam's hazard classification, the IDF may be equal to or below the PMF; hazard classification–based IDF requirements vary among different federal and state agencies. In addition, since many dams were constructed using different information or technologies from those currently available, existing dams may fail to meet current regulatory IDF requirements. In many cases, guidelines and regulations often require less stringent design criteria for dams built before a certain date, a practice which FEMA (2013) suggests should be discontinued.

In addition, discharge capacity can vary over time as various physical processes limit flow control. For instance, reservoir debris or spillway blockage can limit discharge capacity over time; such conditions commonly occur following flood events (USBR and USACE 2017, Chapter IV-2). For hydropower dams,

releases via powerhouse discharge may be limited because of equipment maintenance, power failure, or operational constraints.

While spillway, powerhouse, and other outlet work capacities can vary widely based on hydrology, layout, and operational objective, many dams require significant spillway capacities to accommodate IDF flows (ranging from the 100-year flood to PMF, according to FERC [2015]). These spillway capacities are often much larger than the combined powerhouse and outlet work capacity, though designs vary considerably. For instance, Grand Coulee Dam (the largest hydropower project by generating capacity in the US) can accommodate 1,000,000 cfs through its spillway, 192,000 cfs through its outlet works, and 273,000 cfs through its power plants.[28] Fort Peck Dam (the largest hydraulically filled dam in the US) can accommodate 275,000 cfs through its spillway, 50,000 cfs through its bypass conduits, and 15,000 cfs through its power plants.[29]

4.2 DAM FAILURE MECHANISMS

Dams are designed to withstand a wide variety of environmental loading conditions. When these design loads are exceeded or when unforeseen events or combinations of events occur, the dam structure may fail. Typical dam design includes engineering to prevent failure from multiple mechanisms, including overtopping, internal erosion, sliding, overturning, overstressing, spillway and energy dissipation issues, and other mechanisms. These processes are described in more detail in the following subsections. Several historical dam failure events are noted, with some selected events described in more detail in Appendix A.

An important consideration for dam safety risk assessment is that some historical dam failures cannot be attributed to a single failure mechanism and may instead result from a chain of events that lead to failure. As noted in the 2018 Independent Forensic Team (IFT) report on the Oroville Dam spillway incident (IFT 2018),

> there was no single root cause of the Oroville Dam spillway incident, nor was there a simple chain of events that led to the failure of the service spillway chute slab, the subsequent overtopping of the emergency spillway crest structure, and the necessity of the evacuation order. Rather, the incident was caused by a complex interaction of relatively common physical, human, organizational, and industry factors, starting with the design of the project and continuing until the incident.

This complex series of near-failure forcing mechanisms, as described in detail in Appendix B, does not fit cleanly within a traditional dam safety risk assessment framework and would require thorough systems analysis to predict.

4.2.1 Overtopping

Overtopping occurs when water levels upstream of a dam rise above the dam crest. Such increases in water levels result when inflows exceed the design or effective capacity of the operating water conveyance system. Commonly considered causes of overtopping include rain-induced flooding, landslide-induced tsunamis or seiches, upstream dam collapses, or wind-induced wave run-up; reduced outflow capacity can also contribute to rising headwater levels.

---

[28] http://www.crso.info/projects/GCD-1_rev3%20-%20FINAL_er120416.pdf (accessed November 2019)
[29] https://www.nwo.usace.army.mil/Media/Fact-Sheets/Fact-Sheet-Article-View/Article/487625/fort-peck-project-statistics/ (accessed November 2019)

Overtopping poses a particular concern for embankment dams due to erosive action of water flow over the crest and down an embankment slope. Prolonged overtopping can lead to partial or complete failure of the embankment structure, and high flow depths and velocities over the crest will also lead to increased erosion potential. Overtopping erosion can also undermine a concrete dam's foundation, with erosion along abutments being of most concern for concrete dams (Shams-Ghahfarokhi 2014).

The concrete surface itself is less prone to erosion (by abrasion) than are earthen surfaces. A reliable hydrologic hazard analysis is needed to understand the potential range of water levels and overtopping depth and duration that may occur. Recent interest has grown on ways of protecting earth dams from overtopping erosion (FEMA 2014, Hepler et al 2012). These involve such protective measures as placing roller-compacted concrete (RCC) on the downstream face of an earth dam, or cable-tied mats over a geotextile, or simply increasing the durability of rip rap coverings. Vegetation or reinforced turf are also sometimes used, especially for levees or saddle dam sections. Additional information on erosion processes involved in breach modeling is provided in Section 5.6.2 on breach initiation and progression.

Overtopping may also occur via wave action as water levels approach the top-of-structure elevation. The resulting wave overtopping is often quantified as an equivalent discharge per linear foot of the structure and can result in structural erosion or failure. These waves are primarily influenced by wind speed and direction, bathymetry, open water (or fetch) distance, and embankment slopes (USBR and USACE 2017, Chapter IV-2). The USACE Coastal Engineering Manual (USACE 2008) provides calculation approaches for estimating wind-induced wave runup.

The current state of practice with respect to probabilistic analysis of overtopping failures is mature. Overtopping was among the hazards identified in the early National Research Council reports (National Research Council 1983, 1985) and has received considerable research attention in both the hydrological sciences and dam engineering.

Several historical dam failures or incidents have resulted from overtopping. The following are among the most well-known.

South Fork Dam
- Location: Pennsylvania, USA.
- Dam description: 72 ft tall earth and rockfill dam.
- Date of incident: May 31, 1889.
- Incident cause: Flood-induced overtopping of the embankment spillway led to concentrated overtopping flow and erosion, which rapidly failed the dam. The dam had undergone previous repair efforts in which the original design was modified, including significantly reducing the spillway capacity and eliminating the low-level outlet works.
- Consequences: 2,209 fatalities (the largest life loss from any US dam failure) and approximately $17 million in damages (in 1889).
- URL: http://damfailures.org/case-study/south-fork-dam-pennsylvania-1889/

Sella Zerbino Secondary Dam
- Location: Italy.
- Dam description: 46 ft tall concrete gravity dam.
- Date of incident: August 13, 1935.
- Incident cause: Following several hours of very heavy rain, the dam was overtopped, resulting in erosion at the dam toe. Subsequent instability led to a sliding and overturning failure which released nearly 80% of the reservoir storage.
- Consequences: 111 fatalities.

- URL: http://damfailures.org/wp-content/uploads/2015/08/Sella_Zerbino.196122134.pdf

Gibson Dam
- Location: Montana, USA.
- Dam description: 199 ft tall concrete arch dam.
- Date of incident: June 8–9, 1964.
- Incident type: Flood-induced overtopping of the dam, without breach.
- Consequences: No direct fatalities.
- Source: USBR and USACE (2017), Chapter IV-2.

Canyon Lake Dam
- Location: South Dakota, USA.
- Dam description: 20 ft tall earthfill dam.
- Date of incident: June 9–10, 1972.
- Incident type: Flood-induced overtopping of the dam crest and subsequent downstream slope scour led to embankment breach.
- Consequences: 40 fatalities and $5.3 million in damages.
- URL: http://damfailures.org/case-study/canyon-lake-dam-south-dakota-1972/

Laurel Run Dam
- Location: Pennsylvania, USA.
- Dam description: 42 ft tall earthfill dam with rock-lined upstream face and masonry spillway.
- Date of incident: July 20, 1977.
- Incident cause: Flood-induced overtopping of the dam crest and subsequent downstream slope scour led to embankment breach. In 1959, an assessment had found the spillway to be less than half the size desired by the state, yet no upgrades were made.
- Consequences: 40 fatalities and $5.3 million in damages.
- URL: http://damfailures.org/case-study/laurel-run-dam-pennsylvania-1977/

Auburn Cofferdam
- Location: California, USA.
- Dam description: 265 ft tall earth and rockfill cofferdam.
- Date of incident: February 18, 1986.
- Incident type: Flood-induced overtopping of the cofferdam led to erosion, embankment failure, and breach flow. The cofferdam had been completed but had remained in place for about 7 years before the failure event because the main dam's construction had been suspended.
- Consequences: No direct fatalities.
- URL: https://www.usbr.gov/ssle/damsafety/TechDev/DSOTechDev/DSO-14-01.pdf

Taum Sauk Dam
- Location: Missouri, USA.
- Dam description: 90 ft tall rockfill dam (impounding an upper pumped storage reservoir).
- Date of incident: December 14, 2005.
- Incident type: Increasing water levels during pumping operation led to overtopping of the dam crest, erosion, and complete evacuation of the reservoir after the primary water level sensor became detached and recorded incorrect water levels.
- Consequences: No direct fatalities (four injuries) and over $1 billion in damages.
- URL: http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/
- More information: See Appendix B for a detailed description of the event and lessons learned.

Lake Delhi Dam
- Location: Iowa, USA.
- Dam description: 59 ft tall composite dam.
- Date of incident: July 24, 2010.
- Incident type: Flood-induced overtopping of the dam with contributing internal erosion led to failure of the embankment. An inoperable spillway gate also reduced the spill capacity of the dam and contributed to the overtopping.
- Consequences: No direct fatalities and over $1 million in damages.
- URL: http://damfailures.org/case-study/lake-delhi-dam-iowa-2010/

4.2.2   Internal Erosion

Internal erosion represents one of the leading causes of embankment dam failures and can also affect concrete dams (ICOLD 2017). Seepage occurs when water passes through a body of soil and causes internal erosion of soil particles. Piping occurs when soil erosion begins at a seepage exit point and erodes upstream until a pipe or roof is formed through the dam structure. Internal migration (or stoping) occurs when the soil properties in a voided structure can no longer structurally support a pipe or roof and erosion continues because of internal instability. Other internal erosion processes include scour (including concentrated leak erosion and contact erosion) and internal instability (including suffusion). The internal erosion failure process is typically categorized into four phases: (1) initiation, (2) continuation, (3) progression, and (4) breach (USBR and USACE 2017, Chapter IV-4).
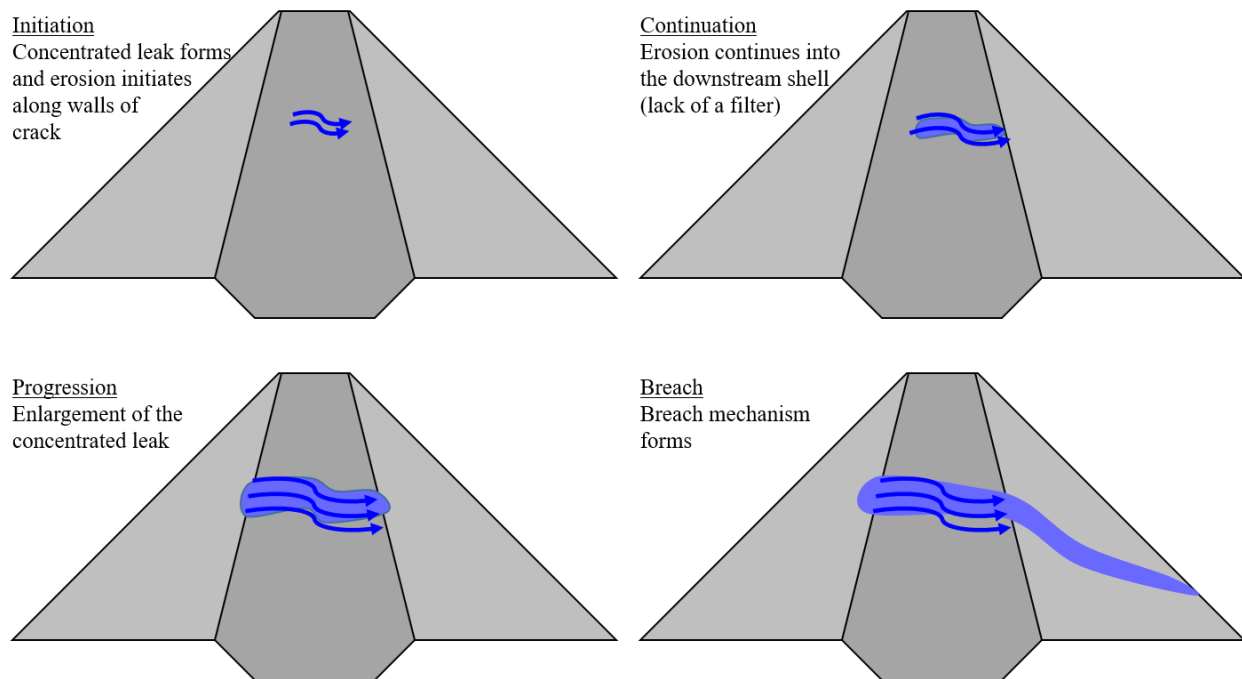
Figure 25. Internal erosion process initiated by a concentrated leak. (*Source*: Adapted from USBR and USACE 2017, Chapter IV-4)

Although seepage and internal erosion are well-recognized and common failure modes, they are often very difficult to predict since practical analytical models are lacking. However, various sources of information on dam embankment and foundation behavior are available to inform risk evaluation. Various design measures aimed at reducing piping risk have been implemented over the years; however, failures and accidents via internal erosion still occur (USBR and USACE 2017, Chapter IV-4).

The current state of practice with respect to probabilistic analysis of internal erosion and piping failures is still a work in progress and is not mature. Furthermore, our scientific and engineering understanding of piping phenomena is poor. The most commonly practiced approaches to internal erosion and piping risk analysis are based fundamentally on the subjective judgment of subject matter experts (ICOLD 2017).

Several historical dam failures or incidents have resulted from internal erosion. The following are among the most well-known.

St. Francis Dam
- Location: California, USA.
- Dam description: 205 ft tall concrete gravity dam.
- Date of incident: March 12–13, 1928.
- Incident cause: Recent investigations identify the failure cause as a weakened, saturated abutment foundation that reactivated an ancient landslide formation. Seepage and uplift forces destabilized the main dam (likely causing overturning and overstressing) and led to rapid dam failure and reservoir release.
- Consequences: At least 432 fatalities and $7 million in damages.
- URL: http://damfailures.org/case-study/st-francis-dam-california-1928/; http://web.mst.edu/~rogersda/st_francis_dam/St-Francis-Dam-for-ASCE-Press.pdf

Baldwin Hills Dam
- Location: California.
- Dam description: 232 ft tall earthfill dam.
- Date of incident: December 14, 1963.
- Incident cause: A crack in the embankment's asphalt liner enabled water penetration and soil erosion beneath it, leading to rapid erosion and a sectional of the dam to collapse.
- Consequences: 5 fatalities and $11 million in damages.
- URL: http://damfailures.org/case-study/baldwin-hills-dam/

Fontenelle Dam
- Location: Wyoming, USA.
- Dam description: 127 ft tall zoned earthfill dam.
- Date of incident: September 3, 1965.
- Incident cause: Seepage through embankment soils at unprotected relief joints led to a fractured foundation and piping downstream of the grout curtain cap. A significant portion of the downstream dam face collapsed, but breach did not occur thanks to rapid reservoir lowering and rock dumping to fill the collapsed dam void.
- Consequences: No direct fatalities.
- URL: http://damfailures.org/case-study/fontenelle-dam/

Lower San Fernando Dam
- Location: California.
- Dam description: 142 ft tall hydraulic earthfill dam.
- Date of incident: February 9, 1971.
- Incident cause: A magnitude 6.6 earthquake struck southern California approximately 6.8 miles from the Upper and Lower San Fernando Dam. While both dams experienced embankment sliding, the lower dam freeboard was reduced from 36 ft to 5 ft following liquefaction and subsequent sliding of the upstream dam slope. The reservoir was drawn down, and dam breach was avoided.
- Consequences: No direct fatalities.

- URL: https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=1624&context=icrageesd

Teton Dam
- Location: Idaho, USA.
- Dam description: 305 ft tall zoned earthfill dam.
- Date of incident: June 5, 1976.
- Incident cause: Hydraulic fracturing and internal erosion during initial reservoir filling likely caused cracking of the dam's impervious core and led to seepage through the downstream dam toe and formation of a sinkhole. Scouring erosion (piping) proceeded quickly and led to the rapid dam failure and reservoir release. The failure was found to stem from similar design and construction flaws as found in the Fontenelle Dam incident.
- Consequences: 11 fatalities and $400 million in damages.
- URL:

Lawn Lake Dam
- Location: Colorado, USA.
- Dam description: 26 ft tall earthfill dam.
- Date of incident: July 15, 1982.
- Incident cause: The dam failed with no warning. A subsequent investigation concluded piping around the outlet pipe was the likely cause of failure. After flowing through steep, mountainous terrain, the breach flow deposited boulders and filled a relatively flat basin before eventually overtopping and causing the cascading failure of Cascade Dam.
- Consequences: 3 fatalities and $31 million in damages.
- URL: http://damfailures.org/case-study/lawn-lake-dam-colorado-1982/

4.2.3 Sliding

As shown in Figure 19, a combination of static and dynamic loads act upon a dam. A well-designed dam will maintain equilibrium under the variety of anticipated design conditions, remaining fixed to the riverbed via adequate foundation and abutment stability and resistive forces. Horizontal "driving" forces resulting from upstream and downstream hydrostatic pressure and from debris, sediment, and ice loadings will (under stable conditions) be balanced by the resistive shear strength of the foundation material and by the frictional forces between the dam and the ground to prevent the dam from moving. Under extreme conditions (including displacement during seismic events), the driving forces may exceed the resisting forces and induce a sliding failure. Uplift pressures along the dam foundation or abutment can reduce resisting forces and contribute to sliding. Often, foundation issues can destabilize the dam and lead to sliding failure. The ratio of the designed resisting forces to the driving forces is considered the sliding factor of safety (Shams-Ghahfarokhi 2014). Sliding failures are equally applicable to both embankment and concrete gravity dams and will occur when the factor of safety decreases to below 1.0 (USBR and USACE 2017, Chapter I-7).

The current state of practice with respect to probabilistic analysis of static sliding failures is mature. The geotechnical and structural strength and deformation of dams have been studied since the early years of modern dam engineering. The dynamic performance of embankment dams, particularly liquefaction behaviors under seismic loading, remains an issue of ongoing research but is also reaching maturity

Several historical dam failures or incidents have resulted from dam sliding. The following are among the most well-known.

Bouzey Dam
- Location: France.
- Dam description: 72 ft tall masonry gravity dam.
- Date of incident: April 27, 1895.
- Incident cause: During initial reservoir filling, significant seepage was observed and was followed by sudden downstream sliding of approximately 1.1 ft. Eleven years later, following repair and reinforcement efforts, the dam failed suddenly via sliding upon second filling.
- Consequences: More than 100 fatalities.
- URL: https://www.usbr.gov/ssle/damsafety/TechDev/DSOTechDev/DSO-98-05.pdf

Austin Dam
- Location: Pennsylvania, USA.
- Dam description: 50 ft tall concrete gravity dam.
- Date of incident: September 30, 1911.
- Incident cause: Multiple faults led to the dam's sliding failure, including poor foundation, design, construction, and operation. The dam had experienced multiple partial failures previously and was still unrepaired when heavy rains contributed to near-overtopping conditions, leakage through and under the dam, and the eventual sudden sliding collapse of a sizable concrete section.
- Consequences: 78 fatalities and approximately $140 million in damages (in 2010 USD).
- URL: http://damfailures.org/case-study/austin-bayless-dam-pennsylvania-1911/

Malpasset Dam
- Location: France.
- Dam description: 218 ft tall concrete arch dam.
- Date of incident: December 2, 1959.
- Incident cause: As initial reservoir filling was nearly complete, the geologic abutment characteristics and increased hydrostatic forces resulted in uplift pressure and a sliding failure of the abutment. Resulting cracks led to rapid failure of the concrete dam, which was designed to minimize the structural thickness.
- Consequences: 421 fatalities.
- URL: http://damfailures.org/case-study/malpasset-dam-france-1959/

Morris Sheppard Dam
- Location: Texas, USA.
- Dam description: 190 ft tall concrete buttress dam.
- Date of incident: December 1986 (observed).
- Incident cause: During a FERC inspection, a portion of the foundation below a hollow spillway section was found to have moved 4.5 inches downstream as a result of sliding, presumably under normal operation. Breach did not occur, and reservoir releases were maintained within the channel capacity.
- Consequences: No direct fatalities.
- URL: https://www.usbr.gov/ssle/damsafety/TechDev/DSOTechDev/DSO-98-05.pdf

Upper Stillwater Dam
- Location: Utah, USA.
- Dam description: 290 ft tall RCC dam.
- Date of incident: Summer 1988.

- Incident cause: During initial reservoir filling, horizontal foundation movement (sliding) was recorded by multiple sensors. Some seepage through cracks and high foundation drain flow occurred, but the dam did not fail.
- Consequences: No direct fatalities.
- URL: https://www.usbr.gov/ssle/damsafety/TechDev/DSOTechDev/DSO-98-05.pdf

Sella Zerbino Secondary Dam
- See Section 4.2.1 for the full event description. Overtopping of the concrete gravity dam resulted in dam toe erosion and a subsequent sliding and overturning failure.

4.2.4 Overturning

Whereas sliding failure occurs from displacement of a dam parallel to the foundation, an overturning failure may occur when overturning moments induced by various driving forces overcome the stabilizing forces (primarily the self-weight of the bulk structure) and cause a rotation of the bulk structure. The overturning moments are often calculated at the dam toe or some other critical joint along the dam body (Shams-Ghahfarokhi 2014). Overturning may be caused by various physical conditions, including insufficient bulk weight or weight distribution, uplift forces from tensile cracking along the dam base, erosion of the dam toe foundation, uplift pressure from inadequate seepage control or pressure relief, and excessive hydrostatic pressures beyond design conditions. As with sliding stability analysis, overturning stability analysis incorporates factor-of-safety calculations to ensure structural stability.

The current state of practice with respect to probabilistic analysis of overturning failures is similar to that of sliding; it is mature.

Several historical dam failures or incidents have resulted from overturning. The following are among the most well-known.

St. Francis Dam
- See Section 4.2.2 for the full event description. Weakening of the dam due to internal erosion along the abutment foundation likely led to overstressing and an overturning failure.

Sella Zerbino Secondary Dam
- See Section 4.2.1 for the full event description. Overtopping of the concrete gravity dam resulted in dam toe erosion and a subsequent sliding and overturning failure.

4.2.5 Overstressing

Overstressing presents a risk for concrete dams and occurs when stresses within the structure, foundation, or other components exceed the material capacity. For instance, under flood conditions, increasing reservoir levels can increase the effective stress in a dam, causing tensile forces to exceed the concrete properties and leading to cracking or instability failure (NRC 2013). Such tensile forces are usually of most concern along joints, foundation blocks, and foundation planes. Finite element analysis is often used to compute internal stresses based on dam construction material, and it is typically assumed that if rigid body analysis reveals tensile stresses at the dam toe, a crack will form and allow full uplift pressure to form via water percolation (Shams-Ghahfarokhi 2014).

The current state of practice with respect to probabilistic analysis of overstressing failures is similar to that of sliding; it is mature.

Several historical dam failures or incidents have resulted from overstressing. The following are among the most well-known.

Pacoima Dam
- Location: California, USA.
- Dam description: 371 ft tall concrete arch dam.
- Date of incident: January 17, 1994.
- Incident cause: A 6.7 magnitude earthquake occurred near Northridge, CA, and resulted in a peak horizontal ground acceleration of 1.6 g, peak vertical ground acceleration of 1.2 g, and peak radial acceleration of 2.3 g, as measured along the left abutment. Pore pressure redistribution was observed from piezometers, with seepage increasing immediately as a result of the earthquake but subsequently reducing. The left abutment shifted horizontally by 16–19 inches and vertically by 3–4 inches, which indicated movement of rock blocks. Tendons near the thrust block were likely elongated and overstressed during the earthquake. Breach did not occur, and minor repairs were made.
- Consequences: No direct fatalities.
- URL: https://www.usbr.gov/ssle/damsafety/TechDev/DSOTechDev/DSO-98-05.pdf

St. Francis Dam
- See Section 4.2.2 for the full event description. Weakening of the dam due to internal erosion along the abutment foundation likely led to overstressing and an overturning failure.

4.2.6   Spillway Failure

As described in Section 4.1.5, spillway discharge capacity is based on the IDF. IDFs are determined based on inflow hydrographs and operational procedures at the dam. Inadequate spillway design or flooding above the IDF can cause spillway failure and lead to further erosion and structural failure (USBR and USACE 2017, Chapter IV-2).

Spillway failures may result from various causes, including gates failing to open, improper gate installation, structural gate failure, spillway debris blockage, hoist failure, improper control operation, seal leakage, or ice formation (Hartford et al. 2016). Spillway channels can also be susceptible to abrasion, and high flows can dislodge material. Degradation of a spillway structure can cause unsafe operation at below-design capacity (e.g., 2017 Oroville spillway incident). Erosion can also occur at the spillway discharge point as the high flow velocity of water exiting a spillway to the lower water body creates a trajectory jet. The jet imparts significant kinetic energy into the tailrace; and energy dissipation design measures to prevent downstream scour are often taken, including the construction of a plunge pool and riprap or lined channels (Shams-Ghahfarokhi 2014).

The current state of practice with respect to probabilistic analysis of spillway hydraulics and spillway gate structures is mature. Spillway hydraulics has been studied for more than a century and is reasonably well understood

Several historical dam failures or incidents have resulted from spillway or energy dissipation problems. The following are among the most well-known.

Folsom Dam
- Location: California, USA.
- Dam description: 340 ft tall composite dam.
- Date of incident: July 17, 1995.

- Incident cause: A spillway gate failed after being opened approximately 2.4 ft with reservoir levels at full capacity. Failure was caused by excessive friction in the trunnion pin, which had not been maintained with appropriate lubricant. Roughly 40% of the reservoir storage was released past the failed gate, which had not been subject to wide opening at high head for nearly 40 years.
- Consequences: No direct fatalities.
- URL: http://damfailures.org/case-study/folsom-dam-california-1995/

Oroville Dam
- Location: California, USA.
- Dam description: 770 ft tall earth and rockfill dam.
- Date of incident: February 2017.
- Incident cause: Following a period of heavy rain that necessitated spillway releases, a portion of the concrete service spillway was damaged and prompted a series of mitigating actions. Eventually, operational decisions led to the project's first use of the earthen emergency spillway, which began to erode with rapid headcutting. The risk of dam breach prompted an evacuation order, but breach was avoided.
- Consequences: No direct fatalities and $1.1 billion in spillway repair.
- Source: IFT (2018).
- More information: See Appendix B for a detailed description of the event and lessons learned.

4.2.7   Other Failure Mechanisms

Dam failures or incidents may result from a variety of other mechanisms that are not fully described in Section 4.2. Operational risk (described in Section 6) and various loads or hazards (described in detail in Section 5.3) can contribute to dam issues, and accounting for them requires proper design and operational procedures to ensure safety.

Beyond the freshwater impoundment dam failure described previously, a few historical uranium mill tailings dam failures have occurred. The most notable (and largest) such event was the Church Rock failure in New Mexico, which released the most radioactive material in US history to that point.[30] On July 16, 1979, a uranium mill tailings disposal pond, which was constructed on a poor geological site, breached and released 1,100 tons of tailings and 94 million gallons of mill and uranium into the Puerco River, affecting Navajo populations living downstream.

---

[30] http://large.stanford.edu/courses/2017/ph241/morris-n1/ (accessed November 2019)

5. DAM SAFETY RISK ASSESSMENT

Risk combines the probability and severity of an adverse event. Kaplan and Garrick (1981) identify a "risk triplet," consisting of three questions used to define risk: (1) What can happen? (2) How likely is it that it will happen? (3) If it does happen, what are the consequences? To answer these questions, both qualitative and quantitative risk assessment approaches may be used, although approaches can vary widely.

Risk analysis for dam safety is often conceptualized by hazard, vulnerability (fragility), and consequences, as visualized in Figure 26. *Hazard* is thought of as a load or initiating event and is characterized in risk analysis by a probability distribution of the magnitudes of the load. For example, the hazard might be an extreme reservoir inflow, an earthquake, or a debris or ice load on a spillway. *Vulnerability* (sometimes called fragility) is the system response to loading and is characterized by a conditional probability of failure. For example, the vulnerability might be the conditional probability of a dam overtopping if a reservoir inflow greater than some discharge occurs, or it might be the conditional probability of a spillway structure failing if earthquake ground shaking greater than some peak acceleration occurs. *Consequences* are what results from a hazard combined with vulnerability, leading to adverse performance of the dam. For example, a certain amount of economic damage might be suffered, or there might be a certain number of fatalities.
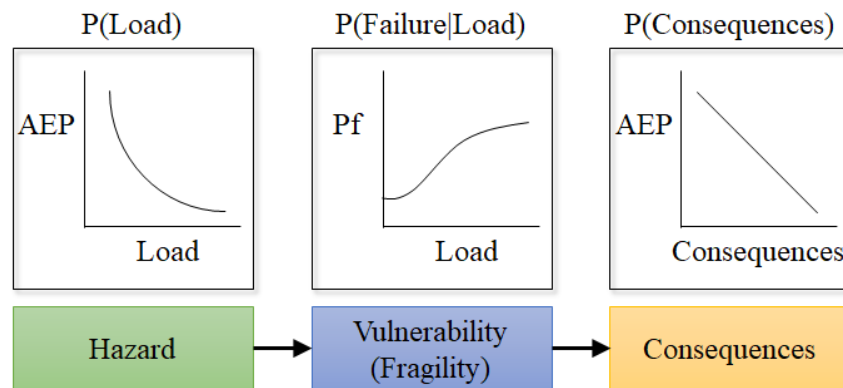
Figure 26. Risk analysis modeling approach. Pf: probability of failure; AEP: annual exceedance probability. (*Source*: Adapted from Baecher 2015)

Risk prediction is both complex and uncertain; and it is widely acknowledged that dam failures often result from a complex series of adverse conditions, flaws, or errors in combination rather than a simple design or construction flaw (Hartford and Baecher 2004; Hartford et al. 2016). The recent February 2017 Oroville Dam spillway incident highlights this concept, as the IFT investigating the incident found "the incident was caused by a complex interaction of relatively common physical, human, organizational, and industry factors" (IFT 2018). The IFT further stated that

> Although the practice of dam safety has certainly improved since the 1970s, the fact that this incident happened to the owner of the tallest dam in the United States, under regulation of a federal agency, with repeated evaluation by reputable outside consultants, in a state with a leading dam safety regulatory program, is a wake-up call for everyone involved in dam safety. Challenging current assumptions on what constitutes "best practice" in our industry is overdue. (IFT 2018)

48

While complexity and uncertainty will continue to be key aspects of dam safety risk assessment, a thorough understanding of the current state-of-practice can provide dam owners, operators, engineers, regulators, and stakeholders with the necessary information to assess the probability and severity of dam safety risks and make risk-informed decisions to ensure public safety and prioritize mitigation solutions.

Section 5 of this report provides an overview of the main features of current dam safety risk assessment practices. Section 6 addresses operational risk considerations and approaches, much of which move beyond traditional dam safety practices yet represent important features for fully characterizing risk and reliability.

5.1 OVERVIEW AND SUMMARY PUBLICATIONS

Like other civil infrastructure, dams are constructed using cost-effective engineering designs and are designed to meet anticipated operational and loading conditions during a selected service life with some factor of safety. Unfortunately, every possible condition cannot be planned for, and the frequency of various conditions cannot always be calculated with high certainty. Over time, dam systems and components deteriorate and require increasing maintenance to maintain performance. To ensure continued safe operation and protect against adverse failure, dams require careful operation, surveillance, and monitoring. Maintaining structural and operational performance is especially important given the long service life (which can often exceed a dam's original design life) to which many dams are subject.

Though federal legislation following the 1976 Teton Dam failure identified a need to develop dam safety risk assessment procedures, the USBR did not start using risk analysis as the primary tool for dam safety decision-making until the mid-1990s. The USACE began implementing risk analysis and risk assessment procedures following the 2005 Hurricane Katrina levee failures.

Traditional dam safety risk assessment follows the Potential Failure Modes Analysis (PFMA) process developed by the FERC, USBR, and USACE (FERC 2017; USBR and USACE 2017). Although PFMAs detail how a dam might fail, they do not directly consider the scope of potential consequences or estimate the likelihood of an adverse event. To accomplish these objectives, dam safety officials and organizations responsible for ensuring dam safety rely upon risk-informed decision-making (RIDM), which builds upon the PFMA process while leveraging PRA approaches. To protect against the risk of failure, various counter measures are taken to reduce the risk to "as low as reasonably practicable" (ALARP).

The importance of RIDM is exemplified in FERC's *Fiscal Year 2014—2018 Strategic Plan* (FERC 2014), which identifies Strategy 1 to "use risk-informed decision making to evaluate dam safety" as a way to address Objective 2.2, "minimize risks to the public associated with FERC-jurisdictional energy infrastructure."

Although RIDM is increasingly being used, much existing dam safety practice has relied upon deterministic, standards-based approaches in which the focus of risk identification is on the dam's physical structure and not its operation, data collection, or communications. This limited purview and a focus on relatively few loading scenarios (e.g., floods, earthquakes, and normal operation) may overlook various critical failure mechanisms that can lead to failure.

Although NRC has not gained wide experience with using PRA for dam safety-related regulation, its "Backgrounder on Probabilistic Risk Assessment"[31] provides a concise summary of PRA and the NRC's use of PRA for complex systems. As it states,

> the NRC's regulation, oversight, and enforcement reduces risk by making a bad event and its corresponding effects less likely. The NRC and the nuclear industry use PRA as one way to evaluate and reduce the overall risk to the public and environment.

The following definitions are important to understanding dam safety risk assessment:

- **Hazard:** "threat; condition, which may result from either an external cause (e.g., earthquake, flood, or human agency) or an internal vulnerability, with the potential to initiate a failure mechanism. A source of potential harm or a situation with a potential to cause loss" (ICOLD 2005).

- **Potential failure mode:** "a way that dam failure can occur (i.e., the full sequence of events from initiation to failure) for a given loading condition" (FEMA 2015).

- **Probability:** "a measure of the likelihood, chance, or degree of belief that a particular outcome or consequence will occur" (USACE 2014a).

- **Statistical probability:** a frequency-based measure of probability that could include the outcomes of a repetitive experiment or population variability (ICOLD 2005). Statistical probability may also be referred to as the frequentist interpretation of probability.

- **Subjective probability:** "quantified measure of belief, judgment, or confidence in the likelihood of an outcome, obtained by considering all available information honestly, fairly, and with a minimum of bias" (ICOLD 2005). Subjective probability may also be referred to as the Bayesian interpretation of probability.

- **Uncertainty:** "the result of imperfect knowledge about the present or future state of a system, event, situation, or population under consideration" (FEMA 2015). Uncertainty is frequently classified into either aleatoric uncertainty (i.e., uncertainty associated with natural variability) or epistemic uncertainty (i.e., uncertainty associated with knowledge limitations).

- **Risk:** "a measure of the probability and severity of an adverse effect to life, health, property, or the environment" (ICOLD 2005).

- **Risk analysis:** "the use of available information to estimate the risk to individuals or populations, property or the environment, from hazards" (ICOLD 2005).

- **Risk assessment:** "the process of making a decision recommendation on whether existing risks are tolerable and present risk measures are adequate, and if not, whether alternative risk reduction measures are justified or will be implemented" (ICOLD 2005).

- **Risk-informed decision-making:** decision-making that is "made considering risk estimates and many other contributing factors that might include confidence in the risk estimates, risk uncertainty,

---

[31] https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/probabilistic-risk-asses.html (accessed November 2019)

deterministic analyses, and the overall dam safety case in addition to other local or regional considerations" (FEMA 2015).

- **Risk management:** "the systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, assessing, mitigating and monitoring risk" (ICOLD 2005).

- **Consequences:** "in relation to risk analysis, the outcome or result of a risk being realized. Impacts in the downstream, as well as other, areas resulting from failure of the dam or its appurtenances" (ICOLD 2005).

Figure 27 provides an illustration of the relationships among risk analysis, assessment, and management. Figure 28 illustrates the risk assessment framework, which involves sequential modeling of initiating events, system responses, outcomes, exposure factors, and consequences (see vertical columns). As illustrated in the framework, dam performance PRA involves risk identification, risk estimation, risk evaluation, and risk treatment (see horizontal rows in Figure 28).

Initiating events to consider include both external (e.g., flooding or other loads and hazards discussed in Section 5.3) and internal events (e.g., piping or other failure mechanisms discussed in Section 4.2). Per Bowles and Schaefer (2014),

> each external initiating event is divided into a number of loading intervals to characterize a range of loading magnitudes to achieve numerical precision in the risk analysis calculations. Several sub-steps may be necessary to adequately characterize the system response to a range of magnitudes of initiating events that can lead to the outcome of dam failure or no failure. Various types of consequences of dam failure may be considered

such as economic, financial, life loss, environmental, and social impacts. Once the risks have been identified and estimated, evaluation is performed to assess whether the calculated risk is tolerable. If not, various risk treatment (control) activities may be performed to manage the risk.

More information on failure mode identification (Section 5.2), loads and hazards affecting dam safety (Section 5.3), event and fault tree analysis (Section 5.4), failure probabilities and fragility curves (Section 5.5), and breach initiation and progression (Section 5.6) are provided in the sections that follow. For additional detail, see USBR and USACE (2017), (Donnelly (2006, 2007), Hartford and Baecher (2004), SPANCOLD (2012), Vick and Stewart (1996), and von Thun (1985, 1999).
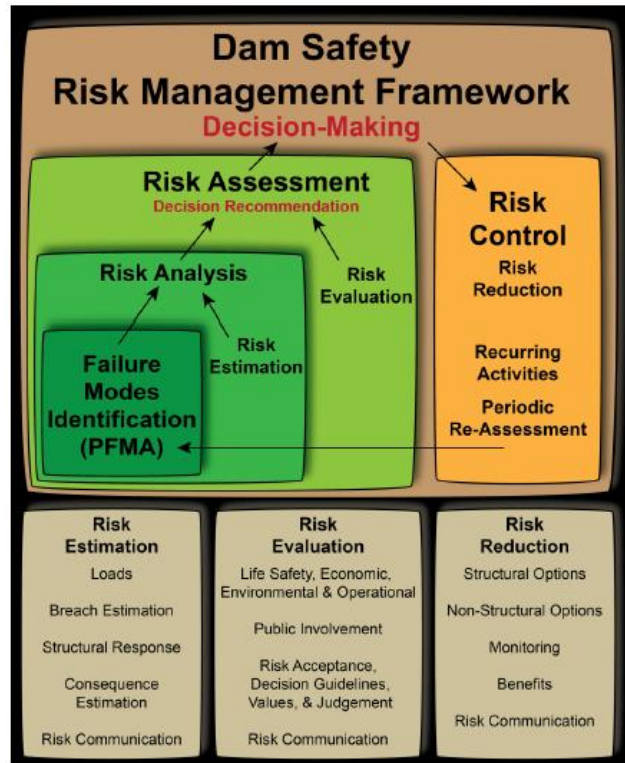
Figure 27. Relationships among risk analysis, risk assessment, and risk management. (*Source:* USBR and USACE 2017, Chapter IX-1)
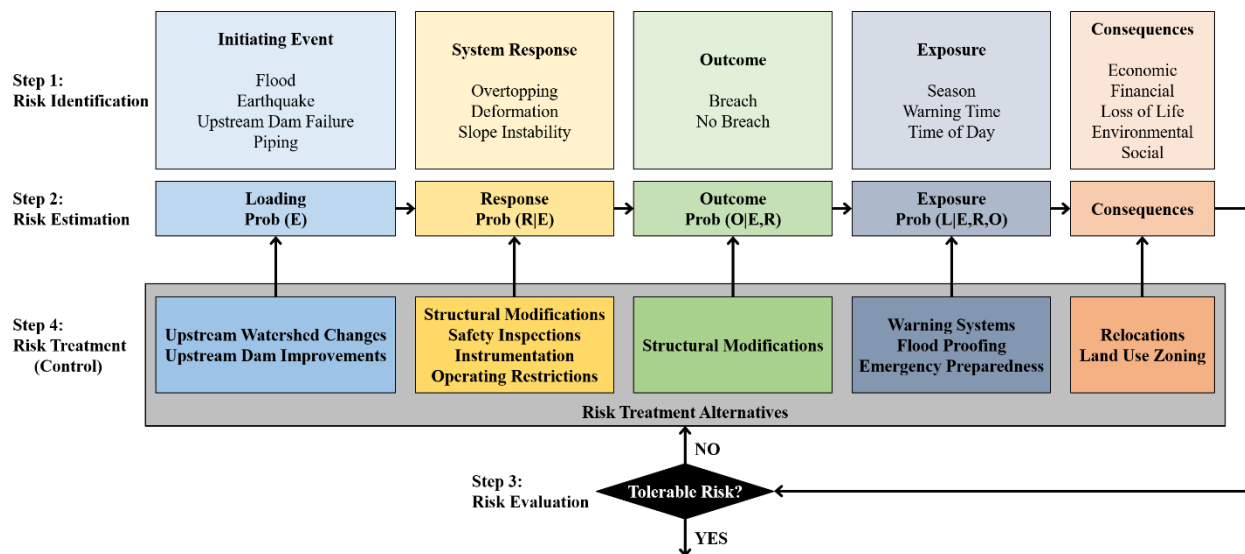
Figure 28. Framework for dam safety risk assessment. Structural modifications affect both the probability of response and the probability of outcome. (*Source*: Modified from Bowles and Schaefer 2014*)*

5.2   FAILURE MODE IDENTIFICATION

Most historical dam failures have occurred as result of one or more of the principal failure mechanisms described in Section 4.2, including overtopping, sliding, overturning, overstressing, internal erosion, spillway or energy dissipation failure, or operational factors. However, these failure mechanism

categories are often too generalized for analytical modeling. In practice, the dam system is broken down into subsystems to enough detail that a failure model can be sufficiently understood. Oftentimes, the failure may emanate from a low level in the system but propagate and become the failure mode at the next level up.

For the purposes of this document, the term "failure mechanism" is used to describe the state or condition that precipitates to cause a "failure mode." For example, hydraulic overtopping is a failure mechanism that may cause various deleterious events (e.g., erosion, collapse) to transpire and lead to a failure mode (e.g., overtopping failure of an embankment dam).

Traditional failure modes and effects analysis (FMEA) has occasionally been used for dam safety risk analysis (Hydrometrics Inc. 2011; Robertson 2012; Santos et al. 2012; Stewart 2000), but its use is uncommon. Instead, the USBR and the USACE (working together) have developed a unique version of FMEA for use in dam safety risk evaluations, PFMA (USBR and USACE 2017). In principle, PFMA builds on the general approach of FMEA but is tailored to dam safety and involves a disciplined protocol of steps. The PFMA approach is primarily based on subjective expert judgement as elicited in group meetings of involved practitioners, usually including both federal dam engineers and technical experts from contractor organizations.

FERC requires that PFMA be conducted for all FERC-regulated dams, unless a dam is granted an exemption, and defines PFMA as

> An exercise to identify all potential failure modes under static loading, normal operating water level, flood and earthquake conditions including all external loading conditions for water retaining structures and to assess those potential failure modes of enough significance to warrant continued awareness and attention to visual observation, monitoring and remediation as appropriate. FERC (2017)

When PFMA is performed, failure mode identification considers site-specific loading, structural, and operational conditions (described in more detail in Section 5.3). Often, a group of experts, comprising individuals most familiar with a particular dam, is formed to brainstorm potential failure mechanisms and failure scenarios to develop event or fault trees (described in more detail in Section 5.4). Other PFMA activities include data and information collection to assess investigation, design, construction, analysis, performance, and operation; site visits to assess potential failure mechanisms and structural and geologic conditions, review operations, and interview owners and operators; identification of surveillance and monitoring enhancements and risk reduction measures for each potential failure mode; and documentation of the analysis. California Department of Water Resources (2014) provides a PFMA report for Oroville Dam completed a few years before the 2017 spillway incident. Although significant portions of the report are blacked out for security-related concerns, it is worth noting that the potential failure modes identified were categorized as either flood loading, static loading earthquake loading, or operational. A large number of candidate potential failure modes were not carried forward.

The 2018 *Independent Forensic Team Report: Oroville Dam Spillway Incident* was critical of the current PFMA approach now used by US federal dam owners and operators:

> Shortcomings of the current Potential Failure Mode Analysis (PFMA) processes in dealing with complex systems must be recognized and addressed. A critical review of these processes in dam safety practice is warranted, comparing their strengths and weaknesses with risk assessment processes used in other industries worldwide and by other federal agencies. Evolution of "best practice" must continue by supplementing current practice with new approaches, as appropriate. (IFT 2018)

Performing failure mode identification—including identifying loads and hazards affecting a dam and developing event and fault trees—answers the first questions of the risk triplet: "what can go wrong?" To answer the next questions ("how likely is it?" and "what are the consequences?"), risk assessments rely on failure probabilities and fragility curves (described in more detail in Section 5.5) and consequence modeling (including modeling breach initiation and progression as described in more detail in Section 5.6).

5.3 LOADS AND HAZARDS AFFECTING DAM SAFETY

While scientific dam design has often applied a deterministic standards-based approach in which the dam is designed to withstand certain defined loads, many older dams had no such standards to follow. Still, given the significant number of dams throughout the US, the rate of dam failure is low, as noted in Table 3 in Section 2.5. The sections that follow describe some of the common loads and hazards affecting dam safety. Note that these loads and hazards are not necessarily mutually exclusive (e.g., a sizable flood and a sizable earthquake could co-occur in time). Hence, the frequency of occurrence for various loading events, individually or in combination, is important in a risk assessment framework.

Hartford et al. (2016) provides detailed information on hazards and disturbances related to dam systems. Among the topics covered are models of time, space, severity, and duration. Readers are referred to that literature for additional insight.

5.3.1 Seismic Hazards

Seismic hazards (both natural and induced by human activity) are one of the primary hazards for which dams are designed. Failures resulting from seismic activity can be abrupt (e.g., the 2011 failure of Fujinuma Dam [Pradel et al. 2012]). Figure 29 shows a simplified diagram of how seismic hazards propagate through bedrock and result in ground shaking, which can affect structures (including dams and reservoirs) at the Earth's surface.
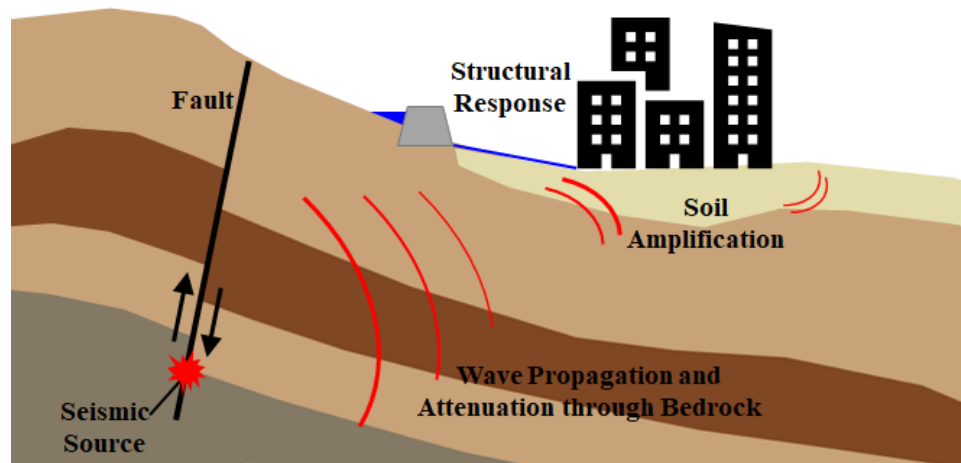
Figure 29. Seismic hazard diagram.

Figure 30 provides a qualitative view of the relative seismic hazards in the US as quantified by the USGS for use in building codes. Specific seismic hazards that may impact dams include ground shaking, fault rupture, soil liquefaction, ground upheaval or subsidence, and tsunami or seiche effects (USBR and USACE 2017, Chapter II-3).
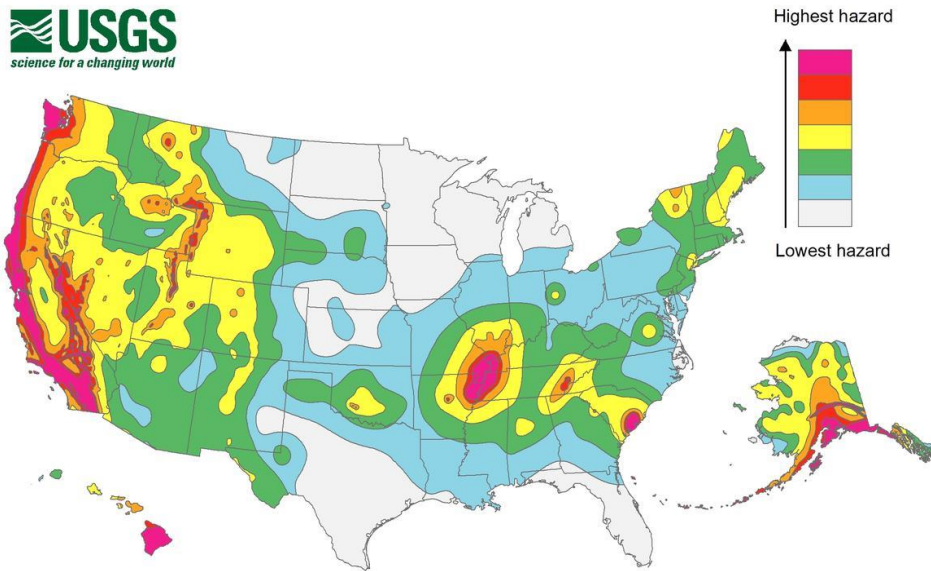
Figure 30. USGS national seismic hazard map. (*Source:* USGS)[32]

The level of seismic investigations required typically depends on both the seismicity of the region being evaluated and the threat to life, property, or environment posed by dam failure. FEMA's *Federal Guidelines for Dam Safety* (FEMA 2005) includes a chapter on earthquake analyses and design of dams that provides general guidelines for specifying design earthquake loadings and evaluating the safety of existing dams (or designing new dams).

Various design standards have been used for performing deterministic earthquake-related dam design and safety analysis, including the maximum credible earthquake, maximum design earthquake, safe shutdown earthquake (SSE), and operating basis earthquake (OBE). For example, NRC's NUREG/CR-7046 (NRC 2011) specifies two combined effects of flood scenarios resulting from seismic dam failure: Alternative 1 includes consideration of an SSE, and Alternative 2 includes consideration of an OBE. These terms are described in more detail in CFR 10, Appendix S to Part 50.[33]

These deterministic approaches require some basic information related to earthquake magnitude, site-to-source distance, relations to peak ground acceleration/velocity and strong ground shaking, and (in some cases) correction for at-site soil conditions above the dam's bedrock. This approach is scattered with uncertainty throughout, and many studies attempt to employ conservatisms. For example, the minimum distance from the dam to a point along the fault is used despite the fact that the source may occur elsewhere along the fault with varying likelihood. To account for the decrease in ground motion at points further from a seismic source, various ground motion attenuation relations have been employed (e.g., Graizer and Kalkan 2007; Feng et al. 2015).

As the current state-of-practice in earthquake science for dam safety practice, probabilistic seismic hazard analysis (PSHA) involves areas of high uncertainty and relies heavily on the use of quantified expert opinion. PSHA is covered in significant detail in the Senior Seismic Hazard Analysis Committee (SSHAC) implementation guidelines provided in NUREG-2213 (NRC 2018). Additional PSHA-relevant

---

[32] https://earthquake.usgs.gov/hazards/hazmaps/ (accessed November 2019)

[33] https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-apps.html (accessed November 2019)

literature includes Baker (2008), NRC (2012b), McCann and Addo (2012), and ANS 2.29. (ANS 2008). An update to ANS (2008) is currently under revision.

PRA for seismic hazards often involves calculating the probability that a certain level of ground motion will be exceeded during a reference time period. The methodology, first described in Cornell (1968), involves

- identifying seismic sources near the location of interest
- developing a magnitude-recurrence relationship for each source
- determining the distance-to-source probability of the location of interest
- developing appropriate ground motion prediction models for the region of interest
- integrating the ground motion probability over all sources and magnitude-distance combinations with an uncertainty prediction variable based on one or more ground motion prediction models
- repeating the calculation for multiple ground motion levels to develop a hazard curve

Fundamentally, this approach requires the development of a seismic-hazard source model and a ground motion model; it is described in detail in Chapter 7.3 of Hartford et al. (2016) and in ANS (2008). Discussion of federal best practices on seismic hazard analysis is provided in Chapter II-3 of USBR and USACE (2017). Example applications of probabilistic seismic analysis for dams and structures can be found in Lin and Adams (2007), Baker and Cornell (2008), Zimmaro and Stewart (2015), Zacchei et al. (2017), and Martin McCann ("Risk assessment for seismic prioritization of dams," unpublished notes for a seminar presented to the USACE, Office of the Chief of Engineers, Washington, DC, 1997).

5.3.2   Large Floods

Large flood events can induce various different deleterious or extreme loading conditions resulting from increased water levels and higher velocities. The primary threat large floods pose to dams is overtopping failure induced by increased water levels (e.g., 2006 Ka Loko Dam failure [Hartford et al. 2016]), although the risk of damage from seepage/piping and structural overstressing also is increased. In addition to flood hydraulic effects, various types of floating or submerged debris within the water body (common in large floods) can contribute to increased loads on a dam or damaging impacts to system components. While some dams maintain significant storage capacity to accommodate large flood inflow volumes (e.g., dams designed primarily for flood control), others follow run-of-river operation and have little or no storage volume. These rely entirely on gates or other active passage structures to pass increased flows (e.g., dams designed primarily for navigation).

Most critical infrastructure (including dams) in the US has been designed to withstand the effects (i.e., pass flows with sufficient freeboard) resulting from a probable maximum precipitation (PMP) event in the watershed upstream of the dam. These precipitation estimates were used as input to subsequent hydrological modeling, which considers various other system characteristics, such as antecedent conditions, runoff and loss characteristics, and river/reservoir routing. Based on the modeled hydrological conditions, inflows to the reservoir and water levels (the PMF) are estimated. These methods are still widely used in many applications related to dams and NPPs, although probabilistic flood estimates for critical infrastructure are becoming more prevalent.

In contrast to these deterministic PMP/PMF estimates, much of the noncritical civil infrastructure throughout the US (e.g., highways, bridges, culverts) is designed to pass inflows resulting from a storm of a certain return period (i.e., average recurrence interval) and may be based on the precipitation or the flow rate as a design parameter. For instances when a design precipitation is used as input to a hydrologic model, point precipitation frequency estimates from National Oceanic and Atmospheric Administration (NOAA) Atlas 14 may be used and are available for return periods of up to 1,000 years and throughout

most of the US (they are not available in a few states in the northwestern US). Application of point precipitation frequency estimates to watersheds has historically been accomplished using areal reduction factors, such as those found in TP-29 (US Weather Bureau 1957).

For instances when a probabilistic stream, river, or reservoir design discharge is used for hydrologic and hydraulic modeling, the USGS offers guidelines for determining flood flow frequency and magnitude using Bulletin 17C (England et al. 2018), an update to the previous Bulletin 17B that was the standard of practice for over 30 years. This process fundamentally requires the availability of suitable stream gage data, which may or may not be available for the location of interest. The Bulletin 17C method develops frequency-based estimates of flow using gage data for annual peak flows and is recommended for recurrence intervals of up to 500 years (equivalent to an annual exceedance probability [AEP] of 0.002). These probabilistic flow estimates can be used in subsequent routing and analysis (similar to that described previously for deterministic approaches) to estimate water levels. Discussion of federal best practices on developing reservoir and river stage exceedance probabilities is provided in Chapter II-1 of USBR and USACE (2017). Although most states and federal agencies use PMP/PMF for assessing critical infrastructure, probabilistic approaches can be applied for high-return-period events.

Under a risk-informed framework, flood loading for dam safety evaluation is often assessed using a hydrologic hazard curve (HHC), developed based on hydrologic hazard analysis (HHA). These HHCs combine peak estimates of flow, reservoir/river stage, and volume probabilities plotted against the AEP. As noted in USBR (2004), the peak discharge and volume estimates resulting from an HHA application may exceed the PMF, in which case USBR assumes that the PMF represents an upper limit of risk. An example is provided in Figure 31, which compares probabilistic reservoir elevation frequency estimates with dam spillway crest and PMF elevations. The dam stage points shown result from modeling water elevations under various analytical approaches, including using streamflow-based (event-based) statistics, precipitation frequency estimates, balanced hydrograph inputs, and inflow design flood hydrograph ratios. Discussion of federal best practices for probabilistic HHA is provided in Chapter II-2 of USBR and USACE (2017).

Dam Stage Frequency
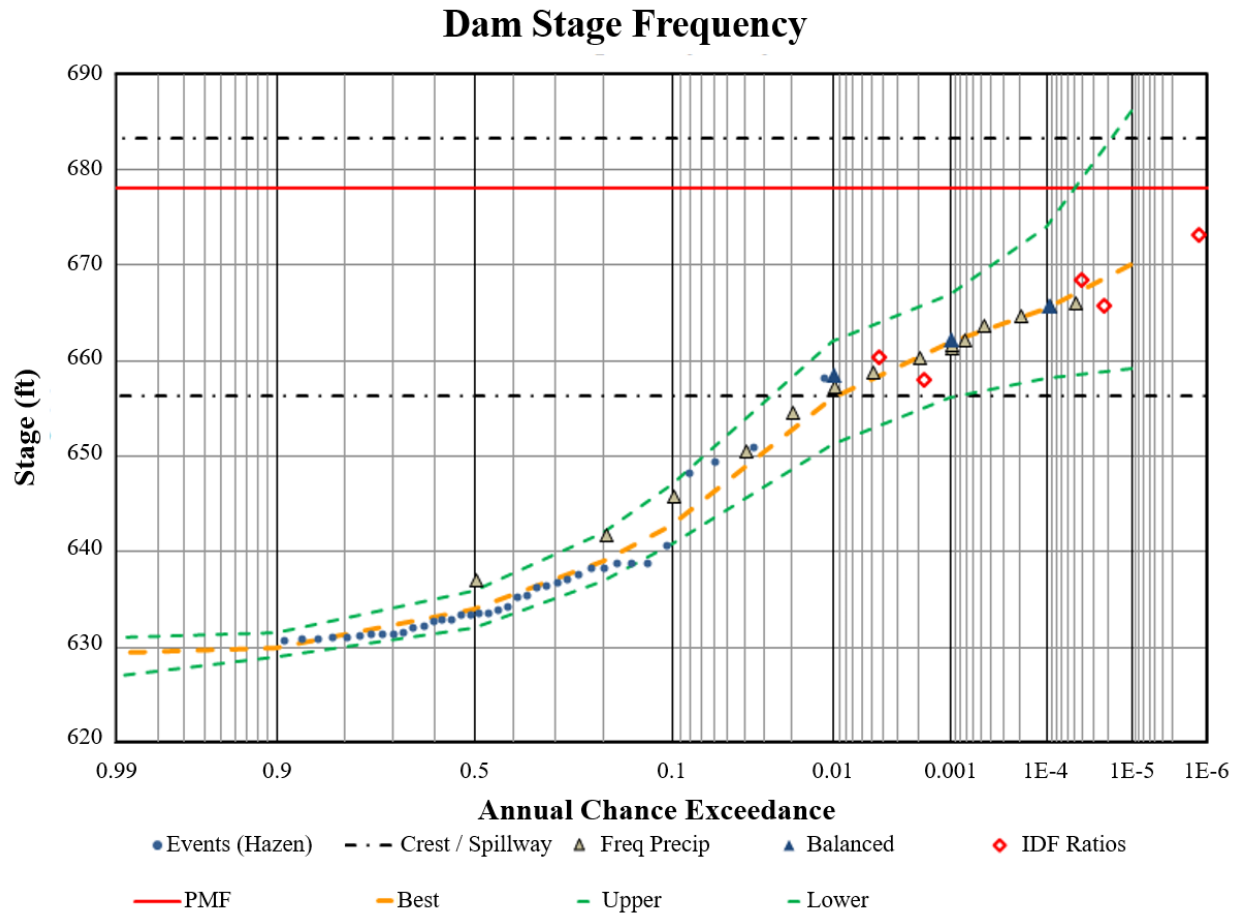
Figure 31. Example hydrologic hazard curve for reservoir elevation frequency. (*Source:* Adapted from USBR [2017], Chapter II-2)

5.3.3   Other Disturbances

A variety of other disturbances may also pose hazards for dam safety, especially when they are combined. The following are among the most prevalent:

- **Floating debris**: Trees, vegetation, boats, vehicles, and various structures can all be mobilized and find their way into waterways following floods, fires, land clearing, landslides, or other events. Once it reaches a dam, this material (unless otherwise safely passed or removed) can pose a serious safety concern by reducing outlet flow capacity (e.g., blocking hydropower intakes or spillway conveyances) and lead to increased water levels behind the dam (e.g., the 2013 Marseilles Lock and Dam incident in Illinois [Olson and Morton 2014]). The debris can also damage structures or components through increased static or impact loading and can lead to erosion under increased velocities or disturbed flow patterns. More information, including risk-related models, is provided in Chapter 7.4 of Hartford et al. (2016).

- **Ice and icing effects**: Like floating debris, ice can cause damaging loads and impacts on dam systems and components, limit outlet flow capacity (e.g., Wilsey Dam, British Columbia tunnel freezing event [Schellenberg et al. 2017]), and affect riverine hydraulics. Ice jams upstream of dams can also lead to elevated water levels and increased overtopping risk. When the weather is cold enough, ice can also adhere to various moving, mechanical equipment (e.g., gates, chains), preventing proper operation

(e.g., spillway gates freezing in place). More information, including risk-related models, is provided in Chapter 7.5 of Hartford et al. (2016).

- **Sedimentation**: In addition to floating debris and ice, sediment can limit a dam's discharge capacity by blocking inlet or outlet structures and can decrease storage capacity (e.g., Elephant Butte Reservoir, New Mexico, reservoir capacity loss [Ferrari 2008]). Under high velocities, coarse sediment releases through low-level outlets can increase erosion downstream of a dam. More information is provided in Chapter 7.6 of Hartford et al. (2016).

- **Reservoir landslides**: Landslides can pose several risks to a dam. One of the most immediate impacts from large landslides is the development of sizable impact waves with run-up that result from the sudden energy transferred through the displacement of water by earthen material (e.g., Vaiont Dam incident in Italy [Ward and Day 2011]). Following a landslide, large volumes of sediment can quickly enter a river or reservoir through landslides and lead to increased sediment loading or landslide dam development. A landslide can also contribute significant floating debris as trees and other vegetation are uprooted. More information, including risk-related models, is provided in Chapter 7.7 of Hartford et al. (2016).

- **Fire-induced erosion and disruption**: Fires near dams or upstream river systems can lead to multiple hazards, including increased debris and sediment conveyance resulting from erosion. Power supplies and communication may also be disrupted by fires (e.g., 2015 Boulder Creek Forest Fire in British Columbia [Boultbee et al. 2018]). More information, including risk-related models, is provided in Chapter 7.8 of Hartford et al. (2016).

- **Tornadoes**: Tornadoes can occur nearly anywhere on the Earth's surface, and they occur with varying frequency and intensity across different regions. Although they impact fairly small surface areas, tornadoes touch down approximately 1,200 times per year in the US (Hartford et al. 2016). The high winds associated with tornadoes can cause direct or indirect (e.g., through projectile impacts) damage to dam structures and components and can disrupt power supplies and communication (e.g., 2010 Chickamauga Dam incident in Tennessee [Sohn and Stone 2010]). More information, including risk-related models, is provided in Chapter 7.9 of Hartford et al. (2016).

- **War and sabotage**: Manmade damage to dam structures can occur through war or sabotage activities or through intentional destruction (e.g., bombing of Ruhr Valley dams in Germany during World War II in 1943, bombing of several North Korean dams during the Korean War in 1953, and destruction of several dams downstream of the Banqiao Dam in China following its disastrous failure in 1975 [Xu et al. 2008]). The Mosul Dam in Iraq and Three Gorges Dam in China (along with many others) are commonly identified as potential targets of militaristic strikes or saboteurs, and cyberattacks on dam computer systems represent an ever-increasing threat (e.g., 2016 Bowman Avenue Dam incident in New York [Thompson 2016]).

5.4 EVENT AND FAULT TREE ANALYSIS

Most risk analyses begin with a systematically structured model of the events that could, if they happened in a particular way, lead to failure. This type of model is an event tree. An alternative analytical tool to the event tree is the fault tree, and often the two are used in a reliability analysis to complement each other. A fault tree starts not with events possibly contributing to failure, but with the failure state itself, and asks what might need to happen for that failure state to occur.

5.4.1   Event Tree Methods

The use of event tree analysis for dam safety risk evaluation was pioneered by BC Hydro and USBR in the 1980s. Event tree analysis and the related fault tree analysis methods in application to dam safety risk are described in Hartford and Baecher (2004) and in more general terms in Pate-Cornell (1984). Commercial software applications that support the development and application of event trees are listed in Section 7.2.

An event tree begins with an initiating event and graphs the sequences of subsequent hypothetical events that ultimately could lead to failure. Examples of initiating events include earthquakes, floods, and hurricanes. An example of something other than a natural hazard that might be an initiating event is excessive settlement, which may cause equipment failure (e.g., spillway gate availability) and simultaneously disrupt utility services needed to deal with that equipment failure.

Event tree models are pervasive in dam safety risk analysis. They are described in the following sources: Beim and Hobbs (1997), Hartford and Baecher (2004), USBR and USACE (2017), and von Thun (1996, 1999).

The steps in developing an event tree analysis are

1. Define what "failure" means.
2. Identify initiating events.
3. Build an event tree of the system.
4. Develop models for individual components.
5. Identify correlations among component failures or failure modes.
6. Assess probabilities and correlations for events, parameters, and processes.
7. Calculate system reliability.

It is sometimes said that a principal benefit of risk analysis lies simply in structuring the problem as an event tree and in trying to identify interactions and correlations (i.e., failure modes and effects analysis), whether or not quantitative reliability calculations are ever carried out or used.

Although a variety of methods are available for analyzing engineering risks, event trees have become the most common approach in dam safety studies. Event trees provide an intuitive structure within which the analyst can organize the variety of considerations of concern about a particular dam. As event trees typically progress from start to finish in chronological order, they allow users to think about and record how a chain of events might unfold. They are also adaptable to unique conditions at a particular dam. Problems are de-composed into small pieces and then brought back together.

The use of event tree analysis for dam safety in federal practice is detailed in the USBR-USACE Best Practices training aids (USBR and USACE 2017, Part I-5). An example for a seismic liquefaction hazard is shown in Figure 32.
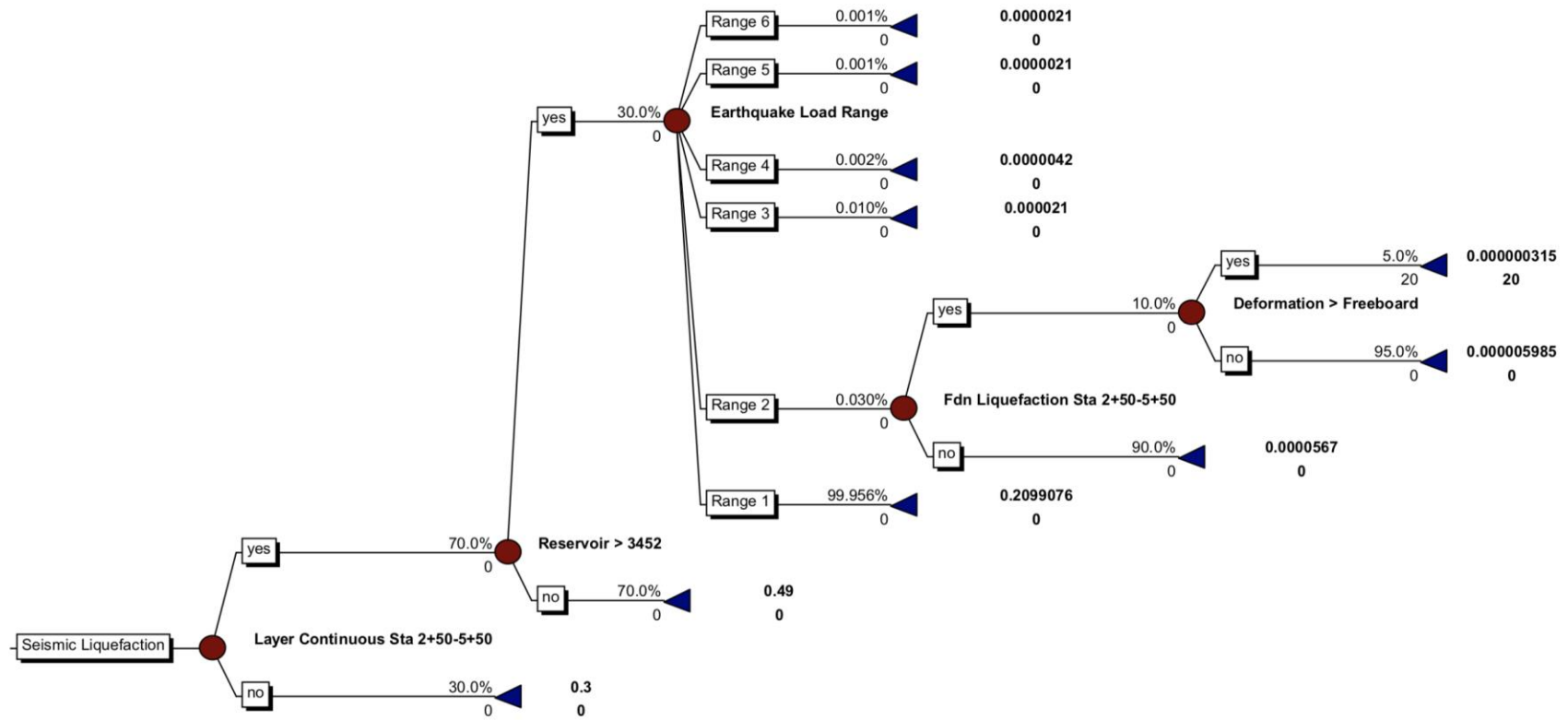
Figure 32. Example event tree for seismic ground shaking hazard. (*Source:* USBR and USACE 2017)

- At the initiating node, either liquefaction happens or it does not. The respective probabilities of these outcomes are 0.7 and 0.3. The probabilities sum to 1.0 because the events are mutually exclusive and collectively exhaustive. This is a requirement at each node.

- At the next node, the pool elevation is considered. The elevation is either higher than 3452 ft or it is not. The respective probabilities are coincidently also 0.7 and 0.3. If the pool is lower than 3452 ft, there is no consequence.

- At the next node, the earth load range is discretized into six bins, with corresponding probabilities.

- At the next node, for each load range, the foundation at Sta 2+50 to 5+50 liquefies or does not. The respective probabilities are conditioned on each of the six load ranges.

- The last node addresses whether the deformation in the foundation lowers the crest sufficiently to exhaust the freeboard of the dam. If "yes," consequences obtain; if "no," they do not.

The probability of any end leaf can be calculated by multiplying the chain of conditional probabilities along the path of nodes leading to that leaf. The sum of the probabilities of all of the end leaves must be 1.0.

At the same time, alternative approaches to risk analysis, most specifically fault tree methods (Section 5.4.2), have proved difficult to apply in practical dam safety studies. Unlike a piece of mechanical equipment, a dam is not easily broken down into a fully enumerated set of components, and it is not easy to link failures among a subset of those components to subsequent failures of others. It may turn out in future research that fault tree approaches shed new light on dam safety assessments; but at present, event trees are the standard approach.

Ultimately, event tree analysis is used to inform a decision process by explaining how a dam might be expected to perform. It supports considerations that in the past had not been considered formally: the likelihoods of various performance modes and the consequences to the dam and to downstream uses should such performance modes occur. Approached from this perspective, an event tree is a diagnostic tool; it is not intended to generate numbers alone but to draw inferences about how a dam might perform when it is subject to particular service conditions.

Evolving practice in seismic hazard, nuclear safety, and other risk analysis disciplines is to separate aleatory and epistemic uncertainties into two separate but conjoined trees. Aleatory uncertainties are those that deal with variations in time or space: randomness in the world. Epistemic uncertainties are those that deal with limited knowledge (i.e., uncertainties in what is known).

The aleatory uncertainties such as reservoir inflows or the geotechnical performance of an embankment are typically characterized by assumed states of nature, physics-of-failure models, and statistically inferred parameter values. Give the assumed states, models, and parameters, a probabilistic characterization can be made of possible frequencies of behaviors of the real-world systems. These are aleatory uncertainties conditioned on assumptions about nature. The uncertainties about the assumptions of states, models, and parameters are epistemic.

Two trees are thus created: an *event tree* and a *logic tree*. The event tree contains only the aleatory events conditioned on possible realizations of states of nature, model validity, and parameter values. The logic tree contains only the epistemic uncertainties about the possible states of nature, models, and parameters. First, a random path is constructed through the logic tree to establish one realization of the possible states of nature, valid models, and corresponding parameter values (Figure 33). This one realization of the

epistemic uncertainties is then used as input (conditioning) for all the probabilistic outcomes in the aleatory event tree. This simplifies numerical calculations and ensures that implicit correlations in the event tree due to common dependence on epistemic uncertainties in the logic tree are faithfully maintained.
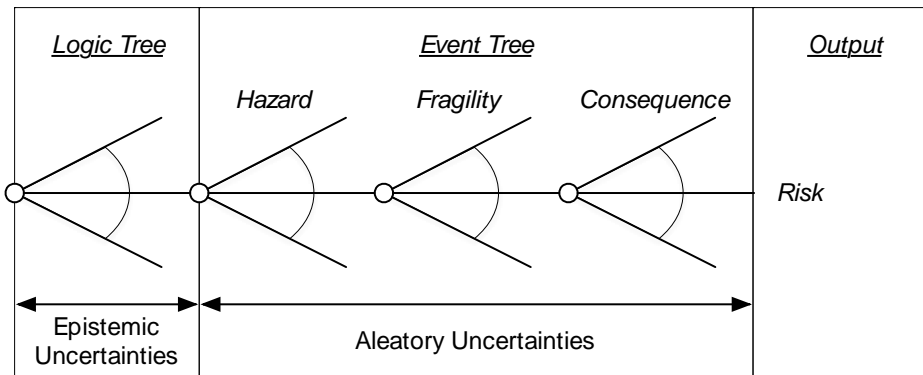
Figure 33. Logic tree describing fixed-but-unknown conditions (states) of nature, as conditioning.

The event tree structure attaches to individual "end leaves" of the logic tree, so all calculations within the event tree are conditioned on the realized states of nature in the logic tree. This arrangement generates implied correlation structures among the otherwise independent aleatory uncertainties. The final combined tree need be no more complex than before, since the number of combinations of all uncertain events, both aleatory and epistemic, remains the same.

5.4.2 Fault Tree Analysis

A review of the use of fault trees in dam safety risk analysis is provided in Hartford and Baecher (2004). A brief discussion of the choice between event trees and fault trees is provided by Paté-Cornell (1984). Fault tree analysis originated at Bell Laboratories in the 1960s in application to the US Ballistic Missile Program (Ericson 1999). It has since gained wide use in the aerospace and defense industries and in NPP reliability research.

There are only a limited numbers of specific applications of fault tree methods in application to dam safety in the literature (Bhattacharjya and Deleris 2012; McCann 2002; Patev et al. 2005; Patev and Putcha 2005). The principal uses of fault trees in dam safety are in application to mechanical and electrical systems, such as spillway gate availability (Lewin 2001a and 2001b; Lewin and Ballard 2001; Barker et al. 2003), valve reliability, and SCADA system performance. Johnson has applied fault tree methods to scour and channel stability (Bury and Kreuzer 1986). Commercial software applications that support the development and application of fault trees are listed in Section 7.3.

Event trees start with initiating events or causes and progress toward ever more detailed consequences. The ordering of events in an event tree can be rearranged so long as the relationships among conditional probabilities are adjusted; but in concept, the logical progression from cause to effect in a tree is an important, if sometimes concealed, principle of event tree analysis.

In contrast, fault trees start with consequences (i.e., failures), and progress backward toward ever more detailed causes (Figure 34). Thus, the logical structure of a fault tree is reverse to that of an event tree, in that the logic moves from consequence to cause. A system failure mode is considered the "top event," and a fault tree is developed in branches below this event, showing causes. Event tree analysts ask what might

happen if an initiating event occurs; whereas fault tree analysts ask how a particular outcome can come to pass. In concept, fault trees are photographs showing conditions at an instant in time. They may also show conditions at the transition between two events in an event tree, or the top event may be used as the initiating event in an event tree.
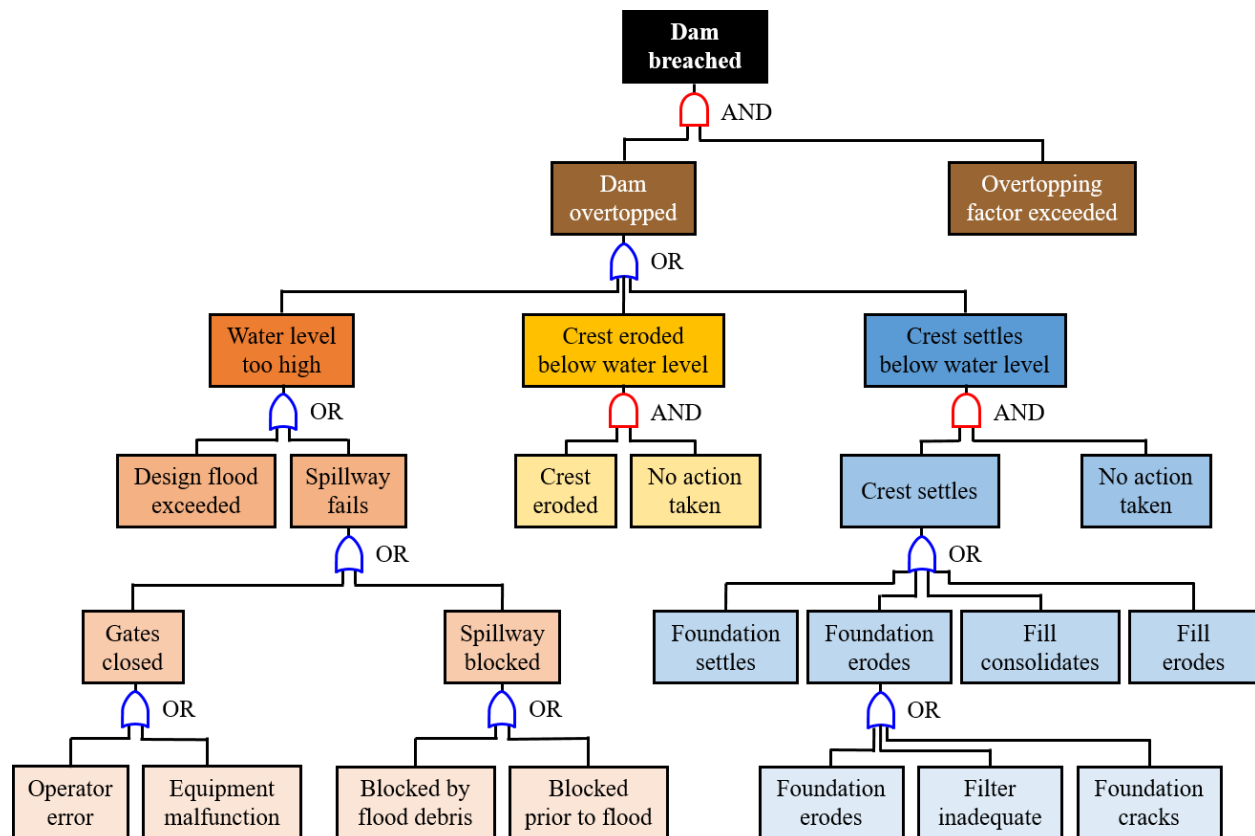
Figure 34. Example of a fault tree applied to the problem of dam failure. (Source: Adapted from Parr and Cullen 1988)

It is sometimes suggested that event trees and fault trees can be used interchangeably, but this is true only with difficulty. In fact, event trees and fault trees evolved out of different needs and are adapted to different tasks (Bier 1997). A fault tree presents all ways of producing a single event, using binary logic from Boolean algebra and resembling a root system rising to a main stem (Pate-Cornell 1984). It is most suited to well-defined systems, such as mechanical equipment, for which all the components can be enumerated and their interrelationships specified. It is less well-suited to poorly defined situations, such as earth structures or the geological subsurface, for which discrete components may not be differentiable or interrelationships may not be unequivocal (Bier 1997). It is also poorly suited to non-Boolean conditions in which component performance may have multiple states (Pate-Cornell 1984). Fault trees identify specific outcomes and they reason backward to uncover the possible ways an outcome might come to pass.

Another important difference between fault trees and event trees lies in the distinction between *failure modes* of a system and *failure mechanisms*. This distinction is clear in classical reliability theory but less clear in dam safety practice. A *mode* is a state or condition of a system or component. This can be a failing mode if its existence leads to adverse consequences, or it can be a safe mode it its existence does not. The elements of the fault tree of Figure 34 are modes in this sense (e.g., a gate is closed, or it is not; the spillway is blocked, or it is not; the crest is overtopped, or it is not). Modes are described by nouns

64

and adjectives. A *mechanism*, in contrast, is a set of processes or behaviors. ISO14224 (ISO 1999) defines a failure mechanism as "a process that leads to failure. The process can be physical, mechanical chemical, or a combination thereof." The branching elements in the event tree of Figure 35 used for calculating the probability of internal erosion in an embankment dam mostly describe things that happen: erosion is initiated, erosion continues, erosion progresses further, intervention is unsuccessful. Mechanisms are described by verbs and adverbs.
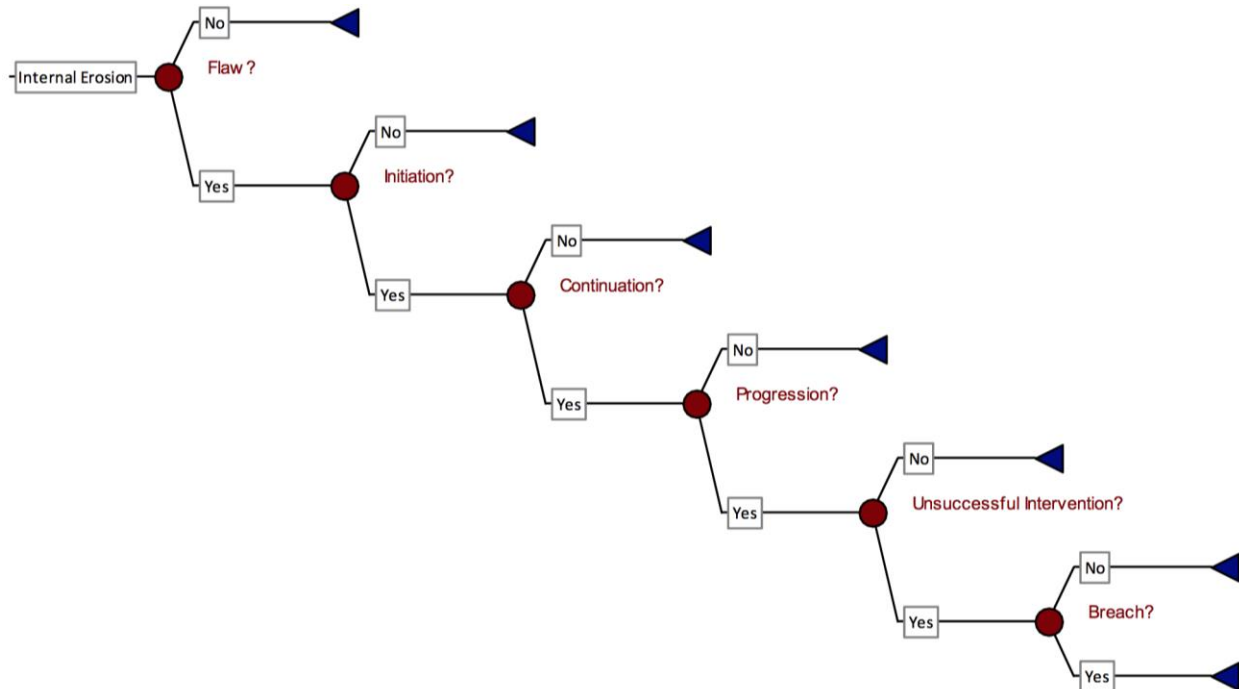
Figure 35. Schematic event tree for internal erosion. (Source: USBR and USACE 2017)

5.5   FRAGILITY CURVES

Modeling and analysis of initiating events and failure mechanisms is similar across the many ways a dam behaves. Initiating events are commonly treated as naturally varying in time and space (i.e., as frequencies), even though some uncertainties associated with initiating events may be epistemic, as is the case in PSHA. When included in a risk analysis of dam safety, however, initiating events are most often modeled as due to aleatory uncertainty. Treating initiating events as aleatory implies annual probabilities of events of a given size occurring or being exceeded, as, for example, in flood frequency relations or earthquake recurrence functions.

Initiating events are used as input to an event tree representation of the dam system's response to the corresponding loading. Within the event tree (Section 5.4.1) individual nodes may represent model, parameter, and other uncertainties; or they may represent the performance of components and sub-systems. Increasingly, dam safety practice is to separate out the model, parameter, and other epistemic uncertainties into their own "logic trees" and to leave only the component and subsystem performance uncertainties within the main event tree. These component and subsystem performance uncertainties are often summarized in load-response relationships known as fragility curves (or functions). ICOLD (2005) defines a fragility curve as "a function that defines the probability of failure as a function of an applied load level."

The term "fragility curve" arises primarily in structural engineering, where it is used to mean a summary of structural response, expressed as the probability of failure or of other adverse performance as a function of an applied load. The fragility curve is a simplified, summary model of component or subsystem behavior under load.

5.5.1 Fragility Curves

Porter (2018) defines a fragility curve (Figure 36) as

> A mathematical function that expresses the probability that some undesirable event occurs (typically that an asset—a facility or a component—reaches or exceeds some clearly defined limit state) as a function of some measure of environmental excitation (typically a measure of acceleration, deformation, or force in an earthquake, hurricane, or other extreme loading condition).
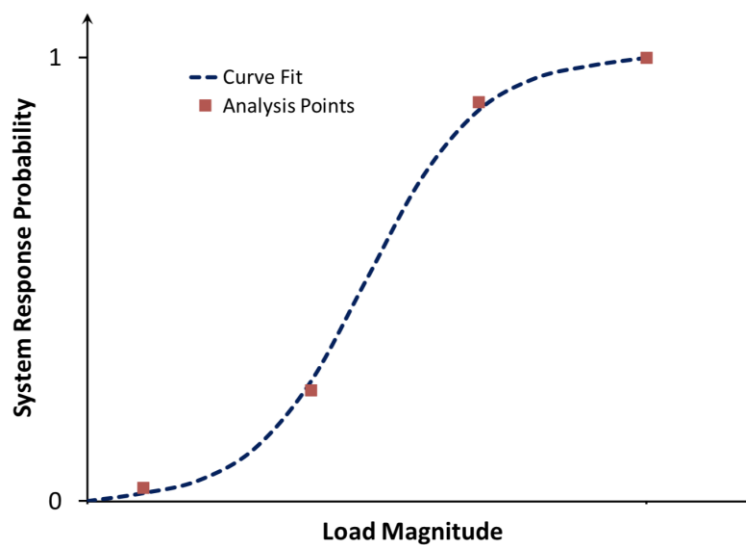
Figure 36. Schematic fragility (systems response) curve. (Source: USBR and USACE 2017).

A more general definition is the conditional probability that a structure or component reaches a limit state (fails or performs adversely), given an environmental load. An example is shown in Figure 36. Fragility curves are also sometimes called "fragility functions." USACE and USBR use the term "systems response curve" for this relationship (USBR and USACE 2017). Among the first uses of the term "fragility curve" was its use in respect to NPP risk analysis in the paper of Kennedy et al. (1980).

In PSHA, fragility curves are sometimes said to be cumulative distribution functions (CDF) of the capacity of a structure or component to resist an applied load or environmental condition. This is, however, not strictly true. A counter example is the probability of cavitation at a point in a spillway conveyance as a function of the discharge released through the spillway gates. As the discharge rises, at first the probability of cavitation damage increases; but as the associated hydraulic jump moves downstream, the probability peaks and then diminishes. The CDF analogy is useful in many cases, but not in all cases.

Log-Normal fragility curves

In PSHA and certain other applications, fragility curves are commonly modeled using the cumulative logNormal distribution. There is no necessary reason for this. The assumption of log-Normality is one of

simplicity and historical use. However, the log-Normal function is thought to fit observed structural failure data well, although the fit must be verified for the individual situation.

The log-Normal fragility curve $F(d|x)$ follows the relation

$$F(d|x) = P(D \leq d|x) = \Phi\left(\frac{\ln x - \ln \theta}{\beta}\right) = \Phi\left(\frac{\ln (x/\theta)}{\beta}\right),$$

in which D = damage state, d = particular value of the damage state, x = load, θ = median capacity of the component to resist damage state d, β = standard deviation of ln of the capacity of the component to resist the damage state. Denoting the logarithmic mean and standard deviation μ_{lnX} and σ_{lnX}, respectively, $\theta = \exp(\mu_{lnX})$ and $\beta = \sigma_{lnX}$.

Multiple damage states

In most practical situations, there is more than one damage state; that is, the fragility curve is not a simple Boolean, failure or no-failure, but describes a range of adverse performances from moderate to severe. An example of a fragility curve for multiple damage states (slight-moderate-extreme-collapse) is shown in Figure 37. Fragility curves for multiple damage states are a nested set of curves. The curve associated with the most severe damage state is at the bottom with the least probability, and the curve for the least severe damage at the top with the greatest probability.

The fragility curves in Figure 37 are sequential; that is, post-loading the component exists in exactly one damage state, and the component passes through each damage state to its final level. The component progresses from slight damage to complete damage. There are other possibilities for multiple damage states, but these are less common. For example, the component may exist in more than one damage state at the same time (simultaneous), or there may be exclusive and exhaustive damage states that are not sequential (Porter 2018).
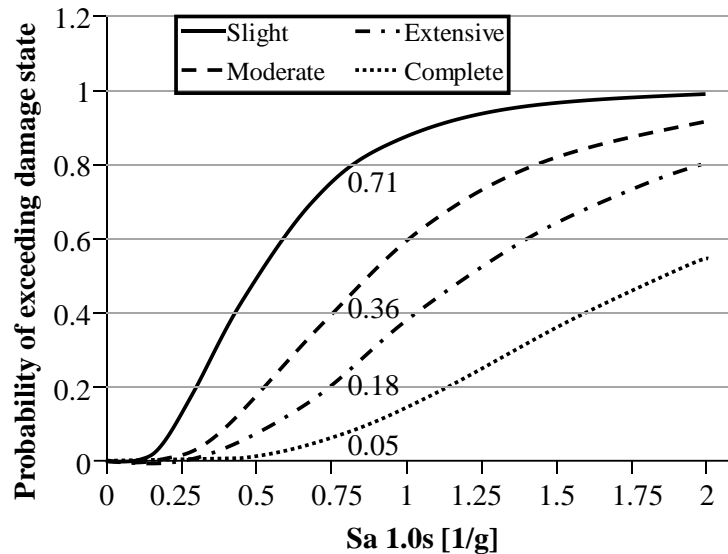
Figure 37. An example fragility curve with multiple damage states for concrete bridges in a database of Northern Italian structures. (*Source:* Modified from Carturan et al. 2013). Sa 1.0s is spectral acceleration at a frequency of one second.

Reliability curves

Reliability curves describe the time-dependent performance of a system or component, relating failure rates or probabilities to age. These curves are distinct from fragility curves, which relate failure rates or probabilities to the load on a system or component.

For mechanical and electrical systems and components in dams, reliability curves are often modeled as Weibull distributions (Patev et al. 2013),

$$F(t) = P(T \leq t) = 1 - exp\left\{-(t/\alpha)^\beta\right\},$$

where T, t = time to failure, α = scale parameter, and β = shape parameter.

Extensive data on mechanical and electrical gate component reliability from USACE asset management sources are provided in the Appendix to Hartford et al. (2016) as Weibull parameters. The USACE has also collected data and developed reliability models for gate components at its facilities.

Vulnerability curves

Fragility curves relate the probability of exceeding some damage state as a function of the load on the system or component. *Vulnerability curves* relate the extent of loss or the consequence to the load on the system or component. The loss might be repair cost, loss of life, loss of functionality, or some level of environmental degradation. Vulnerability curves are also sometimes referred to as damage functions, loss functions, vulnerability functions. Vulnerability measures loss; fragility measures probability.

5.5.2   Identifying Fragility Curves

As with any estimate, there are only three ways of assigning fragility curves: (1) statistical analysis of empirical data, (2) modeling from first principles, and (3) using subjective judgment (Porter et al. 2007).

The statistical-empirical curve is based on an analysis of historical performance data (Foster et al. 2000). Given the low rate of catastrophic failure of modern dams, however, empirical fragilities for entire dams or major dam subsystems are little used. Historical data for components are more readily available. Large dam-owning organizations such as USACE or large hydropower operators usually maintain asset management data on failures of mechanical and electrical systems such as hydraulic gates and generators. These data are shared through trade groups such as CEATI International in Montreal.[34]

The modeling approach to fragility curves is often used for engineered systems or components, such as the strength of the structural frames supporting spillway gates or the geotechnical stability of embankments. A large collection of literature on structural and geotechnical reliability engineering exists to support these modeling efforts (Baecher and Christian 2003; Ditlevsen 1996; Griffiths et al. 2007; Melchers 1987)

The judgmental approach uses subject matter experts (SMEs) subjectively to assess fragility curves. This has been common for failure mechanisms such as internal erosion for which there are few empirical data and inadequate physics-based models. The use of expert opinion elicitation (subjective probability) in dam safety risk analysis is pervasive. USACE and USBR have developed tailored approaches based on the concept of PFMA (USBR and USACE 2017). The NRC-developed Senior Seismic Hazard Analysis Committee procedure (NRC 2018) has been widely used for conducting seismic hazard analysis related to

---

[34] www.ceati.com (accessed November 2019)

dam safety (McCann and Addo 2012), but it has been less widely used for general dam safety risk analysis.

Two approaches to the use of expert opinion have evolved in dam safety studies, one principally in European practice and the other principally in US federal practice. The European practice is to use expert judgment to assign values to the input parameters of reliability (i.e., physics-of-failure) models, and then to use the reliability models to propagate those uncertainties to probabilities of failure (Vrijling 2001). The US federal practice, in contrast, is to use expert elicitation directly to assign values to the probabilities of failure without involving a physics-of-failure model.

5.5.3   Examples of Fragility Curves in Dam Safety

Most studies of dam safety risk include some form of fragility curve. The concept and nature of fragility curves are discussed by Porter (2018) and USBR and USACE (2017). Examples are shown in Figure 36 and Figure 37. Figure 38 shows four fragility curves for four failure models of a coastal flood levee.

For concrete dams, example fragility curves are provided in Ellingwood and Tekie (2001) and Chase (2012).

For embankment dams involving geotechnical failure mechanisms, example fragility curves are provided in Altarejos-García et al. (2014), Duncan (2000), Fenton and Griffiths (2008), Schweckendiek and Kanning (2016), and Fell (2015).

For internal erosion and piping of embankment dams, example fragility curves are provided in Fell et al. (1992), Foster et al. (1998), Foster et al. (2000), Hartford and Baecher (2004), McDonald (1995), and USBR and USACE (2017).

For spillway structures and systems and key components (e.g., gates, gate hoists, valves), example fragility curves are provided in Langseth and Perkins (1983), Lewin (2001a), Patev et al. (2005), and Patev and Putcha (2005).
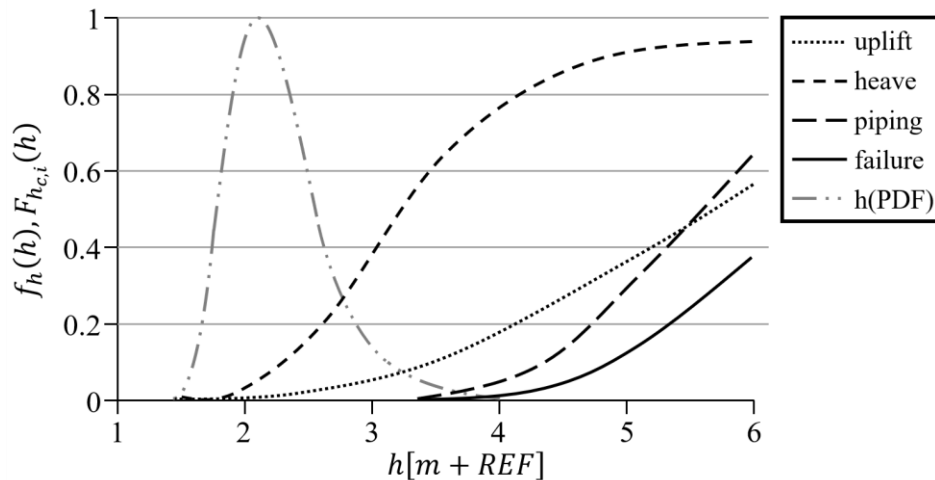
Figure 38. Application example for field observations, dike ring 10 (Mastenbroek) – prior fragility curves for uplift, heave, piping and failure and probability density of the water level. (*Source:* Modified from Schweckendiek et al. 2014)

5.6   DAM BREACH MODELING

Dam breach modeling is a widely used tool for evaluating dam breach impacts. Typical dam breach modeling involves analyzing breach initiation and progression to provide a basis for estimating downstream flows and the consequences of a dam breach. The size and geometry of the breach and the timing of breach development determine peak flows through the breached dam and the breach hydrograph causing downstream flooding.

The analysis of breach initiation and progression focuses on failures of earth dams and embankments, including failures of natural foundation materials beneath or adjacent to constructed dams. Failures of rigid structures, such as spillway gates or a concrete dam section, are typically assumed to occur near-instantaneously, with the size and shape of the breach determined by the size and shape of the structure that fails.

Wahl (1998) undertook a literature review for USBR on the need for breach parameter information for modeling breach formation and progression. This review provides excellent and detailed coverage of the contemporary state-of-the-art and practice. Emphasis in this review was given to the particular use of dam breach analysis within the context of the risk assessment as used by USBR. Then-current methods for predicting embankment dam breach parameters and numerically modeling dam breach events were reviewed. This review was accompanied by an international workshop of some 35 experts.

The review led to conclusions about the importance of characterizing breaching processes. It distinguishes between breach initiation time and breach formation time and concludes that this distinction is important to the ability to accurately assess warning time and thus downstream consequences. Breach prediction equations based on case studies were thought to have significant uncertainty, and formation time is particularly difficult to predict. Breaching typically occurs through headcut erosion (i.e., progressive scouring of foundation or embankment material in an upstream direction) that initiates at the toe of the dam and advances headward until the crest is breached. However, this mechanism is not characterized in most physics-of-failure models.

The Wahl review concluded that dam breach models should address the following questions:

1. For a given set of conditions, will a dam breach?
2. How much time is required to initiate a breach?
3. How will the breach develop once it is initiated (e.g., ultimate dimensions, rate of development, total time to reach ultimate dimensions)?

Further, the breach model "should be applicable to both overtopping and piping- or seepage-induced failures, although the initial focus of model development should be on the more tractable problem of overtopping failures."

5.6.1   Empirical Models

Breach analysis models are divided into two broad categories (CDNR 2010): empirical methods and physics-of-failure methods.

Empirical methods of breach analysis are based on analyses of dam-failure case histories and are currently the main approach used for evaluation of potential breaches of earthen dams and embankments. A number of investigators have conducted statistical analyses of data on failures of earthen dams to derive empirical relationships among measurable attributes such as reservoir and dam dimensions and the

geometry and timing of dam breaches. These empirical methods may be categorized into three types according to the Wahl review:

- **Parametric models** use case studies to estimate time to failure and ultimate breach geometry and then simulate breach growth as a time-dependent process and predict breach outflows using hydraulics.

- **Predictor equations** estimate peak discharge from an empirical equation based on case study data and assume an outflow hydrograph.

- **Analogue comparison** considers other dams similar in size and construction for which a historical failure is well documented.

The empirical approaches rely on case study data. In general, the database of well-documented dam failure cases is limited and contains few high dams with large reservoirs. Also, the assumption of linear growth of breaches is usually poor.

Parameters predicted by empirical methods typically include time to failure, breach width, and slope angles of the side slopes of the breach. Some empirical models also predict breach peak discharge (Wahl 1998; CDNR 2010). Examples of methodologies derived in this fashion include MacDonald and Langridge-Monopolis (1984), von Thun and Gillette (1990), Froehlich (1995a, 1995b), and Froehlich (2008). Differences between the different empirical methodologies result from differences in the case-history data sets used to derive the methodologies, as well as increasing sophistication over time in the statistical approaches employed.

All such approaches are necessarily based on analysis of a limited set of case histories suitable for analysis. Wahl (2004) counted about 108 suitable case histories, of which about 75% were failures of dams less than 15 m in height (Wahl 2004). More recently, Xu and Zhang (2009) reported a multiple regression analysis that considered data from 182 earth and rockfill dams in China and the US, of which nearly half were over 15 m in height; however, because data were incomplete for many of the case histories, their regression analyses were based on a small fraction of the total set of case histories.

An additional factor limiting the use of case histories is that accurate data on breach dimensions, geometry, and progression for the case histories are lacking. Case studies typically provide data on the geometry and dimensions of the breach at the end of the failure event, but not during the failure process. Estimates or measurements of breach outflows may also be available. Case study data are especially weak regarding the time needed to initiate a breach, the rate of breach formation, and the total time required for failure (Wahl 1998).

Rates of breach enlargement are typically estimated from photographs, eyewitness accounts, and small-scale experiments (Froehlich 2008). MacDonald and Langridge-Monopolis (1984) identified the uncertainty in breach geometry and failure timing data as a principal limitation on the reliability of model predictions. Although newer empirical methodologies employ more complex statistical approaches, the more sophisticated approaches cannot overcome the problems resulting from the limitations of the data available from case studies from which the methodologies are derived and which provide the basis for evaluating their predictive power.

Wahl (2014) observed that research associated with the development of physics-of-failure erosion models has demonstrated the importance of soil erodibility in dam breaching and has generated interest in incorporating erodibility into empirical dam breach parameter prediction equations. Walder and O'Connor (1997) presented an early empirical methodology that incorporated a measure of erodibility.

Xu and Zhang (2009) presented an empirical methodology based on case studies that included an erodibility factor. Evaluation of their model by Wahl (2014) found that it produced reasonable predictions of observed breach parameters for medium- and high-erodibility dams and suggested that the inclusion of erodibility would improve the predictive performance of empirical models.

However, the Xu and Zhang methodology is not currently recommended for several reasons—including their use of a definition for failure time that is inconsistent with the failure-time parameters used in other breach parameter methodologies and incompatible with HEC-RAS (Hydrologic Engineering Center– River Analysis System) (USACE 2014b). Other researchers have aimed to combine empirical analyses with more physically realistic treatments of hydraulics. For example, Froehlich (2016) presented a semi-theoretical model that includes a nonlinear expression to determine the maximum peak discharge produced by an instantaneous trapezoidal breach.

5.6.2   Physics-of-failure Models

Physics-of-failure models of breach initiation and progression treat the development of a breach as an erosional process, based on hydraulics, soil and rock mechanics, and sediment transport. Such methodologies incorporate data on materials characteristics of a dam or embankment, dam dimensions, fluid dynamics during the breach, and tailwater effects. Breaching may be precipitated by overtopping, internal erosion, a seismic event, or other external disturbance.

Data, algorithms, and other analytical tools that can be used in evaluating the erodibility of earthen dams, embankments, and natural foundation materials; evaluating the potential for initiation of internal erosion and other breaching modes; and calculating rates of internal erosion and breach development are compiled in a toolbox included in the USBR *Dam Safety Risk Analysis Best Practices Training Manual* (USBR and USACE 2017, Sections IV-1 to IV-4). USBR notes that the information in this toolbox is not assembled into "cookbook" predictive methodologies but may be considered or applied in specific evaluations that are informed by engineering judgment.

In general, most current embankment dam seepage and slope stability analyses employ deterministic approaches that use approximated soil properties and other parameters. Traditional probabilistic approaches have also been applied, mostly using the first-order second-moment method, point estimate method, and Monte Carlo simulation (Calamak and Yanmaz 2014). Some recent applications (Wang 2012; deWolfe et al. 2010; Allahverdizadeh et al. 2015) have employed the random finite element method, which accounts for spatially random shear strength parameters and spatial correlation by combining nonlinear elasto-plastic finite element analysis with random field theory. This method and a USBR-developed computer program, *Pf-slope* are also described in detail in USBR (2009).

Lack of methods for measuring some relevant parameters, particularly measures of the erosion susceptibility of cohesionless materials used in earthen dams and embankments, is identified as a large source of uncertainty in evaluating potential failures.

Several physics-of-failure models of breach initiation and progression have been developed.

BREACH. The National Weather Service BREACH model (Fread 1988; several revised versions of the model were released in later years) is the best-known example of these. This model is designed to predict both breach characteristics (breach dimensions and timing) and the outflow hydrograph for an earthen dam breached by overtopping or internal erosion. Because of simplifications incorporated in the model, it does not realistically simulate all breach processes, including head-cutting erosion of overtopped dams and collapse of the crests of dams breached by internal erosion. Those limitations are expected to cause it

to systematically underestimate breach dimensions and overestimate failure time, particularly for large dams (CDNR 2010).

SIMBA (Simplified Breach Analysis). The SIMBA (Simplified Breach Analysis) model under development at the USDA–Agricultural Research Service Hydraulic Engineering Research Unit in Stillwater, Oklahoma (Temple et al. 2005; Hanson et al. 2005) and the HR-BREACH model under development at HR Wallingford, Great Britain (Mohamed 2002; Mohamed et al. 2002) are semi-empirical. In these models, the breaching process is subdivided into phases in which different flow and erosion mechanics predominate, and the individual phases are modeled semi-empirically using equations derived from laboratory and real-world data.

Both models were developed for analysis of experiments and could make use of measured values of soil erodibility parameters (Wahl et al. 2008). SIMBA is applicable to overtopping failures of homogeneous embankments of cohesive materials, and HR-BREACH is designed to model both overtopping failure and piping failure of homogeneous embankments or composite embankments with noncohesive zones, surface protection, and a cohesive core. A third model, **FIREBIRD BREACH**, which was being developed at Montréal Polytechnic (documented by Wang and Kahawita 2002 and Wang et al. 2006) uses fundamental differential equations to simulate hydraulic conditions and erosion processes. It incorporates coupled equations for hydraulics and sediment transport and is capable of modeling overtopping failures of homogeneous embankments of either cohesive or noncohesive materials (Wahl et al. 2008). The Working Group on Embankment Dam Erosion and Breach Modeling, organized under the DSIG of CEATI International, later concluded that the difficulty of using this model made it unsuitable for continued evaluation (USBR 2017).

According to Wahl et al. (2008) the use of physics-of-failure models has been hindered by difficulties in quantifying the erodibility parameters and a lack of models that effectively incorporate objective measures of erodibility. Wahl (2014) observes that evaluation of the erodibility of rockfill dams appears to be especially challenging because there are very limited data on erosion rates for rockfills under specific hydraulic conditions. It has been proposed that gravel- and cobble-size material in rockfills has low erodibility, similar to high-plasticity clay, due to similarities in the critical shear stresses and velocities needed to initiate particle movement; however, their erosion processes are dissimilar. While erosion rates and process for cohesive materials (i.e., clay) may be controlled by the detachment rate of clay-sized particles, rockfills built from cohesionless material (i.e., individual loose rocks) may erode rapidly once the critical shear stress is exceeded.

WinDAM. Subsequent development of the SIMBA model in the USDA resulted in the WinDAM model series. The current version of WinDAM, WinDAM C (USDA 2016) models breach initiation (but not subsequent breach development) by overtopping of homogeneous earthen embankments or earthen auxiliary spillways of dams, as well as by internal erosion of homogeneous cohesive embankments. It incorporates methodology from the SIMBA model (USBR 2017). Breach development must be predefined (West et al. 2018). Process phases included are (1) failure of vegetal cover (for overtopping) and development of concentrated flow; (2) downward erosion in the area of concentrated flow, resulting in headcut formation; and (3) downward and upstream movement of the headcut, potentially breaching the spillway or embankment. Each phase is described by a set of threshold-rate relationships based on the process mechanics. A headcut erodibility index describes the resistance of the exposed geologic materials to erosive attack during the third phase of the process (USDA 2016). Plans for future development of the WinDAM model series include (1) adding the potential to initiate failure at the embankment toe, in stability berms, or in groin areas (zones of flow and stress concentration during overtopping); (2) modeling of slopes protected by concrete block or reinforced vegetation; and (3) modeling of zoned embankments (USBR 2017).

HR-BREACH. HR-BREACH has been further developed into the EMBREA and AREBA models (USBR 2017; West et al. 2018). According to West et al. (2018), EMBREA can compute breaching of cohesive and noncohesive embankments, including zones of materials with different erodibilities. It handles multiple failure mechanisms, can consider non-trapezoidal breaches, and does not pre-define breach development; and it is capable of modeling mass and micro failure of banks due to soil slope instability during the breach growth process. It was validated against 4 historical dam failure cases, 7 field cases, and 18 laboratory cases and was considered to provide good performance. AREBA is simpler than EMBREA and has fewer capabilities. According to West et al. (2018), it is able to model overtopping failures in homogeneous and composite embankments and internal erosion failures in homogeneous embankments. Breach development must be predefined, but simple slope stability equations are calculated. AREBA has been validated against laboratory experiments and field case study data, as well as EMBREA modeling results.

DSIG identified EMBREA and SIMBA (now incorporated into WinDAM) as the models offering the greatest opportunity for future industry use. In its 2014 guidance on applying HEC-RAS for dam break studies (USACE 2014b), the USACE recommended NWS-BREACH, WinDAM, and HR-BREACH as the physics-of-failure computer models most suitable for use in modeling dam breaches as input to HEC-RAS.

Determining breach parameters. USACE (2014b) suggests that dam attributes should be within the range of values considered in the regression analysis used to develop the breach parameters. If the dam under investigation is outside the range of values in the case studies, breach parameters should be carefully examined for reasonableness. The USACE cautions that breach parameters from different multiple regression analyses must not be combined in a mix-and-match fashion (USACE 2014b). Froehlich (2016) suggests, however, that the semi-theoretical approach he described could be extended to higher dams and larger reservoirs than are represented by the 41 dams on which it was based, since the peak discharge predicted by his semi-theoretical formulation is bounded by the maximum flow that could be produced by an instantaneous breach.

5.6.3   Modeling Breach Progression with Hydrologic and Hydraulic Models

Many hydrologic models (e.g., HEC-HMS [Hydrologic Modeling System]) and hydraulic modeling packages (e.g., HEC-RAS) from governmental and commercial sources now incorporate algorithms or modules for modeling dam failure breach progression, typically using breach parameters obtained with other methods. Use of hydraulic models is commonly prioritized over use of hydrologic models because a dam failure is fundamentally a hydraulic process; and hydraulic models allow more accurate simulation of the influences of reservoir shape, tailwater, and drawdown and fewer modeling simplifications (CDNR 2010). Because modeling packages published by USACE's HEC are widely accepted nonproprietary models that have widespread use in the US, and because of the shortcomings of hydrologic models relative to hydraulic models, this discussion focuses primarily on the use of the HEC-RAS hydraulic model for analysis of breach progression.

Analysis of breach progression with HEC-RAS requires specification of failure mode (piping or overtopping), breach width, side slope angles, and failure time. These are typically determined using empirical methods. Weir flow coefficients must be specified for both the dam crest and the breach flow section. The weir flow coefficient for the crest of an unbreached dam may be determined from the dam design; values for typical dams range from 2.6 to 2.8, and the State of Colorado recommends a value of 2.6 (CDNR 2010). The breached section of a dam acts like a broad-crested weir with side slopes, and CDNR (2010) identifies a weir flow coefficient of 3.08 as appropriate for an overtopped dam as well as for modeling of piping failures. A base flow (determined from watershed hydrology) and the shape of the breach progression curve must also be specified. A sine wave progression is identified as the best

representation for most breaches, as a dam breach typically progresses slowly at the start and end of failure, and more rapidly in the middle of the progression; but a linear progression may be more appropriate if there would be substantial tailwater submergence (CDNR 2010). The model representation of upstream and downstream reaches and the selection of computational time steps both need to be tailored to the special situation of a dam breach; the USACE (2014b) provides advice on these topics.

Based on breach modeling results, or using an integrated software, failure-induced dam breach flow can be simulated to assess downstream flood impacts. Routing of the breach flow often accounts for attenuation as the flood wave moves downstream. By assessing the flood hydrograph, maximum water levels and flood duration can be assessed. Using HEC-RAS's 2D modeling capabilities or other 2D or 3D hydraulic and hydrodynamic models, flood inundation can be easily assessed, often at high spatial resolution. Maps for 1D models can also be produced but may not be as useful for localized flood evaluation, such as near critical infrastructure. Flood mapping (Figure 39) and animations that visualize simulated flood inundation can provide valuable tools for preparing flood hazard protection plans or responding to active flooding and forecasts.
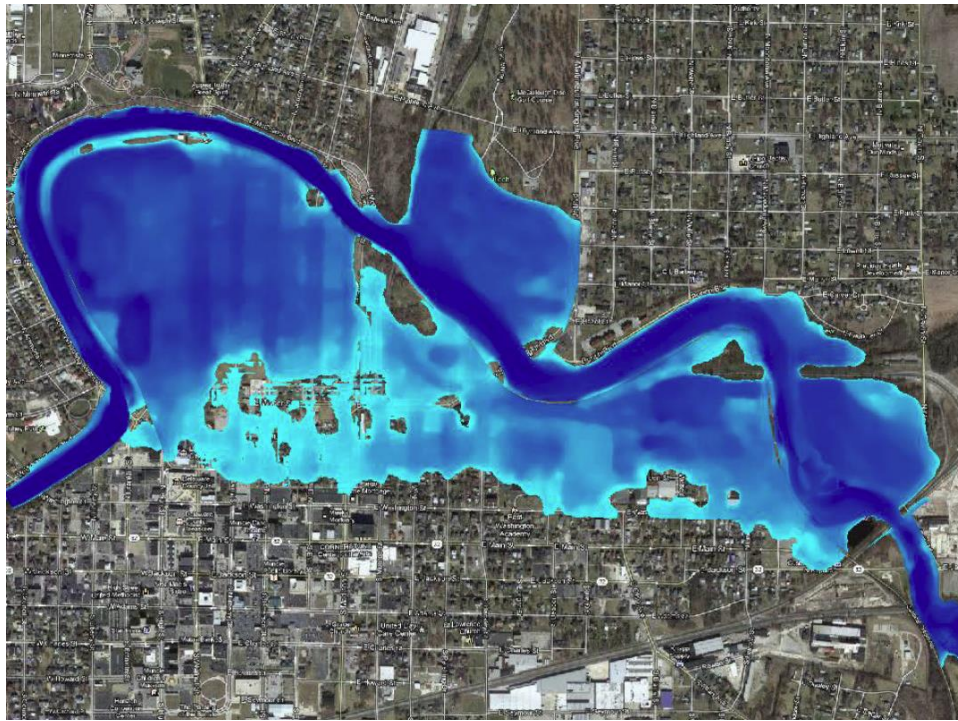
Figure 39. Example HEC-RAS flood inundation map showing water depth. (*Source:* USACE 2016)

5.6.4   Uncertainty in Breach Initiation and Progression

As noted in the Wahl literature survey and workshop, breach prediction equations based on empirical case studies have significant uncertainty, and formation time is particularly difficult to predict. Uncertainties related to dam breach initiation and progression are a dominant source of uncertainty in estimating the consequences of potential dam failures. The major sources of this uncertainty are:

1. The inherent challenges of obtaining observational data on a dam breach in progress; that is, the number of calibrating cases is small.

2. The large number of parameters affecting the predictions and the wide range of those possible parameter values related to the erodibility of earthen materials.

3. Difficulties in determining the erosion susceptibility of dam and embankment materials

Wahl (1998 and 2004) have described and discussed the results of several published modeling studies that explored the sensitivity of peak discharge, flood elevation, and timing of the flood wave peak to specific breach parameters.

Recent studies on uncertainty in breaching characterization. There have been a number of recent studies attempting to quantify the uncertainty associated with breaching predictions.

Zagonjolli (2007) in a dissertation at Delft University of Technology developed the physics-of-failure model BREADA for simulating the gradual failure of embankments due to overtopping and calibrated it against historical dam failures. The study also attempts to use data analytic methods (data mining) to understand the accuracy and error of breach models, using a data set of 23 dam failures, mostly dams of small and medium height. The dissertation uses sensitivity analysis to characterize these uncertainties. The study also provides a comprehensive review of empirical and physics-of-failure models as of its publication date.

Both the BREADA model and data analytics methods were tested by Zagonjolli (2007) against the failure of the Schaeffer Dam in Fremont County, CO, which overtopped in 1921:

> The results show a wide range of predicted peak outflows. When using empirical equations, the peak outflow discharge varies in a range of ±50%. Though the best performing empirical equation for the Schaefer dam can be identified, this does not imply its direct applicability to other failure events. When the dam breach models BREACH and BREADA are used the predicted peak outflow varies in a narrower range depending on the assumptions and selected parameters. Good results are obtained from the […] data mining model that predicts only a 10% lower peak outflow than the recorded one.

Kim and Sanders (2016) applied breach modeling and flood routing to two South Korean dams that failed by overtopping in 2002 during Typhoon Rusa. The uncertainties reported deal not only with breaching but also with the entire hydrodynamic modeling of the flood plain. The study concludes that

> an uncalibrated 2D hydrodynamic flood model is capable of predicting flood heights from an extreme rainfall event causing multiple dam failures with an accuracy of 0.4 m and flood extent with an agreement of 86–87% when all important sources of flood water are incorporated into the model and high-quality topographic data are used with vertical accuracies of 0.15–0.20 m.

Peter et al. (2018) developed a physics-of-failure breaching model based on earlier work from many studies and then calibrated its predictions against the set of 15 failures summarized in Wahl (1998) using a Bayesian inverse updating method. This is a methodology now popular in the aerospace industry and in climate change modeling (Wynn et al. 2001), but the results for uncertainty bounds are not significantly different from other recent results.

Addressing uncertainty. USACE (2014b) recommends several strategies for addressing the uncertainty in analyses of dam breach initiation and progression. Engineering judgment is required in all aspects of the analysis. Analysts are advised to use site-specific geotechnical information to help identify reasonable breach shapes (e.g., side slopes of a breach section) and to determine the appropriateness of a particular

physical or empirical modeling approach. Several different regression-equation methodologies should be used to estimate breach parameters and failure times, and physics-of-failure computer models of breaching, such as NWS-BREACH, WinDAM, and HR-BREACH, should be used to provide additional insights and estimates.

A sensitivity analysis should be performed by running models with each of the different sets of parameter estimates. Results should be checked for reasonableness by examining breach flow rates and velocities at different stages of breach development. If the model is showing high flow rates and velocities at the full breach development time and when the breach has reached its full size, that is an indication that either the breach is too small or the development time is too short. If flow rates and velocities through the breach become very small before the breach has reached its full size and development time, that is an indication that the breach size may be too large or the development time too long.

Note that the impact of uncertainties in breach initiation and progression on peak flow and flood elevation decreases with increasing downstream distance from the failed dam through attenuation. Different sets of breach parameters and failure times may result in widely divergent outflow hydrographs at locations close to the breached dam; but as the hydrographs are routed downstream, they will tend to converge (Wahl 1998; USACE 2014b). A primary reason for this convergence is that the total volume of water released from the dam is essentially the same (determined by the volume of stored water behind the dam at the time of failure, plus inflows). Factors affecting the rate of convergence include the volume of the outflow hydrograph, steepness in the rise of the outflow hydrograph, slope of the downstream reaches, available storage in the downstream floodplain, and roughness of the downstream reaches.

6. OPERATIONAL RISK

An operational risk is the potential loss resulting from "inadequate or failed internal processes, people, and internal systems, or from external events." This definition is adapted from the financial sector, in which operational risk is specifically defined (Basel Committee on Banking Supervision 2004), but it has been widely adopted by the chemical processing, oil and gas, and other hazardous industries (Meel et al. 2007). The aviation industry uses a similar definition of operational risk based on systems engineering (FAA 2000).

Operational risk stands apart from risks associated with physical aspects of the dam, such as its structural integrity or its capacity to withstand earthquakes or landslides. Operational risk is related to the hazardous results occurring from an unusual combination of common operational events (Hartford et al. 2016). It may reflect both errors of commission and of omission. Fully enumerating the many such rare chains of events in a PRA is possible but seldom practicable.

In contrast to the consideration of extreme loads against structural or geotechnical capacities, experience has shown that the majority of dam incidents, and even many dam failures, do not result from extreme loads but rather from operating events. These incidents and failures occur because an unusual combination of reasonably common events occurs, and this combination may have an adverse outcome. Examples of reasonably common individual events include moderately high reservoir inflows, the SCADA system early warning failure, spillway gate(s) unavailability because of maintenance, operator error, and high pool level. When multiple such events occur in combination, the result may be an incident or even a failure, even though none of the individual events was extreme on its own.

6.1 DAM OPERATIONS

Dam operations are multidimensional activities influenced by factors including but not limited to: corporate ownership and management structures, regulations, water and power markets, logistics and technology. For example, an individual dam may be owned by one organization and operated by another. In other cases, a series of dams may be owned by a single organization and operated as a system. The retention, release, and allocation of water from dams are influenced by a variety of factors, ranging from power purchasing agreements to public water supplies.

In the energy sector, operational risk normally includes health and safety (individuals), productive asset management (processes), information security (SCADA and systems), and environmental impacts (external disturbances). European chemical industries submit data to the Major Accident Reporting System, and a database for chemical companies in the United States was created from risk management plans submitted by facilities subject to the Environmental Protection Agency's chemical accidental release prevention and response regulations at 40 CFR Part 68 (Meel et al. 2007). In the dams sector, the National Performance of Dams Program[9] serves a similar if less formal purpose.

The aspects of a dam system of concern for operating risk include, among other components and processes:

- Equipment failures (i.e., mechanical and electrical reliability)
- SCADA systems
- Human factors
- External disruptions: debris, ice, reservoir landslides, internal fires
- Communication systems availability
- Site access during storms or winter conditions
- Maintenance practices

- Malicious attack (hacking, terrorism, sabotage)

Each of these describes a collection of related considerations, and all of these possibly interact to create chains of operational events that may lead to adverse performance and possibly to failures.

Over time, engineered systems require rehabilitation, repair, and replacement as wear and tear from basic, cyclic, and extreme loading conditions degrade components. Hence, there is a need for operations to include maintenance planning and other dam safety activities. Finally, dam operations are increasingly accomplished using sophisticated monitoring and control technologies that enable quick response amid changing conditions.

From a dam safety perspective, major historical dam failures have usually been caused by complex interactions between both physical and human factors (as well as organizational factors) which lead to adverse conditions. Such interactions may proceed over many years or decades before issues are detected or manifested. According to Norstedt et al. (2008), "research has demonstrated that many accidents can be explained by a gradual drift toward an unsafe condition as a result of economic pressure–inducing reorganizations, cost cuts in maintenance, or delayed retrofits of technology."

6.2 HUMAN FACTORS AND RELIABILITY

The root causes of primary dam failure mechanisms are physical factors that affect dam safety. Human factors, which comprise the decisions, actions, and inactions of dam owners and operators, also influence dam safety. Human reliability failures can originate from decisions made during construction or operation. Hartford et al. (2016) note that, "for spillway systems, many of the human errors occur during the operations phase, but they also occur in design deficiencies, maintenance practices or strategies, lack of updated safety manuals and upper management decisions regarding such systems." Sowers (1993) reports that 58% of civil and geotechnical failures originate from design decisions, with one-third of those failures occurring during construction and two-thirds during operation.

Dams and spillway systems are inherently complex, and human error plays a critical role in the success or failure of these systems. To account for the potential negative impacts posed by human failure events, or ameliorating impacts resulting from mitigating actions, human reliability analysis (HRA) is used. HRA is "a structured approach used to identify potential human failure events and to systematically estimate the probability of those errors using data, models, or expert judgment."[35] HRA is typically performed by a multidisciplinary team responsible for assessing PRAs, plant design and behavior, engineering, plan operations, procedures, monitoring and control, and cognitive and behavioral science. These various factors can all play a role in human reliability and are used as input to HRA.

Many HRA methods were originally developed for NPP or aerospace application but can be adapted for use in the risk analysis of dam systems. Among the available methods, Hartford et al. (2016) reports the Technique for Human Error Rate Prediction (THERP) and A Technique for Human Event Analysis (ATHEANA) as most suitable for dam spillway operation. Several reports have been published on the inclusion of HRA in the analysis of water and other civil engineering infrastructure (Bea 2006; El-Shahhat et al. 1994; Grigoriu 1984). A detailed review of the use of HRA in dam safety and hydropower operations is provided by Hartford et al. (2016, Chapter 8).

---

[35] https://www.nrc.gov/docs/ML1025/ML102560372.pdf (accessed November 2019)

6.3 SCADA SYSTEMS

Modern large dams are equipped with automated SCADA systems. These systems combine sensors with industrial controllers, computers and data storage, and communication links and facilitate remote or automatic control of components of the flow-control system.

This sequencing of information from sensors to controllers can increase reliability concerns, particularly since programming may be locally customized. The Taum Sauk failure (discussed later in this section) was related to SCADA misperformance (Regan 2010), and a number of other incidents are summarized in the NPDP.[9] Many dam failure precursors may be detected by onsite personnel before equipment detection may occur, and the lack of onsite workers can prove detrimental if site conditions deteriorate (Hartford et al. 2016).

SCADA system reliability is essential for protecting equipment and ensuring dam safety. Some installations use equipment built to military-grade standards to withstand extreme environmental conditions (e.g., temperature, moisture, vibration, and voltage extremes). Programming errors and component failures may still incapacitate SCADA systems and negatively affect the communication of sensor readings to an operator. Consequently, many sensitive facilities are equipped with redundant hardware and communications capability to reduce risk. In addition, many systems rely on external power to activate equipment and are equipped with onsite emergency backup generators in case of loss of offsite power.

A SCADA system usually has an emergency alarm capability and, based on operator judgment, can be overridden by the operator (Hartford et al. 2016). Remotely operated SCADA systems typically rely on an integrated communication system accomplished using internet connection and corporate information systems. Some organizations use satellite-based communication, which bypasses land-based network security issues and reduces susceptibility to cyber-attack. Malicious cyber-attack has been widely identified as a potential vulnerability of SCADA systems (Konstantas 2016; EU 2016; NCS 2004; OAG 2012). An Inspector General report at the US Department of Interior recently identified "industrial control systems" at USBR dams as subject to cyber-attack from insider threats (USDOI 2018).

Note that although the rapid development and automation of information and communication technologies have enabled improved surveillance and remote monitoring, various accidents and incidents have been caused by an overreliance on these technologies, misoperation, or malfunctioning equipment. For example, in 2005, the Taum Sauk pump storage upper reservoir failed because of overtopping erosion of the dam embankment.[36] Upon investigation, the cause of the failure was attributed to malfunctioning water level monitoring equipment that became dislodged and was unable to record proper readings. With measurements reading lower than actual conditions, and a secondary backup probe installed at an improper elevation, the reservoir level could not be accurately controlled. Near the end of a pumping cycle to fill the upper reservoir, overtopping of the embankment occurred and led to erosion and uncontrolled reservoir releases. Visual observation of the reservoir was nonexistent, with water control relying entirely on monitoring equipment. Fortunately, personnel were onsite shortly after overtopping occurred and were able to control the water level. Erosion led to emptying of the full reservoir. This case study exemplifies the importance of properly functioning SCADA and monitoring equipment and the need to consider nontraditional failure modes in risk assessments.

Currently, SCADA systems are rarely incorporated in current dam safety risk analysis, as the systems analyses and modeling approach to this aspect of dam system performance are poorly explored. This is not the case for other systems risk modeling as explored and used in applications to chemical plant safety

---

[36] http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/ (accessed November 2019)

(AIChE 2009) and NPP safety (NRC 1999). The lessons learned in these other application areas indicate that the range of errors associated with sensor and SCADA systems is broad, and not all of these can be described and modeled in detail. As a result, analysts default to ways of modeling sensors by their frequency of erroneous readings, possible inaccuracy (bias), and possible imprecision (noise).

From a systems engineering point of view, the introduction of communications and controls associated with SCADA systems adds dynamics and feedback to dam system behavior. Current risk analysis deals mostly with static systems. That is, there are few feedback loops in the behavior of a system. Inputs are translated directly to outputs, although they may be perturbed by random disturbances. When sensors are introduced into a system, information on prevailing performance indicators is communicated to controllers and human operators, and control actions made in response may change the state of the operating system and introduce nonlinear behaviors to the system (Leveson 2012).

6.4 CONDITION MONITORING AND MAINTENANCE

Federally owned and non-federal, FERC-licensed dams have condition monitoring and maintenance programs. Condition monitoring primarily involves data collection (visual observation and instrument readings), processing, and evaluation to continuously evaluate dam safety. Visual observation may include inspecting the dam and appurtenant structures to identify any unusual conditions that could jeopardize dam safety. Instrumentation involves the use of electrical and mechanical instruments or systems that measure pressure, flow, movement, stress, strain, and temperature. For example, Table 7 shows the FERC minimum recommended monitoring matrix for existing dams (FERC 2017) Given the common dam failure mechanisms described in Section 4.2, various methods of visual inspection are typically practiced for identifying safety-related dam issues. According to the British Columbia *Inspection & Maintenance of Dams: Dam Safety Guidelines* (British Columbia 2016),

- Embankment dams should be inspected for the most threatening deficiencies, which include longitudinal or transverse cracking and misalignment of adjacent dam portions.

- Concrete dams should be inspected primarily for structural cracks, foundation or abutment weakness, or deterioration due to alkali-aggregate reaction (also known as alkali-silica reaction; ASR).

- Spillways, outlets, and gates should also undergo inspection where accessible.

- Safety signage should be inspected for deficiencies resulting from vandalism, readability, overgrowth, or outdated information.

To further support condition monitoring beyond visual inspection, various instrumentation devices may be used to monitor dam conditions. FERC engineering guidelines describe various types of instrumentation commonly used to monitor water level and pressure; seepage and leakage; surface, internal, and joint movement; structural stress and strain; temperature; seismicity; and post-tensioned anchor loads (FERC 2017, Chapter IX-1).

Table 7. FERC minimum recommended monitoring for existing dams. (Source: FERC 2017)

TYPE OF MEASUREMENT	LOW-HAZARD POTENTIAL DAMS — ALL TYPES	SIGNIFICANT AND HIGH-HAZARD POTENTIAL DAMS					
		EMBANK-MENT	CONCRETE GRAVITY	ARCH	BUTTRESS	SEPARATE SPILLWAY AND/OR OUTLET	INTEGRAL POWER-HOUSE
VISUAL OBSERVATION [2]	X	X	X	X	X	X	X
RESERVOIR LEVEL		X	X	X	X	X	X
TAILWATER LEVEL		X	X	X	X	X	X
DRAIN FLOW, SEEPAGE, AND LEAKAGE		X	X	X	X	X	X
PORE/UPLIFT PRESSURE [3]		X	X			X	X
SURFACE SETTLEMENT							
SURFACE ALIGNMENT			X	X	X	X	X
INTERNAL MOVEMENT							
JOINT/CRACK [4] DISPLACEMENT			X	X	X	X	X
FOUNDATION MOVEMENT [5]		X	X	X	X	X	X
SEISMIC LOADS [6]		X	X	X	X	X	X
LOADS IN POST-TENSIONED ANCHORS [7]			X	X	X	X	X

[1] This table is provided to help explain the guidelines. Refer to the text of Section 9-4 for more detailed discussion of minimum recommendations. Additional instrumentation should be used to address specific concerns.

[2] Visual observation consists of walking tours of the crest, toes, abutments, etc.

[3] Using existing piezometers, observation wells, or foundation drains; or using existing or new piezometers or observation wells from dams with reduced uplift assumed in stability analysis or that do not meet criteria using conservative estimate of the phreatic surface.

[4] Only on structurally significant joints or cracks that have visible displacement.

[5] Should be considered for dams on compressible or weak foundations.

[6] Should be considered on a case-by-case basis for dams in seismic zones 3 and 4.

[7] For anchors that are required to meet stability criteria, loads should be measured wherever it is possible to measure anchor loads, or anchors should be modified to measure loads.

Maintenance may consist of planned or unplanned activities aimed at maintaining component integrity and operation, mitigating or correcting unusual or adverse conditions, or reducing or eliminating component failures. DOE (2016) identifies several maintenance strategies commonly used in hydropower facilities and equally applicable to dams in general:

- **Time-based preventative maintenance**: Inspection and maintenance activities are performed following a scheduled timeline. An example is the maintenance that is done on spillway gates every year before the spring freshet. The maintenance is performed each year in time for the period of peak need for gate availability.

- **Condition-based maintenance:** Inspection and maintenance activities are performed when operational conditions warrant such action. An example is the monitoring and maintenance performed on hydropower generators that operate nearly continuously without a window for unplanned shutdowns. Poor availability of such machinery can be expensive and time consuming.

- **Corrective (reactive) maintenance**: Inspection and maintenance activities are not planned and occur only after component failure or misoperation. No monitoring systems or instrumentation is required when corrective maintenance strategies are used, and such strategies are typically limited to components that are not critical to system operation or dam safety and that can be replaced quickly or at minimal cost.

Following inspection or based on routine or nonroutine maintenance needs, the Province of British Columbia, Water Management Branch (British Columbia 2016) outlines various maintenance guidelines for ensuring continued safe dam conditions. Routine maintenance may include debris removal, access road upkeep, riprap modification, concrete sealing, drain cleaning, monitoring point protection maintenance, and operating equipment security maintenance. For embankment dams, maintenance should include vegetation control, crest and slope stability, and burrowing animal control. Concrete dams have fewer routine maintenance needs. For both embankment and concrete dams, maintenance needs also include drainage cleaning and maintenance of sealing systems, pumping equipment, monitoring equipment, and instrumentation. Spillway maintenance activities should include the removal and disposal of floating debris; repair or replacement of debris containment structures; removal of soil, sediment, or rock accumulation; and removal of any beaver dams. Outlet gate maintenance should include annual or semi-annual operation of the gates through their full operating range to prevent rust buildup and should typically occur during low storage periods or low flow periods.

While more frequent physical or visual inspections may increase risk identification, that is not always the case. As highlighted in the 2018 report on the Oroville Dam spillway incident (IFT 2018), the underlying conditions that led to spillway damage and the eventual evacuation order probably would not have been identified if more frequent inspections had been conducted. The report highlights an overreliance on several traditional practices and stresses that "periodic comprehensive reviews of original design and construction and subsequent performance are imperative" (IFT 2018).

6.5 INTERACTION WITH THE POWER GRID

According to DOE's *2017 Hydropower Market Report* (Uría-Martínez et al. 2018), the US hydropower fleet consists of 2,241 plants with a total capacity of 80 GW, representing 7% of the nation's electricity generation capacity and 6.3% of electricity generation output. Most of this hydropower capacity is provided by dammed reservoirs, and the energy demands placed on hydropower dams can result in various changes in hydraulic conditions, component operations, and system response.

The power system stability and reliability provided by hydropower (and other energy resources) is essential to national security and uninterrupted information flow and commerce. Hydropower generation is typically highly consistent, predictable, and dependable and can provide near-instantaneous response to changes in load and demand (DOE 2016). Many facilities operate in run-of-river mode, in which electricity generation will largely correlate with water inflows to the system. Storage facilities, on the other hand, can provide significant seasonal or daily storage and respond to changing power demand or hydrologic conditions. Peaking hydropower operations provide a similar service but typically generate only when there is high power demand (McManamay et al. 2016).

In certain regions and seasons, the increasing use of renewable energy (in particular solar and wind) has created shifts in energy supply and demand. The California Independent Systems Operator Corporation has identified a significant trend in daily non-solar (predominantly wind) energy demand resulting from the increased use of these energy sources in California. The emerging trend is to reduce the net grid demand for renewables in the middle of the day (Figure 40), thus creating increased demand on the responsiveness of peaking-power generators like hydropower. The California "duck curve" (so called because of its shape), is expected to become more significant and emerge in other locations as these

variable renewable sources become more widely used. As a result of the increased flexibility demanded, hydropower equipment and components may increasingly undergo more start-stop cycles, operate below rated conditions, and require more frequent gate movements. Consequently, component conditions may degrade more rapidly, and maintenance regimes and operational decision-making may experience increased challenges. These consequences increase dam safety risk and may result in more frequent operational failures (CEATI 2016).
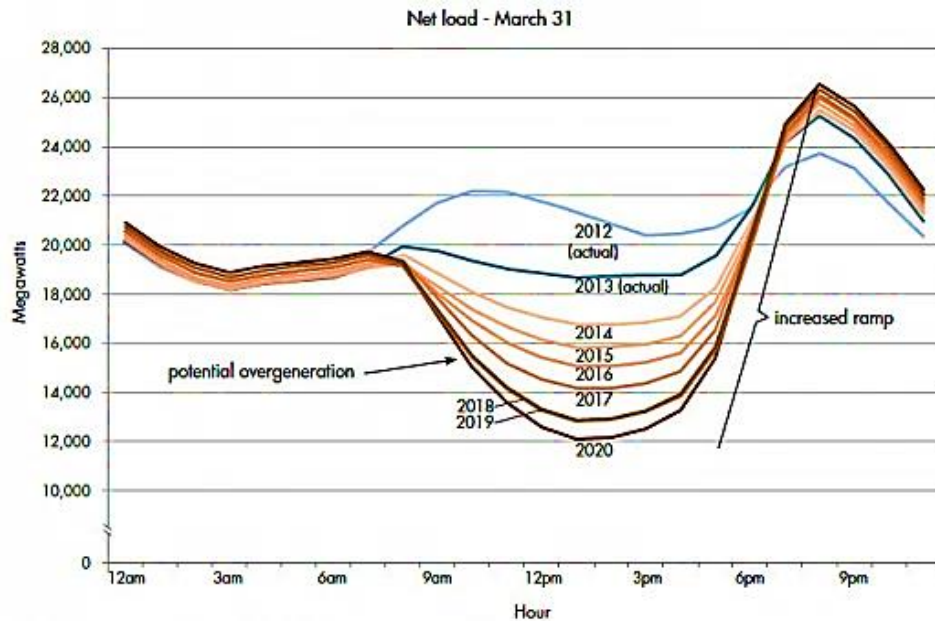
Figure 40. California's "duck" curve showing net-of-renewables grid load in California on March 31, projected to the year 2020. (*Source:* CAISO, reprinted from DOE [2017])

6.6 ADDRESSING OPERATIONAL RISKS

Once general categories of operational risk classes have been identified, there are a limited number of approaches to their appraisal and quantification. The different categories of operational risk may best be approached using different methodologies.

The most common methodologies are those based on subject matter expert (SME) judgment. An example is USACE's use of expert panels (USACE-USBR and USACE 2017). The experts have specific knowledge, experience, and information regarding the risks to be appraised. The simplest SME approach is the use of a self-assessment questionnaire. These questionnaires are used to gather information on the impact and frequency of events and on the effectiveness of mitigation or intervention. On the other extreme is the expert elicitation protocols more commonly used for traditional event tree analysis.

An alternative methodology is scenario analysis. It uses hypothetical operational risk scripts as story lines, which are analyzed by groups of experts. While scenario analysis is more common in financial sector risk analysis (Hassani 2016), an example in the dams sector is FEMA's use of dam failure scenarios in estimating potential loss of life (FEMA 2011). This method is usually implemented using workshops involving experts from a variety of disciplines and a professional facilitator. The process starts by defining a hypothetical situation and attempting to achieve a consensus opinion on the likelihood the scenario would occur and the associated consequences.

A third methodology is to rely on internal or external databases of historical failures, near-misses, or precursor events, possibly similar to nuclear sector OpE databases. An example is the FERC-supported *National Performance of Dams database*. However, classical statistical approaches tend to be ineffective for chains of low-frequency, high-consequence events both because of their rarity and because so many potential combinations of events may exist. For the dam industry, the NPDP[9] provides one such database. In other hazardous industries, such as chemical processing, these databases are often more expansive, and reporting may be legally required, which is not the case for dams.

A fourth methodology is systems simulation, which can be used to model operational risks and to spot emergent behaviors that might otherwise be difficult to identify. An example is Vattenfall's use of Systems Dynamics on its Göte River cascade (Ascila et al. 2015). This approach is newer and less widely used than the others. Systems modeling using simulation (Hartford et al. 2016), systems dynamics (Pavlovic 2016), or related techniques may help to identify potential failure paths.

6.6.1   Systems Engineering

A systems analysis approach to dam safety involves comprehensive consideration of all components of a dam and their interactions, wherein not only are the risks and risk mitigation important for safety, but understanding how to accommodate the risks is critical as well. The term "system" refers to the set of interacting, interrelated, and interdependent elements that dictates a complex whole; while "systems analysis" refers to determination of the plans, design, and operational strategies through the use of scientific methods (Hartford et al. 2016).

The risks posed by a dam system can be challenging to assess because of the variability of the organization and loading conditions associated with components. Traditional treatment of risk as a "single-component" deterministic issue can be detrimental to the perceived reliability of a dam system. Safety analysis that incorporates probabilistic analysis and simulation techniques for assessing variability in component interaction is crucial for understanding and assessing the risks. In addition, a departure from a single-component focus toward a more holistic approach encompassing a multi-interactive systems analysis is necessary.

6.6.2   Flow Control

For risk analysis in the context of systems analysis, "flow control" refers to the wide array of elements—including structures, equipment, sensors, communication facilities, personnel, management arrangements, and policies—that implement the handling of water through the reservoir and past the subject dam to the downstream reach of the river. In general, the main components of flow control are the catchment, reservoir, dam, spillway, and other waterways (e.g., emergency outlets, power generation, bottom drain).

Reservoir and dam operation can be controlled with SCADA equipment and human interaction. Although the use of these control mechanisms is intended to impart a culture of safety with respect to reservoir and dam control, human-operator error and programming errors and component failures associated with SCADA systems are possible.

6.6.3   System Simulation

Simulation or physics-of-failure modeling can be a crucial part of identifying and predicting operational system risks such as hydrological system inflows, since the operation of the dam functions is dependent on the magnitude and timing of reservoir inflows. Although deterministic models are adequate for predicting systems with a high degree of certainty in their inputs, hydrological systems do not contain such degrees of certainty. Recent research is incorporating stochastic approaches in hydrologic modeling by developing and using probability distributions of the output of deterministic models for random parameters.

The elements that make up flow control, as discussed in Section 6.6.2, can be regarded as a dam system. The NPDP[9] says that the "successful performance of the dam system depends on the aggregate satisfactory performance of the system that prevents a failure and uncontrolled release of the reservoir". Whereas physical flow through a dam can be modeled easily and reliably, the interaction of the physics-based operation of the dam system with the nonlinearity of the communication and controls of the SCADA system presents challenges.

An example where failure was caused by a complex chain of events is the 2017 Oroville Dam spillway incident (IFT 2018). A series of events and situations caused a structural foundation failure, which resulted in the deterioration and failure of the spillway structure. This was followed by extreme downstream erosion. That the event was caused by a systemic failure of design and construction practices, site conditions, and post-event response depicts the complex interactions among very simple and prevalent industrial, physical, and human factors and their roles in the sequence leading to such a disaster.

Modeling the complexity of a dam system at the systems level is challenging because of the nonlinearity and randomness of the interactions. Modeling using traditional engineering risk analysis does not address the reliability of physical dam components in conjunction with their integration with communication and control systems (Regan 2010). Overcoming these issues requires a simulation approach.

7. SOFTWARE TOOLS FOR DAM SAFETY RISK ANALYSIS

This section provides an overview of software tools used for dam safety risk analysis projects, presenting a brief description of selected tools. Dam safety risk analysis also commonly employs specialty engineering software tools for structural, geotechnical, hydrologic and hydraulic analyses. The latter group of tools are not surveyed here.

Note: The mention of specific software tools in this section does not constitute endorsement or approval for any specific use by the NRC or ORNL.

7.1 INTEGRATED DAM SAFETY SOFTWARE

Integrated dam safety software combines the identification of categories of uncertainties, tools for fault tree or event tree analysis, and consequence estimation. Sometimes these integrated applications also combine other analytical or statistical tools. The number of available applications is limited, and most have been developed by dam owners and operators, or regulators.

7.1.1 FEMA Risk Prioritization Tool for Dams

The FEMA Risk Prioritization Tool (URS Group 2008) is a screening tool developed under contract to FEMA as a way for dam owners and operators to quickly prioritize safety risks among dams in a portfolio. It is based on qualitative risk analysis and expert judgment rather than detailed quantitative modeling. A description of this tool is provided at the FEMA website:[37]

> The *Risk Prioritization Tool for Dams* is a standards-based decision-making tool for risk-based dam safety prioritization to be used by state dam safety regulators throughout the country to identify those dams within a large inventory that most urgently need attention and then allocate resources accordingly. Once priorities are judged, risk acceptance or tolerability is a matter of policy that will vary from state to state. The tool is quick and easy to implement; applicable to any type or number of dams; accommodates the broad differences between owners and information known about each dam; avoids subjectivity and unnecessary bias; and is defensible and reproducible.

7.1.2 DAMRAE-U (USACE)

According to the contractors who developed DAMRAE-U under contract to USACE (Srivastava et al. 2012),

> Based on a generalized event tree algorithm, a deterministic model (DAMRAE) was developed for the US Army Corps of Engineers to support the dam safety risk assessment. With an objective to incorporate the uncertainty analysis functionality for the event tree-based risk models, we extend the DAMRAE framework to develop a generic uncertainty analysis tool (DAMRAE-U) for dam safety risk assessment. DAMRAE-U provides a convenient way to efficiently characterize, propagate, and display the outcomes of uncertainty analysis. DAMRAE-U is structured to analyze knowledge uncertainty for the event tree variables and natural variability associated with flood and earthquake loadings. It also provides for separating the effects of uncertainty in the existing condition of the dam system on which the event tree model is dependent. In this paper, we present the details of the developed computational framework. Also, an

---

[37] https://www.fema.gov/media-library/assets/documents/13523 (accessed November 2019)

example risk model to illustrate the inputs and outputs of the framework and the implementation of tolerable risk evaluation incorporating uncertainty in risk estimates is included.

7.1.3   DSS-WISE™ Lite (FEMA)

The Decision Support System for Water Infrastructure Security (DSS-WISE)[38] is a two-dimensional dam and levee flood modeling and mapping software program developed by the National Center for Computational Hydroscience and Engineering at the University of Mississippi with FEMA funding.

It runs on a browser-based platform providing access to a secure, web-based environment. The program allows a user to set up and run dam and levee breach scenarios. DSS-WISE solves dynamic shallow-water equations and provides results within about half an hour after user inquiries. DSS-WISE Lite is used internally by federal agencies and state dam safety offices for dam safety studies and preparing EAPs. A post-processing module generates flood hazard maps and carries out loss-of-life analysis based on a USBR methodology.

7.1.4   iPresas Risk Analysis™

The iPresas tool[39] is a risk analysis application developed at the Technical University of Valencia. It is described by the developers as follows;

> The main objective of *iPresas* is to support integrated safety and security management in dams and other critical infrastructures. This support is based on the development of risk models and the application of Risk Analysis techniques, as well as the development of software to fulfill these needs. iPresas also offers services in analysis and performance evaluation of dams and other critical infrastructures. In this website you will find information regarding our activities, services, interests, publications, software... We invite you to navigate through it and to send us any suggestion or comment you might find of interest.

7.2   EVENT TREE ANALYSIS SOFTWARE

The use of event tree analysis for dam safety risk evaluation was pioneered by BC Hydro and USBR in the 1980s. Event tree analysis and the related fault tree analysis methods applied to dam safety risk analysis are described in Hartford and Baecher (2004) and in more general terms in Pate-Cornell (1984).

An event tree is a graphical representation of the chains of events that could lead from some initiating event or hazard occurrence to system failure. As the number of events increases, the diagram fans out like the branches of a tree. A presumption of event tree analysis is that data and engineering judgement are most powerful at detailed levels of dam behavior that involve specific models, parameters and assumptions and less powerful at the aggregate level of an entire dam. Thus, a decompositional approach is warranted. Event trees are commonly used to analyze "open systems" in which possible outcomes are inferred inductively, so it is possible that some failure mechanisms will not be captured in a particular analysis. This is in contrast to fault tree analysis, described in Section 7.3.

Today, event tree analysis is the principal analytical approach to dam safety risk worldwide. Many commercial-off-the-shelf software products are available to perform event tree analysis. Few of these

---

[38] Available at https://www.ncche.olemiss.edu/dss-wise-lite-fema/ (accessed November 2019)
[39] http://www.ipresas.com/en/ (accessed November 2019)

were developed specifically for dam safety. Most are components of statistical decision theory software, which is a much larger market. PrecisionTree™, which is a component of a larger suite of software products—DecisionSuite™—provided by Palisade Software Corporation of Ithaca, NY, is perhaps the largest market shareholder in the dam safety community.

Among the vendors providing event tree analysis software are (alphabetically)

- DATA—TreeAge Software
- DecisionPro—Vanguard Software Cooperation
- Event Tree Analysis (ETA)—SoHaR
- Event Tree Module—Isograph
- PrecisionTree—Palisades Software
- RAM Commander's Event Tree Analysis Module—ALD
- RiskSpectrum—PSA software

7.3 FAULT TREE ANALYSIS SOFTWARE

The use of fault tree analysis is uncommon in dam safety and risk evaluations. It has been suggested by Bury and Kreuzer (1985, 1986), Kreuzer and Bury (1984), and McCann (2002). Johnson (1999) has discussed fault trees for bridge scour problems. It is, however, widely used for modeling the reliability of gates and hydraulic structures (Patev et al. 2013).

Fault tree analysis, in contrast to event trees, is a deductive logic based on set theory and Boolean algebra. In developing a fault tree model, a top-down approach is used. Beginning with a top failure event, one seeks causes that would lead to its occurrence. Next, failure mechanisms or event occurrences are sought for these causes to be realized. A failure mechanism is a description of how a failure mode can occur: it is a system state. Fault tree analysis is widely used in mechanical and electrical reliability studies of "closed systems," that is, those in which all the complements and their relationships are identifiable.

Among the vendors providing fault tree analysis software are (listed alphabetically)

- EMFTA: Open Source Tool for Fault Tree Analysis—CMU
- Fault Tree Analysis—Isograph
- Fault Tree Analyzer—ALD
- Fault Tree Diagram Software—SmartDraw
- ITEM Toolkit Fault Tree Analysis—Item Software

7.4 MONTE CARLO SIMULATION

Monte Carlo methods (or MC simulation) comprise a broad category of numerical methods for solving stochastic models (and complex integrations). They use random sampling and sampling statistics to obtain quantitative estimates with associated numerical uncertainty, which is quantified statistically. They are commonly used for models that are difficult to solve using other approaches. In physics-based problems like dam safety, MC methods are useful for simulating systems with many coupled degrees of freedom, or complex, correlated uncertainties. MC methods are common in risk analysis across a broad range of disciplines, from engineering to medicine to finance.

Among the vendors providing MC simulation software are (listed alphabetically)

- @RISK—Palisades Software

- Crystal Ball —Oracle
- GoldSim—GoldSim Software
- Model Risk—Vose Software
- Matlab and Simulink—The Math Works
- Risk Engine for Mac—Engineering for the Real World

8.   SUMMARY

This report presents the history and importance of dam safety in the US, major federal and state organizations engaged in dam safety, primary physical and operational considerations in dam engineering, principal features of dam safety risk assessment and modeling, critical aspects of operational risk, relevant software tools for dam safety risk analysis, historical dam failures, and insights from recent dam incidents and failures.

Despite a long history of dam stewardship, the US only recently instituted dam safety programs during the Carter Administration following the high-profile dam failures of Buffalo Creek (1972), Teton (1976), and Kelly Barnes (1977). Today, all states but one have adopted state dam safety programs. The current state-of-practice in US dam safety risk assessment has been used by the dam safety community for over 20 years and was adopted by FERC under the term *risk-informed decision making* (RIDM). RIDM enables structured, engineered approaches to identifying, classifying, and quantifying potential dam failures and provides a mechanism for dam owners, designers, operators, and regulators to communicate dam safety risk and mitigate concerns. More comprehensive PRA is practiced by the USACE, USBR, and many private sector dam owners; yet its implementation may be challenging because of gaps in knowledge, uncertainty associated with the physics of dam failure, and difficulty in communicating results with stakeholders. Whereas the nuclear industry has widely used PRA for decades, its application to dam safety is relatively new but maturing.

As dams continue to age beyond their design lives, they will be exposed to continued risk of large floods, earthquakes, and other hazards, and the threat of dam failure disasters may grow in the future. Climate change may exasperate this exposure, and shifting technological paradigms, cyber security threats, and operational demands may impact risk. Yet federal and state dam safety frameworks have provided a valuable safety net for preventing major calamities, and risk prioritization tools have been leveraged with success.

As dam owners and regulators (both federal and state) know well, funding to support dam safety, repair, and maintenance is low compared with the need. Given a recent ASDSO estimate of $64 billion needed to rehabilitate the nation's dams, and continued low funding, the financial needs will continue to grow. With luck, significant disasters such as those which occurred in the US before the 1980s will be avoided; yet, with more than 90,000 dams across the country and increasing at-risk populations, high-fatality and high-cost events are inevitable. Some risk, however small, is unavoidable. Yet it is in the interest of the nation to invest in dam upgrades and safety programs to sustain our critical infrastructure and protect downstream communities and infrastructure (including NPPs).

Given the potential threat that dam failure flooding poses to NPPs, this report supports the NRC in surveying the current state-of-practice in dam safety risk assessment. The information assembled herein is intended to aid the NRC in developing guidance on the use of PFHA methods and support the provision of risk information to NRC's licensing and oversight framework in the context of flooding hazards due to dam failure. Over time, the state-of-practice of dam safety will continue to evolve, yet many foundational principles described here will remain unchanged.

9. CITED REFERENCES FOR MAIN REPORT

AIChE (American Institute of Chemical Engineers). (2009) *Guidelines for Chemical Process Quantitative Risk Analysis*. AIChE, New York, NY, USA.

Allahverdizadeh, P., D. V. Griffiths, and G. A. Fenton. (2015). "The random finite element method (RFEM) in probabilistic slope stability analysis with consideration of spatial variability of soil properties." *Proceedings of the International Foundations Congress and Equipment Expo 2015*, San Antonio, TX, March 17–21, 2015.

Altarejos-García, L., F. Silva-Tulla, I. Escuder-Bueno, and A. Morales-Torres. (2014). "Practical risk assessment for embankments, dams, and slopes." *Risk and Reliability in Geotechnical Engineering* 437.

ANCOLD (Australian National Committee on Large Dams). (2003). *Guidelines on Risk Assessment*. Australian National Committee on Large Dams, Sydney.

ANS (American Nuclear Society). (1992). *Determining Design Basis Flooding at Nuclear Power Plant Sites*. American National Standards Institute/American Nuclear Society, La Grange Park, IL.

ANS (American Nuclear Society). (2008). *Probabilistic Seismic Hazard Analysis.* ANS 2.29-2008 (R2016). American Nuclear Society, La Grange Park, IL.

Ascila, R., G. Baecher, D. Hartford, A. Komey, R. Patev, and P. Zielinski. (2015). "Systems analysis of dam safety at operating facilities," USSD Annual Conference. Louisville, KY: United States Society on Dams.

Babb, A. O., and T. W. Mermel. (1968). *Catalog of Dam Disasters, Failures, and Accidents*. US Bureau of Reclamation, Springfield, VA.

Baecher, G. B. (2015). "Uncertainty in dam safety risk analysis." *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards* 10(2) 92–108.

Baecher, G. B., and J. T. Christian. (2003). *Reliability and Statistics in Geotechnical Engineering*. J. Wiley, Chichester, West Sussex, England; Hoboken, NJ.

Baecher, G. B., M. E. Pate, and R. deNeufville. (1980). Risk of dam failure in benefit-cost analysis. *Water Resources Research* 16(3), 449–456.

Baker, J. W. (2008). *An Introduction to Probabilistic Seismic Hazard Analysis*. From a report of the US Nuclear Regulatory Commission. Version 1(3), 72 pp. Available at https://web.stanford.edu/~bakerjw/Publications/Baker_(2008)_Intro_to_PSHA_v1_3.pdf. Accessed November 2019.

Baker, J. W., and C. A. Cornell. (2008). "Uncertainty propagation in probabilistic seismic loss estimation." *Structural Safety* 30(3), 236–252.

Barker, M., B. Vivian, J. Matthews, and P. Oliver. (2003). "Spillway gate reliability and handling of risk for radial and drum gates." *NZSOLD/ANCOLD 2003 Conference on Dams*, Wellington, New Zealand.

Basel Committee on Banking Supervision. (2004). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Bank for International Settlements, Basel, Switzerland.

Bea, R. (2006). "Reliability and human factors in geotechnical engineering." *Journal of Geotechnical and Geoenvironmental Engineering* 132(5), 631–643.

Bedford, T. and R. Cooke. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge, Cambridge University Press.

Beim, G. K., and B. F. Hobbs. (1997). "Event tree analysis of lock closure risks." *Journal of Water Resources Planning and Management* 123(3). doi.org/10.1061/(ASCE)0733-9496(1997)123:3(169)

Bhattacharjya, D., and L. A. Deleris. (2012). "From reliability block diagrams to fault tree circuits." *Decision Analysis* 9(2), 128–137.

Bier, V. M. (1997). "An overview of probabilistic risk analysis for complex engineered systems." Chapter 15 in *Fundamentals of Risk Analysis and Risk Management*, V. Molak, ed., Lewis Publishers, Boca Raton, FL.

Bonnet, M., A. Witt, K. Stewart, B. Hadjerioua, and M. Mobley. (2015). *The Economic Benefits of Multipurpose Reservoirs in the United States-Federal Hydropower Fleet*, ORNL/TM-2015/550, Oak Ridge National Laboratory, Oak Ridge, Tennessee.

Boultbee, N., O. Robson, S. Moalli, and R. Humphries. (2018). "Upper Lillooet River hydroelectric project: The challenges of constructing a power tunnel for run-of-river hydro projects in mountainous British Columbia." *Engineering* 4 (2), 260–266.

Bowles, D. S., L. R. Anderson, T. F. Glover, and S. S. Chauhan. (1999). "Understanding and managing the risks of aging dams: Principles and case studies." *Proceedings of the Nineteenth USCOLD Annual Meeting and Lecture*, Atlanta, Georgia, May 16–21, 1999.

Bowles, D. S. and M. Schaefer. (2014). "Probabilistic Flood Hazard Assessment, Dam Performance PRA and Nuclear Plant Risk." *Proceedings of the 9th Nuclear Plants Current Issues Symposium*, Charlotte, North Carolina, July 9, 2014.

Bradlow, D. D., A. Palmieri, and S.M.A.Salman. (2002). *Regulatory Frameworks for Dam Safety: A comparative study*. Law, Justice, and Development Series, The World Bank, Washington DC.

British Columbia. (2016) *Inspection & Maintenance of Dams: Dam Safety Guidelines.* Version 3. Province of British Columbia, Water Management Branch. Available at https://www2.gov.bc.ca/assets/gov/environment/air-land-water/water/dam-safety/2016_new_body_with_index_and_cover-final.pdf. Accessed November 2019.

Bury, K. V., and H. Kreuzer. (1985). "The assessment of the failure probability for a gravity dam." *Water Power and Dam Construction* 37.

Bury, K. V., and H. Kreuzer. (1986). "The assessment of risk for a gravity dam." *Water Power and Dam Construction* 38(2).

Calamak, M. and A. M. Yanmaz. (2014). "Probabilistic assessment of slope stability for earth-fill dams having random soil parameters." *Proceedings of the 5th International Symposium on Hydraulic Structures*, Brisbane, Australia, June 2014.

California DWR. (2014). *Potential Failure Mode Analysis Study Report: Oroville Dam*, FERC Project No. 2100-CA. California Department of Water Resources, Sacramento CA, p. 408.

Carturan, F., C. Pellegrino, R. Rossi, M. Gastaldi, and C. Modena. (2013). "An integrated procedure for management of bridge networks in seismic areas." *Bulletin of Earthquake Engineering*, 11(2), 543–559, Dordrecht, The Netherlands.

CDNR (Colorado Department of Natural Resources). (2010). *Guidelines for Dam Breach Analysis*. Colorado Department of Natural Resources, Division of Water Resources, Office of the State Engineer, Dam Safety Branch, Denver.

CEATI (Centre for Energy Advancement through Technological Innovation). (2016). *Dam Safety Technology Roadmap*, Report to the Dam Safety Interest Group, Centre for Energy Advancement through Technological Innovation. Montreal, 44 pp.

Chase, M. E. (2012). *Fragility Analysis of a Concrete Gravity Dam Embedded in Rock and Its System Response Curve Computed by the Analytical Program GDLAD_Foundation*. US Army Engineer Research and Development Center, US Army Corps of Engineers, Vicksburg, MS.

CNSC (Canadian Nuclear Safety Commission). 2015. *Regulatory Oversight Report for Uranium Mines, Mills, Historic and Decommissioned Sites in Canada: 2015*. Canadian Nuclear Safety Commission, Ottawa, Canada.

Cornell, C. A. (1968). "Engineering seismic risk assessment." *Bulletin of the Seismological Society of America* 58, 1583–1606.

deWolfe, G. F., D. V. Griffiths, and J. Huang. (2010). "Probabilistic and deterministic slope stability analysis by random finite elements." *Proceedings of the 2010 GeoTrends Biennial Geotechnical Seminar*, Denver, CO, November 5.

Ditlevsen, O. (1996). *Structural Reliability Methods*. Wiley, Chichester, New York.

DOE (Department of Energy). (2016). *Hydropower Vision: A New Chapter for America's 1st Renewable Electricity Source*. Wind and Water Power Technologies Office, US Department of Energy, Washington, DC.

DOE (Department of Energy). (2017). "Confronting the duck curve: How to address over-generation of solar energy," Office of Energy Efficiency and Renewable Energy, US Department of Energy, Washington, DC.

Donnelly, C. R. (2006). "Safe and secure—Risk-based techniques for assessing the safety of dams, Part I." *International Water Power and Dam Construction*, December, 28–33.

Donnelly, C. R. (2007). "Safe and secure—Risk-based techniques for assessing the safety of dams, Part II." *International water power and Dam Construction*, January, 34–41.

Duncan, J. (2000). "Factors of safety and reliability in geotechnical engineering." *Journal of Geotechnical and Geoenvironmental Engineering* 126(4), 307–316.

El-Shahhat Ashrat M., D. V. Rosowsky, and W.-F. Chen. (1994). "Accounting for human error during design and construction." *Journal of Architectural Engineering* 1(2), American Society of Civil Engineers. doi.org/10.1061/(ASCE)1076-0431(1995)1:2(84)

Ellingwood, B., and P. Tekie. (2001). "Fragility analysis of concrete gravity dams." *ASCE Journal of Infrastructure Systems* 7(2).

England, J. F., T. A. Cohn, B. A. Faber, J. R. Stedinger, W. O. Thomas, A. G. Veilleux, J. E. Kiang, and R. R. Mason. (2018). "Guidelines for determining flood flow frequency." *Bulletin 17C, US Geological Survey Techniques and Methods*, book 4, chapter B5, 148 pp. doi.org/10.3133/tm4B5.

EPRI (Electric Power Research Institute). (1984). A Probabilistic Risk Assessment of Oconee Unit 3 (NSAC-60), Electric Power Research Institute, Nuclear Safety Analysis Center.

Ericson, C. (1999). "Fault tree analysis—A history." *Proceedings of the 17th International Systems Safety Conference*, Orlando, FL.

ESHA (European Small Hydropower Association). (2004). *Guide on How to Develop a Small Hydropower Plant*. European Small Hydropower Association, p. 151.

EU (European Union). 2016. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." *Official Journal of the European Union*, Strasbourg, France.

FAA (Federal Aviation Administration). (2000). *FAA System Safety Handbook*, Chapter 15, "Operational Risk Management. Guidance." Federal Aviation Administration, Washington DC, p. 23.

Fell, R. (2015). *Geotechnical Engineering of Dams*. CRC Press, Taylor & Francis Group, Boca Raton, FL.

Fell, R., P. MacGregor, and D. Stapledon. (1992). *Geotechnical Engineering of Embankment Dams*. A. A. Balkema, Rotterdam; Brookfield, VT.

FEMA (Federal Emergency Management Agency). (2003). *Dam Safety and Security in the United States*. Federal Emergency Management Agency, Washington DC, p. 48.

FEMA (Federal Emergency Management Agency). (2004a). *Federal Guidelines for Dam Safety*. Federal Emergency Management Agency, Washington, DC, p. 63.

FEMA (Federal Emergency Management Agency). (2004b). *Federal Guidelines for Dam Safety: Hazard Potential Classification System for Dams*. Federal Emergency Management Agency, Washington, DC, p. 21.

FEMA. (2005). "Earthquake analyses and design of dams." In *Federal Guidelines for Dam Safety*. Federal Emergency Management Agency, Washington, DC, p. 75.

FEMA (Federal Emergency Management Agency). (2007). *Model State Dam Safety Program*. Federal Emergency Management Agency, Washington, DC.

FEMA (Federal Emergency Management Agency). (2011). *Dam Safety in the United States*. Federal Emergency Management Agency, Washington, DC, p. 57.

FEMA (Federal Emergency Management Agency). (2013). *Selecting and Accommodating Inflow Design Floods for Dams*. Federal Emergency Management Agency, Washington, DC, p. 47.

FEMA (Federal Emergency Management Agency). (2014). Technical Manual: Overtopping Protection for Dams, Report P-1015, Federal Emergency Management Agency, Washington DC, p. 332.

FEMA (Federal Emergency Management Agency). (2015). *Federal Guidelines for Dam Safety Risk Management*. Federal Emergency Management Agency, Washington, DC, p. 49.

FEMA (Federal Emergency Management Agency). (2016a). *NDSP Biennial Report to Congress, Fiscal Years 2014–2015*. Federal Emergency Management Agency, Washington DC.

Feng, J., W. Zhenming, E. W. Woolery, and S. Li. (2015). *Comparison of the Ground-motion Attenuation Relationship between the Wenchaun, China, Area and the Central and Eastern United States*. Report of Investigations 28. Kentucky Geological Survey, Lexington, KY.

Fenton, G. A., and D. V. Griffiths. (2008). *Risk Assessment in Geotechnical Engineering*. John Wiley & Sons, Hoboken, NJ.

FERC (Federal Energy Regulatory Commission). (1999). "Arch dams." *Engineering Guidelines for the Evaluation of Hydropower Projects*. Federal Energy Regulatory Commission, Washington, DC.

FERC (Federal Energy Regulatory Commission). (2006). "Embankment dams." *Engineering Guidelines for the Evaluation of Hydropower Projects*. Federal Energy Regulatory Commission, Washington, DC.

FERC (Federal Energy Regulatory Commission). (2014). *Strategic Plan: FY 2014–2018*. Federal Energy Regulatory Commission, Washington, DC, p. 48.

FERC (Federal Energy Regulatory Commission). (2015). "Selecting and accommodating inflow design floods for dams." *Engineering Guidelines for the Evaluation of Hydropower Projects*. Federal Energy Regulatory Commission, Washington, DC.

FERC (Federal Energy Regulatory Commission). (2016). "Gravity dams." *Engineering Guidelines for the Evaluation of Hydropower Projects*. Federal Energy Regulatory Commission, Washington, DC.

FERC (Federal Energy Regulatory Commission). (2017). "Dam safety performance monitoring program." *Engineering Guidelines for the Evaluation of Hydropower Projects*. Federal Energy Regulatory Commission, Washington, DC.

Ferrante, F., M. Bensi, and J. Mitman. (2012). "Uncertainty analysis for large dam failure frequencies."

Ferrante, F., S. Sancaktar, J. Mitman, and J. Wood. (2011). "An assessment of large dam failure frequencies based on US historical data." *ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis*, Wilmington NC, 10.

Ferrari, R. (2008). *Elephant Butte Reservoir: 2007 Sedimentation Survey*. Technical Report No. SRH-2008-4, US Bureau of Reclamation, Denver, CO, p. 162.

Foster, M. A., M. Spannagle, and R. Fell. (1998). *Analysis of Embankment Dam Incidents*. University of New South Wales, School of Civil Engineering, Sydney, Australia.

Foster, M., R. Fell, and M. Spannagle. (2000). "The statistics of embankment dam failures and accidents." *Canadian Geotechnical Journal* 37(5), 1000–1024.

Fread, D. L. (1988). Breach: *An Erosion Model for Earthen Dam Failures*. National Weather Service.

Froehlich, D. C. (1995a). "Peak outflow from breached embankment dam." *Journal of Water Resources Plannig and Management* 121(1), 90–97.

Froehlich, D. C. (1995b). "Embankment dam breach parameters revisited." *Proceedings of the 1995 ASCE Conference on Water Resources Engineering*, San Antonio, Texas, pp. 887–891.

Froehlich, D. C. (2008). "Embankment dam breach parameters and their uncertainties." *J. Hydraul. Eng.* 134(12), 1708–1721.

Froehlich, D. C. (2016). "Predicting peak discharge from gradually breached embankment dam." *J. Hydrol. Eng.* 21(11). doi.org/10.1061/(ASCE)HE.1943-5584.0001424

Graizer, V. and E. Kalkan. (2007). "Ground motion attenuation model for peak horizontal acceleration from shallow crustal earthquakes." *Earthquake Spectra* 23(3), 585–613.

Griffiths, D. V., and G. A. Fenton (eds.). (2007). *Probabilistic Methods in Geotechnical Engineering*. CISM International Centre for Mechanical Sciences, Springer Wien, New York.

Grigoriu, M. (1984). *Risk, Structural Engineering and Human Error*. University of Waterloo Press, Waterloo, Ontario.

Gruner, E. (1963). "Dam disasters." Paper 6648, *Proceedings of the Institution of Civil Engineers* 24(1), January, 47–60. London. doi.org/10.1680/iicep.1963.10759. Accessed November 2019.

Gruner, E. C. (1967). "The safety of reservoirs." *World Dams Today (Japan Dam Association)*, 104–109.

Hanson, G. J., D. M. Temple, M. Morris, M. Hassan, and K. Cook. (2005). "Simplified breach analysis model for homogeneous embankments: Part 2, Parameter inputs and variable scale model comparisons." *USSD Technologies to Enhance Dam Safety and the Environment, 25th Annual USSD Conference*, Salt Lake City, Utah.

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

Hartford, D. N., G. B. Baecher, P. A. Zielinski, R. C. Patev, R. Ascila, and K. Rytters. (2016). *Operational Safety of Dams and Reservoirs*. ICE Publishing, London.

Hassani, B. K. (2016). *Scenario analysis in risk management: theory and practice in finance*. Springer Berlin Heidelberg, New York, NY.

Hepler, T., Fiedler, W., Vermeyen, T., Dewey, R, and Wahl, T. (2012). "Overtopping protection for dams – a technical manual overview," Dam Safety 2012 - Association of State Dam Safety Officials, September 16-20, Denver.

HSE (Health and Safety Executive). (2001). *Reducing Risks, Protecting People—HSE's Decision Making Process*. UK Health and Safety Executive, Her Majesty's Stationery Office, London.

Hydrometrics Inc. (2011). *Guidelines for Conducting a Simplified Failure Mode Analysis for Montana Dams*. Montana Department of Natural Resources and Conservation, Helena, Montana.

ICOLD European Club. (2007). *Dam Legislation*. International Commission on Large Dams, Geneva, 84.

ICOLD European Club. (2012). *Working Group on Safety of Existing Dams*. International Commission on Large Dams, Geneva, 54.

ICOLD European Club. (2017). *Dam Legislation*. International Commission on Large Dams, Geneva, 96.

ICOLD (International Commission on Large Dams). (1987). *Dam Safety Guidelines*. *Bulletin 59*, International Commission on Large Dams, Paris.

ICOLD (International Commission on Large Dams). (2005). *Risk Assessment in Dam Safety Management. A Reconnaissance of Benefits, Methods and Current Applications. Bulletin 130*, International Commission on Large Dams, Paris.

ICOLD (International Commission on Large Dams). (2017). *Internal Erosion of Existing Dams, Levees and Dikes, and their Foundations. Bulletin 164*, International Commission on Large Dams, Paris.

IFT (Independent Forensics Team). (2018). *Independent Forensic Team Report: Oroville Dam Spillway Incident*. Independent Forensic Team.

ISO (International Standards Organization). (1999). *Petroleum, Petrochemical, and Natural Gas Industries: Collection and Exchange of Reliability and Maintenance Data for Equipment*, ISO 14224:2016. International Standards Organization, Geneva, Switzerland. Available at https://www.iso.org/standard/64076.html. Accessed November 2019.

Johnson, P. A. (1999). "Fault tree analysis of bridge failure due to scour and channel instability." *Journal of Infrastructure Systems* 5(1), 35–41.

Kaplan, S., and B. J. Garrick. (1981). "On the quantitative definition of risk." *Risk Analysis* 1, 11–27.

Kennedy, R., C. A. Cornell, R. Campbell, S. Kaplan, and H. Perla. (1980). "Probabilistic seismic safety study of an existing nuclear-power plant." *Nuclear Engineering and Design* 59(2), 315–338.

Kim, B., and B. F. Sanders. (2016). "Dam-break flood model uncertainty assessment: Case study of extreme flooding with multiple dam failures in Gangneung, South Korea." *J. Hydraul. Eng.* 142(5).

Konstantas, J. (2016). "Dam Hackers! The Rising Risks to ICS and SCADA Environments." Security Week.

Kreuzer, H., and K. V. Bury. (1984). "A probability based evaluation of the safety and risk of existing dams." *International Conference on Safety of Dams*, Coimbra, Portugal.

Lane, N. (2008). *Aging infrastructure: Dam Safety*. *CRS Report for Congress*, Order Code RL33108.

Langseth, D. E., and F. E. Perkins. (1983). "The influence of dam failure probabilities on spillway analysis." *Proceedings of the Conference on Frontiers in Hydraulic Engineering*, American Society of Civil Engineers, New York, 459–464.

Leveson, N. G. (2012). *Engineering A Safer World: Systems Thinking Applied to Safety*. The MIT Press, Cambridge, MA.

Lewin, J. (2001a). *Hydraulic Gates and Valves in Free Surface Flow and Submerged Outlets,* 2nd edition. Thomas Telford Publishing.

Lewin, J. (2001b). "Failures and vulnerabilities of reservoir control structures." *Learning from Construction Failures: Applied Forensic Engineering*. P. Campbell, ed. John Wiley & Sons, New York and London, pp. 168–193.

Lewin, J., and G. Ballard. (2001). *Preliminary Reliability Assessment of Spillway Gate Installations: Portland District—Hills Creek Dam Demonstration Risk Assessment, Huntington District Demonstration Portfolio Risk Assessment, and Fort Worth District Portfolio Risk Assessment.* US Army Corps of Engineers, Washington, DC.

Lin, L., and J. Adams. (2007). "Probabilistic method for seismic vulnerability ranking of Canadian hydropower dams." *Canadian Dam Association 2007 Annual Conference: A Climate of Change*, September 22–27, 2007, St. John's, Newfoundland.

MacDonald, T. C., and J. Langridge-Monopolis. (1984). "Breaching characteristics of dam failures." *J. Hydraul. Eng.* 110(5), 567–586.

Mark, R. K., and D. E. Stuart-Alexander. (1977). "Disasters as a necessary part of benefit-cost analysis." *Science* 197, 1160–1162.

McCann, M. (2002). "Fault tree analysis." *Guide to Risk Analysis for Dam Safety*, D. Hartford, ed., Dam Safety Interest Group, Canadian Electricity Association, Vancouver.

McCann, M. W., and K. O. Addo. (2012). "Volume 1: Methodology." *Probabilistic Seismic Hazard Analysis (PSHA) Model*, BC Hydro.

McDonald, L. (1995). "ANCOLD risk assessment guidelines." *Proceedings of the Seminar on Acceptable Risks for Extreme Events in the Planning and Design of Major Infrastructure*, Sydney, Australia, April 26–27, 1994. Balkema, Rotterdam, pp. 105–121.

McManamay, R. A., C. O. Oigbokie, S.-C. Kao, and M. S. Bevelhimer. (2016). "Classification of US hydropower dams by their modes of operation." *River Research and Application* 32, 1450–1468, doi.org/10.1002/rra.3004.

Meel, A., L. M. O'Neill, J. H. Levin, W. D. Seider, U. Oktem, and N. Keren. (2007). "Operational risk assessment of chemical industries by exploiting accident databases." *Journal of Loss Prevention in the Process Industries* 20(2), 113–127.

Melchers, R. E. (1987). *Structural Reliability: Analysis and Prediction*. Wiley, Chichester, West Sussex, England; New York.

Middlebrooks, T. A. (1953). "Earth-dam practice in the United States." *Transactions of the American Society of Civil Engineers*, Centennial Volume, 697–721.

Mohamed, M. A. A. (2002). *Embankment Breach Formation and Modelling Methods*. PhD thesis, Open University, United Kingdom.

Mohamed, M. A. A., P. G. Samuels, M. W. Morris, and G. S. Ghataora. (2002). "Improving the accuracy of prediction of breach formation through embankment dams and flood embankments." *Proc. of the Int. Conf. On Fluvial Hydraulics*, Louvain-la-Neuve, Belgium.

National Research Council. (1983). *Safety of Dams: Evaluation and Improvement*. The National Academies Press, Washington, DC.

National Research Council. (1985). *Safety of Dams: Flood and Earthquake Criteria*. The National Academies Press, Washington, DC.

NCS (National Communications System). 2004. "Supervisory Control and Data Acquisition (SCADA) Systems." National Communications System, Arlington, VA.

Norstedt, U., C.F.O Rollenhagen, and P. E. Eveneus. (2008). "Considering human factors in dam safety." *Hydro Review*, December 1.

NRC (Nuclear Regulatory Commission). (1975). *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants*. US Nuclear Regulatory Commission, Washington, DC, p. 119. ML15334A199.

NRC (Nuclear Regulatory Commission). (1977). *Design Basis Floods for Nuclear Power Plants*, Rev. 2. US Nuclear Regulatory Commission, Washington, DC. ML11321A195.

NRC (Nuclear Regulatory Commission). (1983). *NRC Inventory of Dams*. US Nuclear Regulatory Commission, Washington, DC, p. 108, ML13311B207.

NRC (Nuclear Regulatory Commission). (1987). *Evaluation of External Hazards to Nuclear Power Plants in the United States,* NUREG/CR-5042. US Nuclear Regulatory Commission, Washington, DC. ML14196A083.

NRC (Nuclear Regulatory Commission). (1988). Supplement 4 to NRC Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities." US Nuclear Regulatory Commission, Washington, DC.

NRC (Nuclear Regulatory Commission). (1999). *Implementing a Framework for Risk-informed Regulation in the Office of Nuclear Material Safety and Safeguards*. US Nuclear Regulatory Commission, Washington, DC.

NRC (Nuclear Regulatory Commission). (2002). *Design of Erosion Protection for Long-Term Stabilization*, NUREG-1623. US Nuclear Regulatory Commission, Washington, DC. ML022530043.

NRC (Nuclear Regulatory Commission). (2008). *Design, Construction, and Inspection of Embankment Retention Systems at Uranium Recovery Facilities*. US Nuclear Regulatory Commission, Washington, DC. ML082380144.

NRC (Nuclear Regulatory Commission). (2011). *Design-Basis Flood Estimation for Site Characterization at Nuclear Power Plants in the United States of America*. Prepared by Pacific Northwest National Laboratory for the US Nuclear Regulatory Commission, Washington, DC. ML11321A195.

NRC (Nuclear Regulatory Commission). (2012a). *Information Notice 2012-02: Potentially Nonconservative Screening Value for Dam Failure Frequency in Probabilistic Risk Assessments*. US Nuclear Regulatory Commission, Washington, DC. ML090510269.

NRC (Nuclear Regulatory Commission). (2012b). *Practical Implementation Guidelines for SSHAC Level 3 and 4 Hazard Studies*, NUREG-2117, Revision 1. US Nuclear Regulatory Commission, Washington, DC. ML12073A311.

NRC (Nuclear Regulatory Commission). (2012c). *Request for Information Pursuant to Title 10 of the Code of Federal Regulations 50.54(f) Regarding Recommendations 2.1,2.3, and 9.3, of the Near-Term Task Force Review of Insights from the Fukushima Dai-Ichi Accident*. US Nuclear Regulatory Commission, Washington, DC. ML12053A340.

NRC (Nuclear Regulatory Commission). (2013). *Interim Staff Guidance for Estimating Flooding Hazards due to Dam Failure*, JLD-ISG-13-01. US Nuclear Regulatory Commission, Washington, DC. ML13151A153.

NRC (Nuclear Regulatory Commission). (2018). *Updated Implementation Guidelines for SSHAC Hazard Studies*, NUREG-2213. US Nuclear Regulatory Commission, Washington, DC. ML18282A082.

OAG (Office of the Auditor General). (2012). "Protecting Canadian critical infrastructure against cyber threats." In 2012 Fall Report of the Auditor General of Canada. Office of the Auditor General of Canada, Ottawa, Canada.

Olson, K. R. and L. W. Morton. (2014). "Runaway barges damage Marseilles Lock and Dam during 2013 flood on the Illinois River." *Journal of Soil and Water Conservation* 69 (4), 104A–109A.

Parr, N. M. and N. Cullen. (1998) "Risk management and reservoir maintenance." *Journal of the Institution of Water and Environmental Management* 2, 587–593.

Paté-Cornell, E. M. (1984). "Fault trees vs. event trees in reliability analysis." *Risk Analysis* 4(3), 177–186.

Patev, R. C., and C. S. Putcha. (2005). "Development of fault trees for risk assessment of dam gates and associated operating equipment." *International Journal of Modelling and Simulation* 25(3).

Patev, R. C., D. L. Buccini, J. W. Bartek, and S. Foltz. (2013). *Improved Reliability Models for Mechanical and Electrical Components at Navigation Lock and Dam and Flood Risk Management Facilities*. US Army Corps of Engineers, Washington, DC.

Patev, R. C., C. S. Putcha, and S. D. Foltz. (2005). *Methodology for Risk Analysis of Dam Gates and Associated Operating Equipment Using Fault Tree Analysis.* US Army Corps of Engineers, Waterways Experiment Station, Vicksburg MS.

Pavlovic, B. (2016). "Automated Control Flaw Generation Procedure: Cheakamus Dam Case Study." MSc Thesis, University of Western Ontario, London, Ontario.

Perkins, R. H., M. T. Bensi, J. Philip, and S. Sancaktar. (2011). *Screening Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Power Plant Sites Following Upstream Dam Failures*. Us Nuclear Regulatory Commission, Washington, DC, p. 44.

Peter, S. J., A. Siviglia, J. Nagel, S. Marelli, R. M. Boes, D. Vetsch, and B. Sudret. (2018). "Development of probabilistic dam breach model using Bayesian inference." Available at arXiv:1806.05035v1. Accessed November 2019.

Porter, K. (2018). *A Beginner's Guide to Fragility, Vulnerability, and Risk. University of Colorado Boulder*. University of Colorado, Boulder, 112 pp.

Porter, K., R. Kennedy, and R. Bachman. (2007). "Creating fragility functions for performance-based earthquake engineering." *Earthquake Spectra* 23(2), 471–489.

Pradel, D., J. Wartman, and B. Tiwari. (2012). "Failure of Fujinuma Dam during the 2011 Tohuku earthquake." *Proceedings of the 9th International Conference on Urban Earthquake Engineering*, Tokyo, Japan.

Regan, P. (2010). "Dams as systems—A holistic approach to dam safety." *In 30th Annual USSD Conference on Dams: Collaborative Management of Integrated Watersheds*, Sacramento, CA.

Regan, P. J. (2009). "An examination of dam failures vs. age." *USSD 2009 Annual Conference Proceedings*, US Society on Dams, Nashville, Tennessee.

Robertson, A. M. (2012). "FMEA risk analysis: failure modes and effects analysis." Robertson GeoConsultants, Belo Horizonte, Brazil.

Santos, R.N.C. dos, L.M.M.S. Caldeira, and J.P.B. Serra. (2012). "FMEA of a tailings dam." *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards* 6(2), 89–104.

Schellenberg, G., C. R. Donnelly, C. Holder, M.-H. Briand, and R. Ahsan. (2017). "Sedimentation, dam safety and hydropower: issues, impacts and solutions." Hatch Inc., 24 pp.

Schweckendiek, T., A.C.W.M. Vrouwenvelder, and E.O.F. Calle. (2014). "Updating piping reliability with field performance observations." *Structural Safety*, 47, 13–23.

Schweckendiek, T., and W. Kanning. (2016). *Reliability Updating for Slope Stability of Sikes—Approach with Fragility Curves (Background Report)*. Deltares, Delft, Netherlands.

Shams-Ghahfarokhi, G. (2014). "Probabilistic Analysis of Failures Mechanisms of Large Dams." PhD dissertation, Delft University of Technology, Delft, Netherlands.

Smith, B. T., A. Witt, K. M. Stewart, K. Lee, S. DeNeale, and M. Bevelhimer, M. (2017). *A Multi-Year Plan for Research, Development, and Prototype Testing of Standard Modular Hydropower Technology/R1*, ORNL/TM-2016/102. Oak Ridge National Laboratory.

Sohn, P. and M. Stone. (2010). "Tornado slams dam." *Chattanooga Times Free Press*, Chattanooga, TN.

Sowers, G. F. (1993). "Human factors in civil and geotechnical engineering failures." *Journal of Geotechnical Engineering* 119(2). doi: 10.1061/(ASCE)0733-9410(1993)119:2(238)

SPANCOLD (Spanish National Committee on Large Dams). (2012). *Risk Analysis Applied to Management of Dam Safety*, *Volume 1*. Spanish National Committee on Large Dams, Madrid, 153 pp.

Srivastava, A., D. S. Bowles, and S. S. Chauhan. (2012). "DAMRAE-U: A tool for including uncertainty in dam safety risk assessment." *ASDSO 2012 Conference on Dams*, Association of State Dam Safety Officials, Denver.

Stewart, R. A. (2000). "Dam risk management." *The ICOLD Lecture Proceedings, GeoEng 2000*, A. A. Balkema, Amsterdam.

Takase, K. (1967). "Statistic study on failure, damage and deterioration of earth dams in Japan." *Ninth ICOLD Congress*, 1–19.

Temple, D. M., G. J. Hanson, M. L. Neilsen, and K. Cook. (2005). "Simplified breach analysis model for homogeneous embankments: Part 1, Background and model components." *USSD Technologies to Enhance Dam Safety and the Environment*, 25th Annual USSD Conference, Salt Lake City, Utah.

Thompson, M. (2016). "Iranian cyber attack on New York dam shows future of war." *Time*, March 26.

Uría-Martínez, R., M. M. Johnson, and P. W. O'Connor. (2018). *2017 Hydropower Market Report*. Water Power Technologies Office, US Department of Energy, Washington, DC.

URS Group. (2008). *Risk Prioritization Tool for Dams: Users Manual*. Federal Emergency Management Agency, Washington, DC, 58.

USACE (US Army Corps of Engineers). (1994). *Arch Dam Design*. EM 1110-2-2201, US Army Corps of Engineers, Washington, DC, p. 240.

USACE (US Army Corps of Engineers). (1995). *Gravity Dam Design*. EM 1110-2-2200, US Army Corps of Engineers, Washington, DC, p. 88.

USACE (US Army Corps of Engineers). (2004). *General Design and Construction Considerations for Earth and Rock-Fill Dams*. EM 1110-2-2300, US Army Corps of Engineers, Washington, DC, p.130.

USACE. (2008). *Coastal Engineering Manual*. EM 1110-2-1100, US Army Corps of Engineers, Washington, DC.

USACE (US Army Corps of Engineers). (2014a). *Safety of Dams—Policy and Procedures*. ER 1110-2-1156, US Army Corps of Engineers, Washington, DC, p. 528.

USACE (US Army Corps of Engineers). (2014b). *Using HEC-RAS for Dam Break Studies*. TD-39, US Army Corps of Engineers, Institute for Water Resources, Hydrologic Engineering Center, Davis, CA.

USACE (US Army Corps of Engineers). (2016). *HEC-RAS River Analysis System 2D Modeling User's Manual*. CPD-68A, US Army Corps of Engineers, Institute for Water Resources, Hydrologic Engineering Center, Davis, CA.

USBR (US Bureau of Reclamation). (1976). *Design of Gravity Dams: Design Manual for Concrete Gravity Dams*. US Bureau of Reclamation, Denver, CO, 586 pp.

USBR (US Bureau of Reclamation). (1977). *Design of Arch Dams: Design Manual for Concrete Arch Dams*. US Bureau of Reclamation, Denver, CO, 882 pp.

USBR (US Bureau of Reclamation). (1987). *Design of Small Dams* (5th ed.). US Bureau of Reclamation, Washington, DC, 904 pp.

USBR (US Bureau of Reclamation). (2004). *Hydrologic Hazard Curve Estimating Procedures*. US Bureau of Reclamation, Denver, CO, 85 pp.

USBR (US Bureau of Reclamation). (2009). *Probabilistic Slope Stability Analysis Using the Random Finite Element Method (RFEM)*. US Bureau of Reclamation, Denver, CO, 63 pp.

USBR (US Bureau of Reclamation). (2012). "Embankment Design." *Design Standards No. 13: Embankment Dam*. US Bureau of Reclamation, Denver, CO.

USBR (US Bureau of Reclamation). (2014). "General Spillway Design Considerations." *Design Standards No. 14: Appurtenant Structures for Dams (Spillways and Outlet Works) Design Standard*. US Bureau of Reclamation, Denver, CO.

USBR (US Bureau of Reclamation). (2017). *Evaluation of Numerical Models for Simulating Embankment Dam Erosion and Breach Processes*. US Bureau of Reclamation, Denver, CO, 104 pp.

USBR and USACE (US Bureau of Reclamation and US Army Corps of Engineers). (2017). *Dam Safety Risk Analysis Best Practices Training Manual*. US Bureau of Reclamation, US Army Corps of Engineers, Denver and Washington, DC, updated 2/15/17. https://www.usbr.gov/ssle/damsafety/risk/methodology.html

USCOLD (US Committee on Large Dams). (1975). *Lessons from Dam Incidents, USA*. American Society of Civil Engineers, New York, 391 pp.

USDA (US Department of Agriculture). (2016). "WinDAM C Software: Estimating erosion of earthen embankments and auxiliary spillways of dams." US Department of Agriculture.

USDOI (U.S. Department of the Interior). (2018). *Final Evaluation Report - U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats*. Office of Inspector General, U.S. Department of the Interior, Washington DC, 31.

US Weather Bureau. (1957). *Rainfall Intensity-Frequency Regime: Part 1 – The Ohio Valley, Technical Paper No. 29*, U.S. Weather Bureau, Washington, D.C.

Vail, J., F. Ferrante, and J. Mitman. (2010). "Generic failure rate evaluation for Jocassee Dam." US Nuclear Regulatory Commission, Washington, DC.

Varshney, R. S. (1978). *Concrete Dams*. Oxford and IBH Publishing, New Delhi.

Vick, S. G., and R. A. Stewart. (1996). "Risk analysis in dam safety practice." *Uncertainty in the Geologic Environment*. C. D. Shackelford, P. P. Nelson, and M. J. S. Roth, eds., American Society of Civil Engineers, Madison, WS, 586–603.

von Thun, J. L. (1985). *Application of Statistical Data from Dam Failures and Accidents to Risk-based Decision Making on Existing Dams*. US Bureau of Reclamation, Engineering and Research Center, Denver, 20 pp.

von Thun, J. L. (1996). "Risk assessment of Nambe Falls Dam." *Uncertainty in the Geologic Environment*, Madison, American Society of Civil Engineers, 604–635.

von Thun, J. L. (1999). "Reclamation's public safety dam safety guidelines: Background on philosophy and technical rationale (internal memorandum)." US Bureau of Reclamation.

von Thun, J. L., and D. R. Gillette. (1990). "Guidance on breach parameters." Unpublished internal document, US Bureau of Reclamation, Denver, CO, 17 pp. March

Vrijling, J. K. (2001). "Probabilistic design of water defense systems in The Netherlands." *Reliability Engineering and System Safety* 74(3), 337–344.

Wahl, T. L. (1998). *Prediction of Embankment Dam Breach Parameters: A Literature Review and Needs Assessment*. US Bureau of Reclamation, Denver, CO, 67 pp.

Wahl, T. L. (2004). "Uncertainty of predictions of embankment dam breach parameters." *J. Hydraul. Eng.* 130(5), 389–397.

Wahl, T. L. (2014). *Evaluation of Erodibility-based Embankment Dam Breach Equations*. US Bureau of Reclamation, Denver, CO, 99 pp.

Wahl, T. L., G. J. Hanson, J.-R. Courivaud, M. W. Morris, R. Kahawita, J. T. McClenathan, and D. M. Gee. (2008). "Development of next-generation embankment dam breach models," *United States Society on Dams 28th Annual USSD Conference*, Portland, OR, April 28–May 2, 2008, 767–779.

Walder, J. S., and J. E. O'Connor. (1997). "Methods for predicting peak discharge of floods caused by failure of natural and constructed earthen dams. *Water Resources Research* 33(10), 2337–2348.

Wang, P. and R. Kahawita. (2002). "Modelling the hydraulics and erosion process in breach formation due to overtopping." A. Gyr and W. Kinzelbach, eds, *Sedimentation and Sediment Transport*, *Proceedings of the Symposium*, Monte Verita, Switzerland, 211–220.

Wang, P., R. Kahawita, A. Mokhtari, T. M. Phat, and T. T.Quach. (2006). "Modelling breach formation in embankments due to overtopping." *ICOLD Conference*, Barcelona, Spain, June 2006.

Wang, X. (2012). "Slope Stability Analysis Based on Random Finite Element Method and Probabilistic Approach." Master's dissertation, Delft University of Technology, Delft, Netherlands.

Ward, S. N., and S. Day. (2011). "The 1963 landslide and flood at Vaiont Reservoir Italy. A tsunami ball simulation." *Ital. J. Geosci.* 130(1), 16–26.

West, M., M. Morris, and M. Hassan. (2018). "A guide to breach prediction." HR Wallingford Ltd. Wallingford, UK.

Wynn, H. P., P. J. Brown, C. Anderson, et al. (2001). "Bayesian calibration of computer models—Discussion." Journal of the Royal Statistical Society Series B 63, 450–464. Available at https://www.researchgate.net/publication/292215218_Bayesian_calibration_of_computer_models_-_Discussion. Accessed November 2019

Xu, Y., and Zhang, L. M. (2009). "Breaching parameters for earth and rockfill dams." *Journal of Geotechnical and Geoenvironmental Engineering* 135(12), 1957–1970.

Xu, Y., L. Zhang, and J. Jia. (2008). "Lessons from catastrophic dam failures in August 1975 in Zhumadian, China." *Proceedings of GeoCongress 2008*, New Orleans, March 9–12, 2008.

Yang, H., M. Haynes, S. Winzenread, and K. Okada. (1999). *The History of Dams*. University of California–Davis, Davis, CA.

Zacchei, E., J. L. Molina, and R.M.L.R.F. Brasil. (2017). "Seismic hazard and structural analysis of the concrete arch dam (Rules Dam on Guadalfeo River)." *Procedia Engineering* 199, 1332–1337.

Zagonjolli, M. (2007). *Dam Break Modelling, Risk Assessment and Uncertainty Analysis for Flood Mitigation*. Doctoral Thesis, Delft University of Technology. Available at https://repository.tudelft.nl/islandora/object/uuid%3A71ab29f8-c717-429c-9a44-7b882a2f9b0b. Accessed November 2019.

Zhang, L. M., Y. Xu, and J. S. Jia. (2007). "Analysis of earth dam failures—A database approach." *Proceedings of the First International Symposium on Geotechnical Safety & Risk*, Shanghai, China, October 18-19, 2007.

Zimmaro, P. and J. P. Stewart. (2015). "Probabilistic seismic hazard analysis for a dam site in Calabria (Southern Italy)." *UCLA—SGEL Report 2015/02*, University of California–Los Angeles, Los Angeles, CA.

APPENDIX A. HISTORICAL DAM FAILURE INVENTORIES

APPENDIX A. HISTORICAL DAM FAILURE INVENTORIES

A.1   DAM FAILURE DATABASES

Several inventories of dam failures have been compiled, mostly but not entirely by professional organizations such as ICOLD, USSD, and ASCE; or by government organizations such as USACE, USBR, and FERC (Table A-1). Brief descriptions of select dam failure databases are provided in the text below, and a list of historical, self-reported dam failures involving fatalities is provided in Table A-2.

Table A-1. Inventories and summaries of dam failure statistics.

Source	Organization	Reference
INVENTORIES		
National Inventory of Dams	USACE	website[7]
An Examination of Dam Failures vs. Age	FERC	(Regan 2010)
National Performance of Dams Project	Stanford	website[9]
National inventory of reservoir dam failures (in Chinese).	MWR	(MWR 1993)
Lessons from Dam Incidents USA	USSD	(USCOLD 1975, 1988)
Bibliography of the history of dam failures	—	(Vogel 1980)
Lessons from dam incidents	ICOLD	(ICOLD 1973)
Catalog of dam disasters, failures, and accidents	USBR	(Babb and Mermel 1968)
SUMMARIES		
Dam failures—statistical analysis	—	(Yu et al. 2009; Zhang et al. 2016)
Lessons from historical dam incidents: technical summary	(UK) DEFRA	(DEFRA 2011)
Dam failures	—	(Deangeli et al. 2009)
The statistics of embankment dam failures and accidents	—	(Foster et al. 2000)
A review of dam failure: past, present and future	—	(Ingles 1988)
Application of statistical data from dam failures and accidents to risk-based decision analysis on existing dams	USBR	(von Thun 1985)
Statistical analysis of deteriorations and failures of dams	—	(Silveira 1984)
Disasters as a necessary part of benefit-cost analysis	USBR	(Mark and Stuart-Alexander 1977)
Statistic study on failure, damage and deterioration of earth dams in Japan	—	(Takase 1967)
Dam disasters	—	(Gruner 1963, 1964, 1967)
Earth-dam practice in the United States	—	(Middlebrooks 1953)

The National Inventory of Dams[7] (NID) is the most comprehensive listing of some 90,000 dams in the US. It is a congressionally authorized database maintained and published by the USACE and contains information about a dam's location, size, purpose, type, last inspection, and other information. According to ASDSO,[40] "to be a part of the NID, the dam must either be: of high- or significant-hazard potential classification, equal or exceed 25 feet in height and exceed 15 acre-feet in storage, or equal or exceed 50 acre-feet storage and exceed 6 feet in height." The NID can be accessed from https://catalog.data.gov/dataset/national-inventory-of-dams.

---

[40] https://damsafety.org/media/faq (accessed November 2019)

The **National Performance of Dams Program[9] (NPDP)** database is a newer resource, having been established by FERC in 1994 as an information resource for sharing dam incidents and failures within the engineering community. It is maintained by Jack Benjamin Associates and Stanford University. The NPDP has the important benefit of listing dam safety incidents as well as failures, but it has the limitation of relying on self-reported data. Such data are nearly impossible to obtain otherwise but lack the same level of validation and completeness as data in the USACE NID. The NPDP-related information (including plots) provided in this report are based on the publicly available data as of October 2018, which includes self-reported dam incident and failure data through 2006. Table A-2 includes a catalog of all NPDP dam failure events involving fatalities. The NPDP can be accessed from http://npdp.stanford.edu/.

The Chinese Ministry of Water Resources also maintains a **National Inventory of Reservoir Dam Failures**. However, this inventory is in Chinese and has had little application in the western literature.

Wikipedia provides a list of over 100 international dam failures, but the provenance, completeness, and accuracy of the information is uncertain.

Table A-2. US historical dam failures involving fatalities based on NPDP data[9].

Dam name	Year	State	Dam type	Dam height (ft)	Total fatalities
Ashburnham Reservoir	1850	Massachusetts	Earth		2
Lake Paran	1852	Vermont	Earth	25	1
Kenduskeag Village Dam	1853	Maine			1
Williamsburg Dam	1874	Massachusetts	Earth	43	138
Mud Pond	1884	Massachusetts		66	7
South Fork Dam	1889	Pennsylvania	Earth	72	2,209
Spring Lake	1889	Rhode Island	Earth	18	3
Walnut Grove	1890	Arizona	Rockfill	110	90
Chambers Lake Dam	1891	Colorado			1
Munjoy Hill Reservoir	1893	Maine	Earth	45	4
Portland	1893	Maine			4
Goodrich Reservoir	1896	Oregon	Earth	50	7
Staunton Dam	1896	Virginia	Gravity	46	5
Melzingah Dam	1897	New York	Gravity	50	7
Jefferson County	1897	Colorado			2
Austin	1900	Texas	Masonry	60	8
Oakford Park	1903	Pennsylvania	Earth; Masonry	20	23
Fort Pitt	1903	Pennsylvania		10	2
Austin	1911	Pennsylvania	Concrete Gravity	50	78
Lyman Dam	1915	Arizona	Earth	53	8
Lower Otay Dam	1916	California	Rockfill	154	30
Thompson Mill Dam	1916	Tennessee	Rockfill	21	24
Mammoth	1917	Utah	Earth		1
Saltville Muck Lake	1924	Virginia		100	19
St. Francis	1928	California	Concrete	205	450
Alexander	1930	Hawaii	Earth	119	6
Eastwick Rail Road Fill	1932	Washington	Earth		7

Dam name	Year	State	Dam type	Dam height (ft)	Total fatalities
Castlewood Dam	1933	Colorado	Rockfill; Masonry	70	2
Lake Ludlow Club Dam	1935	New York	Earth	24	3
Wagner Dam	1938	Washington	Earth	50	1
Unnamed Dam (KSS00003)	1951	Kansas			11
Schoellkopf Station	1956	New York			1
Electric Light Pond Dam	1960	New York		26	1
Mohegan Park	1963	Connecticut	Earth	20	7
Baldwin Hills	1963	California	Earth	66	5
Little Deer Creek	1963	Utah	Earth	86	1
Swift Dam No. 2	1964	Montana	Rockfill	157	28
Skagway	1965	Colorado	Rockfill	79	2
Lee Lake	1968	Massachusetts		25	2
Virden Creek Dam	1968	Iowa	Earth	20	1
Canyon Lake Dam	1972	South Dakota	Earth	31	162
Buffalo Creek	1972	West Virginia	Earth	46	125
Anzalduas	1972	Texas	Earth		4
Lake O' the Hills	1972	Alaska	Earth	13	1
Lakeside Dam	1975	South Carolina	Earth		1
Unnamed Dam (COS00008)	1976	Colorado			144
Teton	1976	Idaho	Earth	305	11
Asheville	1976	North Carolina	Earth	50	4
Bear Wallow	1976	North Carolina	Earth	36	4
Mud Mountain Dam	1976	Washington	Rockfill	425	2
Laurel Run	1977	Pennsylvania	Earth	84	40
Kelly Barnes Dam	1977	Georgia	Earth	38	39
Unnamed Dam (MOS00014)	1977	Missouri			20
Swimming Pool Dam	1979	New York	Earth		4
Eastover Mining Company Dam	1981	Kentucky	Mine Tailings		1
Lawn Lake	1982	Colorado	Earth	24	3
DMAD	1983	Utah	Earth	34	1
Bass Haven Lake Dam	1984	Texas	Earth	30	1
Evans and Lockwood Pond Dams	1989	North Carolina	Earth	18	2
Nix Lake Dam	1989	Texas	Earth	23	1
Kendall Lake Dam	1990	South Carolina	Earth	22	4
Timber Lake Dam	1995	Virginia	Earth	30	2
Mike Olson Dam	2000	North Dakota	Earth	29	2
Kaloko Reservoir Dam	2006	Hawaii	Earth	131	7

A.2   CITED REFERENCES FOR APPENDIX A

Babb, A. O., and T. W. Mermel. (1968). *Catalog of Dam Disasters, Failures, and Accidents*. US Bureau of Reclamation, Springfield, VA.

Deangeli, C., G. P. Giani, B. Chiaia, and A. P. Fantilli. (2009). "Dam failures." *WIT Transactions on State-of-the-art in Science and Engineering* WIT Press, 1–50.

DEFRA (Department for Environment, Food, and Rural Affairs). (2011). *Lessons from Historical Dam Incidents: Technical Summary*. Environment Agency, Bristol, UK.

Foster, M., R. Fell, and M. Spannagle. (2000). "The statistics of embankment dam failures and accidents." *Canadian Geotechnical Journal* 37(5), 1000–1024.

Gruner, E. (1963). "Dam disasters." Paper 6648, *Proceedings of the Institution of Civil Engineers* 24(1), January, 47–60. London. doi.org/10.1680/iicep.1963.10759. Accessed November 2019.

Gruner, E. (1964). "Discussion. Dam disasters." *Proceedings of the Institution of Civil Engineers*, 27(2), February, 343–376. https://doi.org/10.1680/iicep.1964.10302. Accessed November 2019.

Gruner, E. C. (1967). "The safety of reservoirs." *World Dams Today (Japan Dam Association)*, 104–109.

ICOLD (International Commission on Large Dams). (1973). *Lessons from Dam Incidents = Leçons Tirées des Accidents de Barrage*. International Commission on Large Dams, CIGB, Paris.

Ingles, O. G. (1988). "A review of dam failure: past, present and future." *Flood Insurance and Relief in Australia*, D. I. Smith and Smith, eds., Australian National University, Canberra, 159–167.

Mark, R. K., and D. E. Stuart-Alexander. (1977). "Disasters as a necessary part of benefit-cost analysis." *Science* 197, 1160–1162.

Middlebrooks, T. A. (1953). "Earth-dam practice in the United States." *Transactions of the American Society of Civil Engineers*, Centennial Volume, 697–721.

MWR (Ministry of Water Resources). (1993). *National Inventory of Reservoir Dam Failures* (in Chinese). The Ministry of Water Resources of the People's Republic of China, Beijing.

Regan, P. (2010). "Dams and civil structures: An examination of dam failures vs. the age of dams." *Hydro Review*, June 1.

Silveira, A. (1984). "Statistical analysis of deteriorations and failures of dams." *Safety of Dams*. *Proceedings of the International Conference on Safety of Dams*, COIMBRA, April 23–28, 1984. A. A. Serafim, ed., A. A. Balkema, Netherlands, pp. 55–60.

Takase, K. (1967). "Statistic study on failure, damage and deterioration of earth dams in Japan." *Ninth ICOLD Congress*, 1–19.

USCOLD (US Committee on Large Dams). (1975). *Lessons from Dam Incidents, USA*. American Society of Civil Engineers, New York, 391 pp.

USCOLD (US Committee on Large Dams). (1988). *Lessons from Dam Incidents*. American Society of Civil Engineers, New York, 236 pp.

Vogel, A. (1980). "Bibliography of the history of dam failures (CD rom)." Risk Assessment International, Vienna.

von Thun, J. L. (1985). *Application of Statistical Data from Dam Failures and Accidents to Risk-based Decision Making on Existing Dams*. US Bureau of Reclamation, Engineering and Research Center, Denver, 20 pp.

Yu, Q., Y. Zhang, X. Wang, W. C. Ma, and L. M. Chen. (2009). "Safety distance assessment of industrial toxic releases based on frequency and consequence: A case study in Shanghai, China." *Journal of Hazardous Materials* 168(2–3), 955–961.

Zhang, L., M. Peng, D. Chang, and Y. Xu. (2016). "Statistical analysis of failures of constructed embankment dams." Chapter 2 in *Dam Failure Mechanisms and Risk Assessment*, Wiley-Blackwell, London, pp. 11–24.

**APPENDIX B. LESSONS LEARNED FROM RECENT DAM FAILURES
AND INCIDENTS**

APPENDIX B. LESSONS LEARNED FROM RECENT DAM FAILURES AND INCIDENTS

Several recent dam failures and incidents have highlighted the importance of dam safety and proper dam safety risk assessment. The following text describes the insights and lessons learned from selected recent events, including

- Missouri River flooding and dam incidents (2011)
- South Carolina dam failures (2015)
- Oroville Dam spillway incident (2017)

Note that the three recent events highlighted in this appendix all resulted primarily from flooding. While flood-induced dam failures and incidents present a significant challenge to dam safety, it is important to consider all potential failure mechanisms in performing dam safety risk assessment. ASDSO provides an online summary[41] of various lessons learned (Table B-1) and case studies related to dam incidents and failures. These lists are not comprehensive but offer a useful resource.

Table B-1. ASDSO lessons learned from dam incidents and failures.[41]

All dams need an operable means of drawing down the reservoir.
Concrete gravity dams should be evaluated to accommodate full uplift.
Dam incidents and failures can fundamentally be attributed to human factors.
Dam owners, engineers and regulators need to address public safety at dams.
Dams located in seismic areas should be evaluated for liquefaction, cracking, potential fault offsets, deformations, and settlement due to seismic loading.
Earth and rockfill embankment dams must be stable under the full range of anticipated loading conditions.
Emergency action plans can save lives and must be updated, understood, and practiced regularly to be effective.
High- and significant-hazard dams should be designed to pass an appropriate design flood. Dams constructed before the availability of extreme rainfall data should be assessed to ensure they have adequate spillway capacity.
Intervention can stop or minimize consequences of a dam failure. Warning signs should not be ignored.
Many earth-cut spillways have been constructed in erodible material that can result in unsatisfactory performance and breaching of the spillway. The integrity of all earth-cut auxiliary spillways should be evaluated to ensure that the design storm can be safely passed.
Regular operation, maintenance, and inspection of dams is important to the early detection and prevention of dam failure.
Seepage along penetrations through embankment dams should be controlled using a filter diaphragm instead of anti-seep collars.
Stability of the dam foundation and other geologic features must be considered during dam design.
The first filling of a reservoir should be planned, controlled, and monitored.

B.1   2011 MISSOURI RIVER FLOOD: DAM INCIDENTS AND LEVEE FAILURES

B.1.1   Overview

In spring and summer 2011, the Missouri River experienced its largest recorded flood event, which pushed some of the largest flood control reservoirs in the US to their capacity and required the USACE to
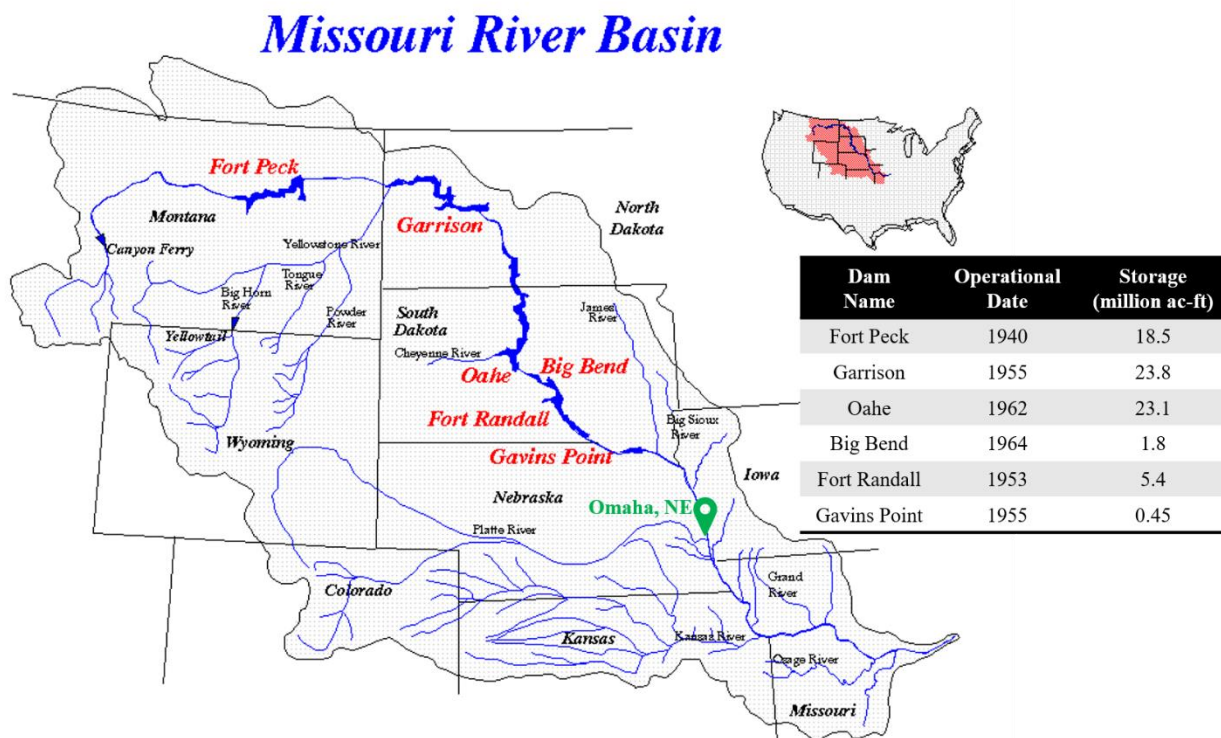
---

[41] http://damfailures.org/ (accessed November 2019)

carefully manage releases over the course of several months. Flood impacts resulted in $2.3 billion in damages, five deaths, and damage to all six USACE mainstem dams.

B.1.2   Missouri River System

The Missouri River Basin (Figure B-1) covers one-sixth of the CONUS, an area of over 500,000 mi^2 across 10 states and one Canadian province; much of the upper basin is mountainous terrain and the lower basin covers flat plains. The climate is highly variable, with cold, harsh winters and warm, wet summers being common.

Today, the once-untamed flows of the Missouri River are captured and released through a series of six mainstem USACE dams that offer flood control, hydropower, irrigation, navigation, and recreation benefits. Flood control regulation of the Missouri River System involves capturing water during periods of high runoff (typically spring and early summer) and releasing the water later in the year over several months and at the lowest rate possible to reduce downstream flood impacts. During a single water-year, the key operational objective is to release all stored water before the start of the next runoff season, thus limiting flood risk in subsequent years (USACE 2012a).


Dam Name	Operational Date	Storage (million ac-ft)
Fort Peck	1940	18.5
Garrison	1955	23.8
Oahe	1962	23.1
Big Bend	1964	1.8
Fort Randall	1953	5.4
Gavins Point	1955	0.45

Figure B-1. Map of Missouri River Basin and USACE mainstem dams. (*Source:* modified from USACE).

B.1.3   The 2011 Flood

In 2011, the Missouri River experienced the largest flood event since the completion of the six USACE mainstem dams and the largest runoff volume since recordkeeping began in the 19th century. As one point of reference, at the peak of the flood, the Missouri River was flowing at over 200,000 cfs past Omaha, Nebraska (Figure B-2). Omaha experienced much higher discharge (approximately 384,000 cfs) at the peak of the 1952 flood event (flood of record); however, that flood was much shorter in duration since it was less regulated.

Hydrologically, the 2011 flood event was enhanced through multiple, combined effects that occurred over several months. A detailed summary of the weather events that contributed to the 2011 flood is contained in Maximuk and Nadolski (2012). In short, the event was primarily caused by a persistent La Niña weather pattern that impacted the upper Missouri River basin and led to much cooler and much wetter conditions than normal. The snowpack across the Great Plains and mountains was much higher than normal. By the time the mountain snowpack began to melt in early May, the Fort Peck reservoir and other downstream system reservoirs were already nearing capacity. The near–record level mountain snowpack (roughly 50% above normal) rapidly melted because of the later-than-normal snowmelt and record rainfall across Wyoming, the Dakotas, and Montana. Contributing to the issue, soil moisture in the upper Missouri River basin was 20–40% above normal in 2010 and contributed to the significant mountain snowmelt once the ground thawed in May.
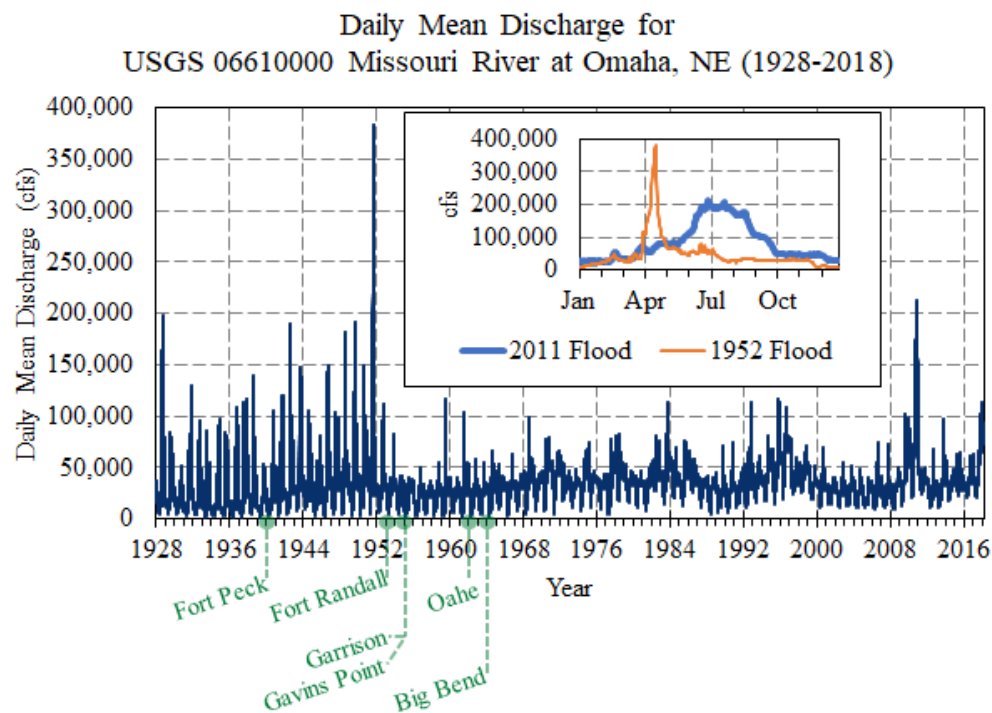
Figure B-2. Missouri River daily mean discharge at Omaha, Nebraska, from 1928 through 2018. Green dots represent dam operational dates. (Data from USGS).

The flood event, for which flows exceeded the original mainstem system design by 20%, was unprecedented and forced the USACE to divert from its Master Water Control Manual (USACE 2006), which guides operators on how to manage flow control releases from the Missouri River dams. By leveraging the flood control capabilities and reservoir storage capacity of the six mainstem Missouri River dams, the USACE was able to flatten the flood hydrograph, trading a longer flood event for a lower peak flood. While peak Gavins Point Dam flow releases of 150,000–160,000 cfs were roughly twice the highest previous release, riverine flows and associated flood levels would have been much higher without flow regulation.

B.1.4 Impacts

The excessive flood flows spilled into the floodplains where levee systems (typically designed to block water for a few days or weeks per year) were saturated and overtopped after months of direct contact. USACE (2012b) reports that 75 federal levees and hundreds of non-federal levees were damaged from

overtopping, erosion, and underseepage resulting from the flood. Prior to the May flood, the Fort Calhoun NPP was shut down due to a refueling outage. Given the flood forecasts, plant remained in safe cold shutdown as it became surrounded by floodwaters (Figure B-3) that were estimated to have resulted from a 500-year event.[42]

Figure B-3. Aerial photograph of the Fort Calhoun nuclear power plant site during the 2011 Missouri River flood. (*Source:* Wikimedia Commons; author: USACE).

Post-flood assessments of the six mainstem dams identified damage to the spillways of all six dams and underseepage issues for five of the six dams. For example, the prolonged release of high flows over the emergency spillway led to erosive widening of the Garrison Dam tailrace channel (Figure B-4). In 2014, the damage repairs planned for the dams were estimated to cost $234 million.[43] The National Climatic Data Center (NCDC) reports a total of five deaths associated with the flood event and a total cost of $2.3 billion across the basin.[44] Despite the damage, the dam and levee infrastructure was found to have functioned as designed and prevented roughly $8.2 billion in damages in the Missouri River basin (USACE 2012c).

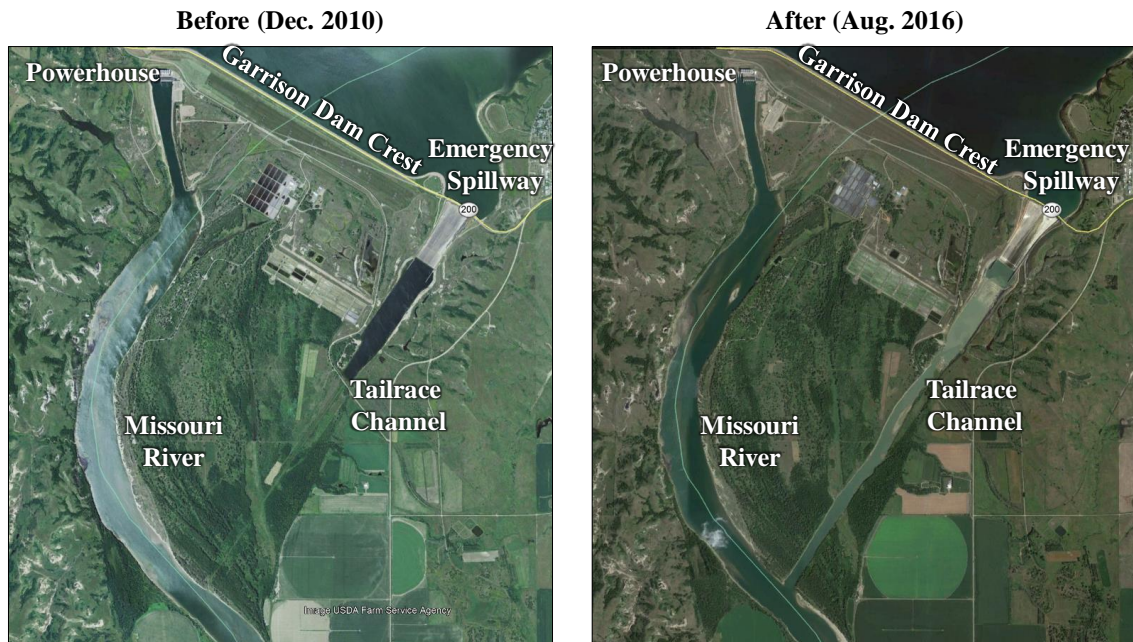[42] http://www.nwd-mr.usace.army.mil/rcc/MRFTF/docs/MRIndependentReviewPanel.pdf (accessed November 2019)

[43] http://www.nwo.usace.army.mil/Media/Fact-Sheets/Fact-Sheet-Article-View/Article/487693/flood-repairs-at-missouri-river-mainstem-dam-projects/ (accessed November 2019)

[44] https://www.ncdc.noaa.gov/billions/events/US/2010-2018 (accessed November 2019)

Figure B-4. Aerial imagery of Garrison Dam before (left) and after (right) the 2011 Missouri River flood.
(Imagery from Google Earth).

B.1.5   Observations and Lessons Learned

Following the flood, numerous post-flood evaluations were made:

- The USACE performed simulations of alternative 2011 flood control scenarios and found that increasing operational flood control storage in the Missouri River Mainstem Reservoir System by 30% could have reduced the peak reservoir release at Gavins Point Dam from 160,000 cfs to 100,000 cfs (USACE 2012a). Although flood risk would have been reduced downstream of the reservoirs, widespread damage would still have occurred. The analysis also found that the additional flood control storage would have negatively affected the four other reservoir purposes (i.e., hydropower, irrigation, navigation, and recreation).

- The USACE appointed a panel to perform an independent technical review[42] of its reservoir system operations during the 2011 flood event. The panel found that while the Corps made appropriate decisions that were in line with appropriate manuals, the manuals and decision-making process could both be improved. It also recommended improvements in snowmelt runoff forecasting, procedures accounting for persistent dry and wet periods, and a system-wide decision support system.

- Following a meeting of experts, the US Government Accountability Office issued a report to Congress (GAO 2014) that concluded that the USACE made appropriate release decisions during the 2011 flood and that probabilistic forecasting using ensemble forecasts would enable better risk-based decision making.

The extensive period of time during which the Missouri River remained above flood level in 2011 was a direct result of USACE operational procedures and an event-specific operational response aimed to reduce peak flood impacts. These types of operational rules can be integrated into forecast and flood hazard models to inform dam safety risk assessment and be used within a probabilistic risk analysis framework. The combination of multiple severe flood-inducing effects (rain-on-snow with high

antecedent baseflow and soil moisture) contributing to this flood event make it a useful case study exhibiting similarities to NRC's current combined effects flooding guidance. Although dam failure did not occur, this flood event caused significant damage to large federal dams and widespread economic impact across the region.

B.2   2015 SOUTH CAROLINA FLOOD: MULTIPLE OVERTOPPING DAM FAILURES

B.2.1   Overview

In early October 2015, parts of South Carolina experienced record rainfall resulting from the unique interaction of a slow-moving low-pressure system and Hurricane Joaquin. The storm complex resulted in $2.2 billion in damage,[44] 25 deaths,[44] and the failure of 49 South Carolina state-regulated dams (shown in Figure B-5), one federally regulated dam, two sections of the levee adjacent to the Columbia Canal, and many unregulated dams (FEMA 2016).
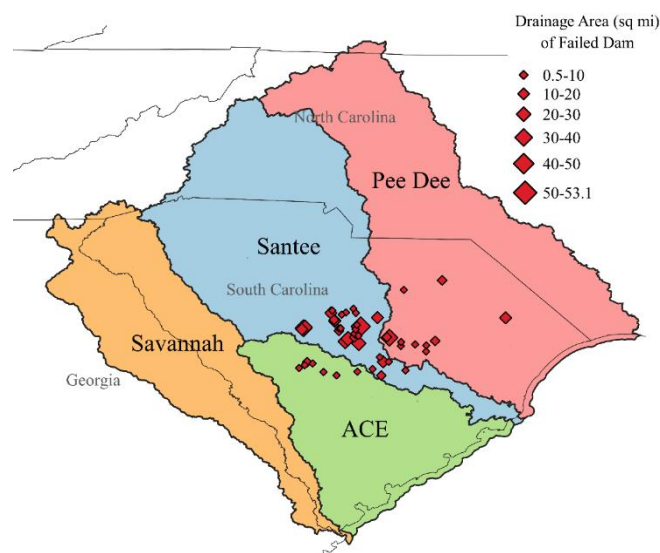
Figure B-5. Map of major South Carolina river basins showing locations of state-regulated dams that failed in the 2015 flood. (*Source:* Data from FEMA [2016]).

B.2.2   Hurricane Joaquin and Record Rainfall

From October 1–5, 2015, record rainfall occurred over much of South Carolina, with coastal and inland rainfall totals ranging from 10 to 26 inches (Figure B-6a). This extreme rainfall exceeded the NOAA Atlas 14 (Bonnin et al. 2006) 6-, 12-, 24-, and 48-hour, 1,000-year precipitation frequency estimates in some locations (FEMA 2016). The rainfall was supplied by above-average sea surface temperatures and warm, moist air spinning around a stalled low-pressure system with influence from Hurricane Joaquin, which was just offshore (Figure B-6b). The resulting weather pattern produced a "funneling" of moisture and rainfall, which resulted in severe flooding (Mizzel et al. 2016). At least 17 USGS stream gages in South Carolina recorded record peak water levels; however, as noted in Mizzel et al. (2016), the flooding severity was likely somewhat reduced by a drought that had persisted across the area before the flood.
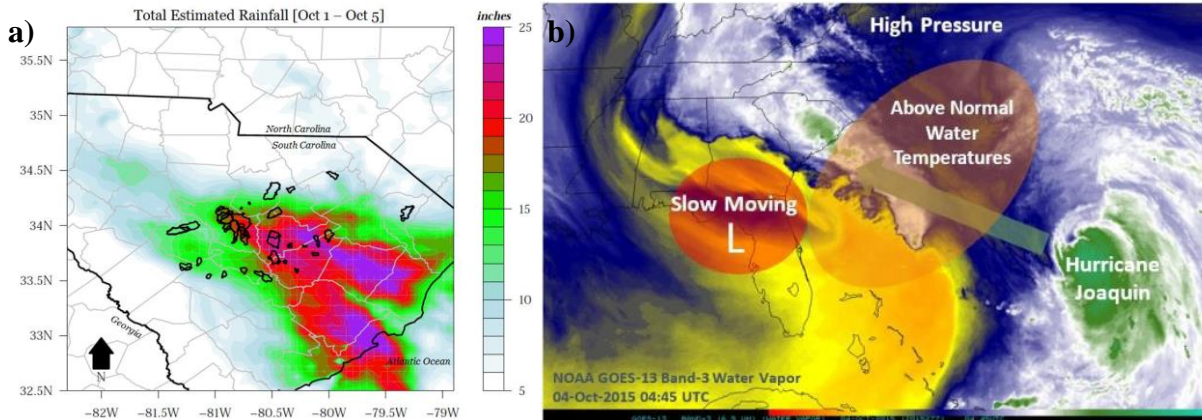
Figure B-6. Total rainfall (left) and atmospheric conditions (right) associated with October 2015 South Carolina floods. The map on the right shows water vapor. (*Source:* FEMA [2016]).

B.2.3   Impacts

With flood flows nearing or exceeding dam design flows, many dams were overtopped and failed, leading to subsequent overtopping failure of other downstream dams. Figure B-5 shows the locations of the dams that failed. Most of these were small dams, but because of the dense development and population adjacent and downstream of the dams, many were classified as high- or significant-hazard dams (Table B-2). Post-flood damage analysis revealed that of the 49 dams that failed, 30 failed because of overtopping, 6 because of piping, and 12 because of embankment failure; one dam was not assessed. Although the failed dams were all earthen, roughly half included grass- or soil-covered crests and the rest had paved or dirt roads at the crests. Heavy vegegation, which can penetrate earthen dams and contribute to failures, was observed at roughly half of the dams that failed. In addition, with many of the failed dams located in close proximity to other failed dams, it is possible that some failures were due to a domino-type effect, particularly from overtopping or structural failure.

Table B-2. Hazard (left) and size (right) classifications of South Carolina state-regulated dams that failed in the 2015 flood. (Data from FEMA [2016]).

a

Hazard classification	Count
High hazard	7
Significant hazard	17
Low hazard	25

b

Size	Total storage (ac-ft)	Height (ft)	Count
Very Small	< 50	< 25	0
Small	≥ 50 and < 1,000	≥ 25 and < 40	46
Intermediate	≥ 1,000 and < 50,000	≥ 40 and < 100	3
Large	≥ 50,000	≥ 100	0

- Among the dams that failed, the Semmes Lake Dam failure was subject to the most public attention. Semmes Lake Dam, owned and managed by the US Army in Fort Jackson, failed due to overtopping flows, causing Semmes Lake to drain (Figure B-7) and potentially contributing to the deaths of two individuals downstream of the dam. Various documentation before and after the failure describe the dam as in poor condition with problematic operational limitations:

- A local newspaper, The State, reported that two years before the Semmes Lake Dam failure, a 2013 USACE inspection report identified several physical concerns with the dam, including holes, broken equipment, and vegetation along the crest.[45]

- Stemming from a lawsuit (still in active litigation) brought upon by downstream property owners, the federal government released documents in March 2018 revealing court documents indicating (based on sworn deposition) that the Semmes Lake Dam spillway was modified to increase lake levels. According to the documents, concrete was added in the emergency spillway, reducing the spillway's release capacity and potentially contributing to the 2015 failure of the dam.[46]

- A 2016 USACE report also identified rusted and broken equipment that prevented the Army from lowering lake levels before the storm event.[47]

Before (Jan. 2015)	After (Dec. 2015)
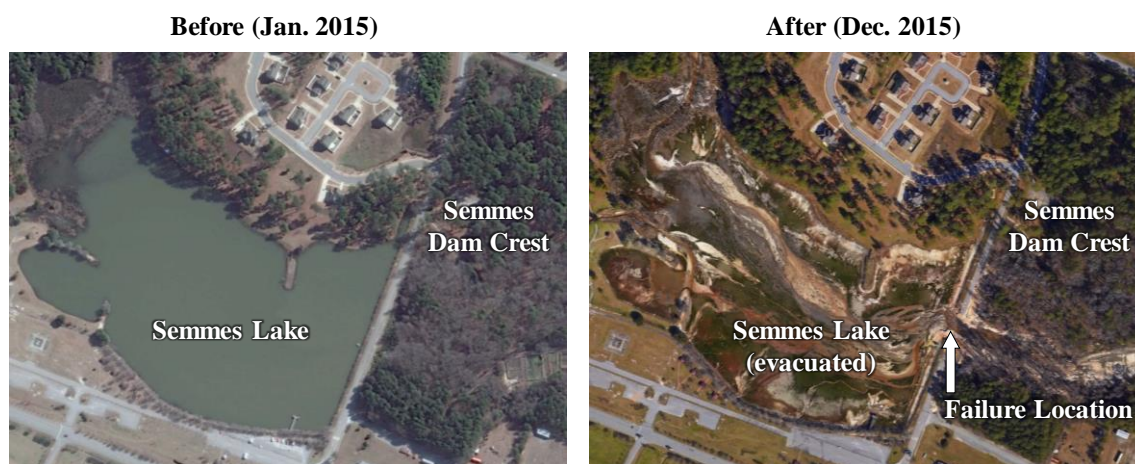
Figure B-7. Aerial imagery of Semmes Lake Dam before (left) and after (right) the 2015 overtopping flood failure. (Imagery from Google Earth).

The NCDC reports a total of 25 deaths and a total cost of $2.2 billion associated with the storm complex.[44] South Carolina accounted for $1.5 billion of the damage and 19 of the deaths, with an unknown number related to dam failure flooding (Mizzel et al. 2016).

B.2.4   Observations and Lessons Learned

As noted, rainfall in some locations exceeded NOAA Atlas 14 (Bonnin et al. 2006) 1,000-year precipitation frequency estimates. That level of precipitation and subsequent runoff overwhelmed much of the existing stormwater and dam infrastructure in central South Carolina, leading to significant flooding, dam failures, damage, and fatalities. Following the flood events, a team of experts conducted several field visits and a workshop to develop a set of findings and recommendations. These are documented in Flynn (2016), with those relevant to dam safety summarized briefly in the following list.

- Effective flood and infrastructure management requires coordinated governance to manage watersheds as a system of systems. This concept is in line with a systems analysis approach.

---

[45] https://www.thestate.com/news/local/article121521217.html (accessed November 2019)
[46] https://www.thestate.com/latest-news/article207162459.html (accessed November 2019)
[47] https://www.thestate.com/latest-news/article208158264.html (accessed November 2019)

- Improved information and visualization tools are needed for understanding complex infrastructure interdependencies and managing watersheds. The experts supported the development of tools for assessing the damage to and vulnerability of dams impacted by extreme weather events and flooding. While flood inundation maps helped to assess the locations of flood waters, it was recommended that more dynamic models be developed to provide insight into the quantity and timing of flooding for pre-disaster planning and to predict and manage watershed failure events.

B.3   2017 OROVILLE DAM SPILLWAY INCIDENT

B.3.1   Overview

In February 2017, the service and emergency spillways at Oroville Dam, California experienced significant damage following an initial failure of the service spillway chute slab and high reservoir inflow conditions that necessitated the use of spillway discharges. Operational decisions led to the eventual use of the emergency spillway for the first time in the dam's nearly 50-year operations. Subsequent, rapid headcutting of the embankment downstream of the emergency spillway weir prompted an evacuation order of 188,000 downstream residents as a precaution against potential dam failure.

Although uncontrolled reservoir releases did not result, the event led to a $1.1 billion spillway repair project. A significant effort was made to evaluate the spillway incident. An Independent Forensic Team (IFT) conducted detailed assessments over many months, resulting in the release of a public report in January 2018. The report (IFT 2018) describes the spillway incident as the result of a "complex interaction of relatively common physical, human, organizational, and industry factors, starting with the design of the project and continuing until the incident."

B.3.2   Oroville Dam and Drainage Basin

Oroville Dam is located in the Feather River Basin in northern California with an upstream drainage basin covering approximately 3,600 mi^2 along the western slopes of the Sierra Nevada Mountain range (Figure B-8). The region typically experiences warm, dry summers and cool, wet winters and springs, with most precipitation occurring in the cool season (November through March) and as snow at higher elevations. Stream flows can fluctuate significantly based on temperature and precipitation rates (Koczot et al. 2005).

At 770 ft in height, Oroville is the tallest dam in the US and began operation in May 1968 following initial construction in the early 1960s. According to the USACE NID[7], the dam offers flood control, hydropower, irrigation, recreation, and water supply benefits. It is owned and operated by the California Department of Water Resources (DWR) and is a component of the Oroville-Thermalito Complex, part of the broader California State Water Project, which is the largest state-owned water storage and delivery system in the US (IFT 2018).

The Oroville Dam facility comprises the main embankment dam, service spillway, emergency spillway, Hyatt Powerplant, and tunnel and outlet systems (Figure B-9). The service spillway is located on the right abutment and consists of an unlined approach channel, a gated headworks structure, a 3,000-ft-long by 179-ft-wide concrete-lined spillway chute, and concrete chute blocks for energy dissipation and flow dispersion. The emergency spillway is located to the right of the service spillway and includes a 930-ft-long gravity ogee weir and an 800-ft-long broad crested weir. (IFT 2018)

Figure B-8. Map of Feather River Basin upstream of Oroville Dam. (*Source:* USGS in Koczot et al. [2005]).

Figure B-9. Aerial imagery of Oroville Dam. (Imagery from Google Earth).

B.3.3   Flooding and Spillway Incident

According to DWR (2018), the Feather River Basin experienced the wettest January and February on record in 2017. During a 50-day span in January and February 2017, a year's worth of runoff flowed into Lake Oroville and required use of the Oroville Dam spillways.

On February 7, DWR personnel observed disturbances in the service spillway as discharge was increased to 52,500 cfs, and an order was made to close the spillway gates to facilitate inspection (IFT 2018). Visual inspection found a large portion of the service spillway chute slab was missing, with a large hole eroded beneath the missing section. With high reservoir inflows forecast and further spillway use needed, DWR began controlled testing of the damage spillway over the next few days to monitor erosion under varying flow conditions.

As major rainfall continued in the contributing watershed, the Lake Oroville water level continued to increase until it exceeded the emergency spillway crest. Water flowed over the emergency spillway for the first time in the project's nearly 50-year history, with overflow increasing for roughly 31 hours until it peaked at about 1.6 ft of overtopping with an estimated 12,500 cfs weir flow (IFT 2018). As water discharged downstream of the spillway weir, it channelized over the natural hillside and led to severe erosion and aggressive headcutting toward the emergency spillway crest structure.
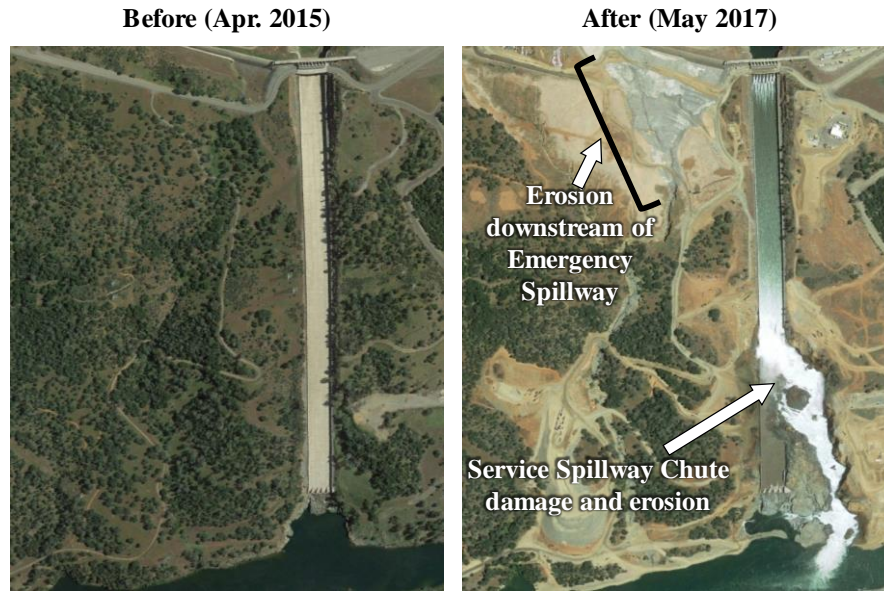
Shortly after overtopping flows had peaked, with erosive headcutting threatening the emergency spillway, an evacuation order was issued on February 12 for the roughly 188,000 downstream residents (IFT 2018). At the same time, DWR began increasing discharge through the service spillway, until it eventually reached about 100,000 cfs. This discharge rate was maintained for the next 3.5 days. Overtopping of the emergency spillway crest lasted for about 36 hours, 5 hours after peaking. The evacuation order was changed to an evacuation warning on February 14, which was later lifted on March 19. The service spillway continued operating with discharge through May 19 when the spillway gates were closed for the season to enable repair.

During the period from February 8 to May 19, the service spillway chute slab and surrounding earthen material continued to erode, with the eventual damage causing an 1100-ft-long by 200-ft-deep scar across the spillway and adjacent hillside.[48] A satellite-view comparison of the Oroville Dam spillways before and after (May 18, 2017) the 2017 incident is provided in Figure B-10.

During the multi-month period of spillway operation in 2017, DWR managed outflow and lake levels while crews repaired erosion areas, removed debris from the diversion pool, and constructed and improved access roads. DWR monitored the Oroville Dam, spillway gates, emergency spillway, Hyatt Powerplant, related structures, and geologic conditions and planned for the service and emergency spillway reconstruction (DWR 2018).

---

[48] Available at https://www.enr.com/articles/45391-a-race-to-the-finish-on-oroville-dam-spillway-fix (accessed November 2019)

Before (Apr. 2015)   **After (May 2017)**

Figure B-10. Aerial imagery of the Oroville Dam spillways before (left) and after (right) the 2017 spillway incident. (Imagery from Google Earth)

B.3.4 Forensic Investigation: Physical Factors

The path leading to the dangerous spillway erosion and eventual issuance of an evacuation order involved a complex series of events that were evaluated in detail by the IFT. As stated in IFT (2018):

> The Oroville incidents were not the result of any particular root cause leading down a simple chain of events to failure. Rather, the incidents were the result of numerous disparate, relatively common physical, human and organizational factors interacting, over the course of decades, with the two primary physical causes of the incident; these being:

- The significant depth of strongly weathered, erodible bedrock
- Vulnerabilities included in the chute slab design and construction

The IFT determined that the primary cause of the service spillway chute slab failure was uplift and removal of a section of the slab, with subsequent high-velocity flow causing erosion of the highly weathered rock and soil foundation beneath the slab and continued removal of the chute slab both upstream and downstream of the original failure location (IFT 2018). The uplift was likely caused by water uplift pressure beneath the slab in excess of the slab's uplift resistance, which raised the slab and would have rapidly increased the pressure and resulted in sudden slab failure. Other physical factors contributing to the service spillway incident included (1) deficient design of the service spillway drain and slab, which was noticed almost immediately after construction and required continued, periodic repair, and (2) simplified chute design, which excluded several more robust features used in other spillway chute designs when Oroville was being developed.

The IFT determined that the primary cause of the emergency spillway damage was "the presence of significant depths of erodible soil and rock in features orientated to allowed rapid headcutting toward the crest control structure" (IFT 2018). As stated in IFT (2018):

Other factors that contributed to the damage at the emergency spillway include:

- Hillside topography that concentrated flows and increased erosive forces, facilitating headcut formation
- Insufficient energy dissipation at the base of the spillway ogee crest structure
- Absence of erosion protection downstream of the crest structures

The service spillway discharge at which damage occurred (about 52,500 cfs) was not unprecedented, as flow rates were lower than the record spillway discharge of 160,000 cfs from January 1997 and other high discharge rates in 2005 and 2006 (IFT 2018). During the course of the incident, the spillway discharges were also well below the service spillway discharge capacity of 296,000 cfs and the emergency spillway discharge capacity of 350,000 cfs. Although the hillside downstream of the emergency spillway experienced significant erosion, note that the estimated peak discharge of 12,500 cfs was only about 3% of the spillway's discharge capacity. Figure. shows daily mean discharge from 1968 through 2017 in the Feather River at a location about 4 miles downstream of the service spillway outlet where flows are largely dictated by the combined discharges from Hyatt Powerplant and the service and emergency spillways.
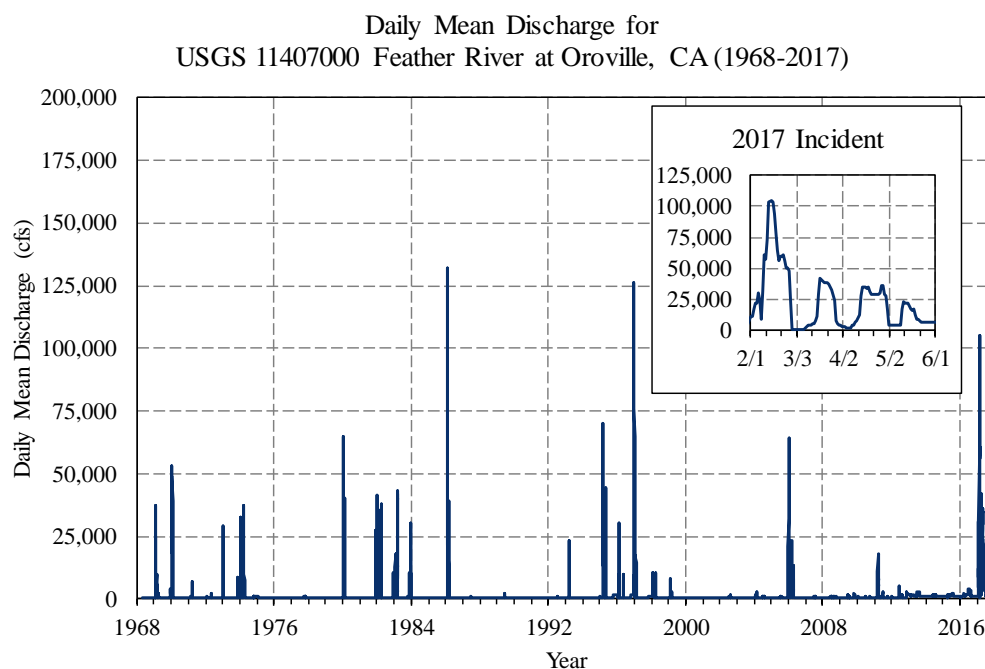
Figure. B-11. Feather River daily mean discharge at Oroville, CA from 1968-2017. (Data from USGS).

Numerous repairs to the service spillway chute slab concrete had been made since the original construction, including documented repairs in 1977, 1985, 1997, 2009, and 2013 (IFT 2018). Likely because of a shallow overlying depth of concrete, the concrete chute slab experienced cracking above and along underdrain pipes immediately after construction. The underdrain pipes, apparently intended to collect groundwater seepage beneath the slab, also collected large leakage flows from the spillway chute. Even with the spillway gates closed, significant drain outfall flows occurred when reservoir levels rose

high enough for gate leakage. Regarding the initial onset of damage to the service spillway chute slab, IFT (2018) states:

> The IFT believes that some combination of the following factors most likely was involved:
>
> - New chute slab damage and/or deterioration of previous slab repairs
> - Expansion of relatively shallow void(s) under the slab, through erosion or shrinkage of clay soils
> - Corrosion of the steel reinforcing bars or dowels across the concrete cracks or joints
> - Reduction in anchor capacity

B.3.5 Forensic Investigation: Human Factors

One of the principal factors driving decision-making during the most critical period of the spillway incident (after damage was observed and before the emergency spillway was activated) was the decision whether to increase service spillway discharges or allow reservoir levels to rise and trigger emergency spillway discharge. According to IFT (2018):

DWR was managing the incident with consideration of at least the following four issues:

- Continued erosion at the service spillway progressing toward and compromising the service spillway headgate structure

- Tailwater from spillway discharges, combined with debris blockage in the river, potentially flooding the Hyatt Powerplant

- Continued erosion at the service spillway causing failure of a power transmission tower located to the right of the service spillway chute

- Potentially overtopping the emergency spillway crest structure for the first time ever in the project's history, with unknown consequences.

Decision-makers were faced with the option to use the emergency spillway (a decision generally supported by operations personnel and DWR executives to reduce the risk of Hyatt Powerplant going offline) or to increase use of the service spillway (a decision generally supported by geologists, dam safety engineers, and Incident Command personnel onsite to reduce the risk of emergency spillway overtopping while maintaining maximum safe service spillway flow based on erosion monitoring) (IFT 2018). Attempts were made to balance risks by limiting service spillway flow to reduce erosion and prevent powerhouse flooding while avoiding overtopping of the emergency spillway.

To support decision-making, near-continuous hydrological modeling and forecasts were leveraged and indicated that higher spillway flows would be needed. According to IFT (2018),

> Hydrologic model uncertainty, although acknowledged, was intentionally ignored as the incident progressed. The use of mean model values was based on the belief that the risks of powerhouse flooding due to either the continued use of the service spillway or the use of the emergency spillway were essentially equivalent. Although perhaps true in regard to powerhouse flooding, the inherent additional risks associated with using the emergency spillway were not being fully considered. Specifically, the potentially unsatisfactory performance of the previously untested emergency spillway was not fully considered.

Despite efforts to maintain reservoir levels below the emergency spillway crest, the weir was eventually overtopped. According to IFT (2018):

> As seen in the Incident Command notes, there were two critical decision points that delayed releasing greater flows through the damaged service spillway, and essentially guaranteed that the emergency spillway would be overtopped, at least by a few inches.
>
> ...
> At these times, operations personnel were continuing to advocate to DWR managers their concerns regarding flooding of the powerplant and loss of the transmission tower due to further service spillway erosion, while DWR dam engineering and dam safety personnel were arguing strongly to avoid discharging over the emergency spillway, based on their review of geologic records from the files completed during the incident. The operational concerns carried the day.

As emergency spillway flows progressively eroded the downstream hillside, DWR was forced to increase the service spillway discharge to roughly 100,000 cfs (IFT 2018). Tailwater levels rose and eventually stabilized at more than 2 ft above the powerhouse flood level, 6 in. from flooding the plant.

According to IFT (2018), "the IFT believes that all decisions were made with the best of intentions, but that the risk tradeoffs were not adequately assessed, due to an unequal balance between the understanding of the potential consequences and the uncertainties of the options under consideration."

As documented in IFT (2018), other human factors contributing to the spillway incident included:

- Limited experience of the spillway designer and a lack of technical expertise in reviewing potential failure modes and geology.

- Inadequate communication between the designer and geologists during design and a lack of consultation with the designer during construction.

- Potential cost and schedule pressures during design and construction.

- Significant overconfidence and complacency from DWR regarding its State Water Project civil infrastructure.

- Strained internal relationships within the DWR organization.

- "Ignorance about the existence of the risks associated with the spillways, which was mainly due to insufficient expertise regarding spillway failure modes and mischaracterization of the geology."

- Weak dam safety culture in which "dam safety did not have adequate priority relative to non-safety goals, such as delivering water, generating power, and controlling costs."

- "Systemic failure of DWR, regulatory, and general industry practices to recognize and address the deficiencies and warning signs that preceded the incident."

B.3.6   Observations and Lessons Learned

Many critical lessons can be learned from the 2017 Oroville Dam spillway incident, many of which are well documented in IFT (2018):

The following are some of the general lessons to be learned by the broader dam safety community:

- To ensure the safe management of water retention and conveyance structures, dam owners must develop and maintain mature dam safety management programs that are based on a strong "top-down" dam safety culture. There should be one executive specifically charged with overall responsibility for dam safety, and this executive should be fully aware of dam safety concerns and prioritizations through direct and regular reporting from a designated dam safety professional, to ensure that "the balance is right" in terms of the organization's priorities.

- More frequent physical inspections are not always sufficient to identify risks and manage safety.

- Periodic comprehensive reviews of original design and construction and subsequent performance are imperative. These reviews should be based on complete records and need to be more in-depth than periodic general reviews, such as the current FERC-mandated 5-year reviews.

- Appurtenant structures associated with dams, such as spillways, outlet works, and power plants, must be given attention by qualified individuals. This attention should be commensurate with the risks that the facilities pose to the public, the environment, and dam owners, including risks associated with events which may not result in uncontrolled release of reservoirs, but are still highly consequential.

- Shortcomings of the current Potential Failure Mode Analysis (PFMA) processes in dealing with complex systems must be recognized and addressed. A critical review of these processes in dam safety practice is warranted, comparing their strengths and weaknesses with risk assessment processes used in other industries worldwide and by other federal agencies. Evolution of "best practice" must continue by supplementing current practice with new approaches, as appropriate.

- Compliance with regulatory requirements is not sufficient to manage risk and meet dam owners' legal and ethical responsibilities.

While Oroville was subject to numerous inspections and reviews occurring at roughly 5 year intervals, the spillway failure modes that occurred in 2017 were identified in almost none of the reviews (IFT 2018). The 2004, 2009, and 2014 review efforts were coordinated with PFMAs in the same years. The 2014 PFMA (described by a very senior, experienced, and respected engineer "as thorough a PFMA as he had ever been involved with") was the first time that the 2017 spillway failure modes had been considered. Although the 2017 service spillway PFM was practically identified during the 2014 PFMA, it was ruled out because it would not result in an uncontrolled reservoir release, primarily owing to generally non-erodible rock foundations. Failure of the service spillway chute slab was considered at a high level, but the PFMA team concluded that slab erosion would not progress to the headgate structure and result in uncontrolled reservoir release.

The IFT concluded (IFT 2018):

- "A critical review of the current PFMA process itself is required", including comparison with other risk assessment processes such as FMEA, fault tree analysis, and various analyses based on systems theory;

- "By limiting the PFMA process to considering mainly failures resulting in uncontrolled release of the reservoir, the process can miss component failures that can be very significant to the dam owner and downstream residents"; and

- "The current PFMA process can have difficulties in properly characterizing risks for large, complex systems, including accounting for human and operational aspects in failures" and "does not explicitly consider how broader organizational factors, such as culture and decision-making authority and practices, can contribute to failure."

The IFT also considered information management shortcomings that affected the incident, noting that in contrast to the non-centralized information stored by DWR, "the system currently used by Reclamation as part of its Safety Evaluation of Existing Dams (SEED) process is a good example" for electronic information management for dams (IFT 2018).

From a regulatory perspective, the IFT noted that "regulators must strive to be fair and reasonable in weighing a) the costs they impose on dam owners in order to perform studies and construction versus b) risks imposed on the public," a situation that involves considerable uncertainty and that resembles the position dam owners face during risk management decision-making (IFT 2018).

A USACE memorandum (USACE 2017) prepared shortly after the Oroville spillway incident aimed to assess the incident and the likely outcomes if USACE internal risk analysis methodologies, including PFMA, had been applied before the incident. The findings, which were based on preliminary analysis, were that the outcome likely would have been similar to the Oroville 2014 PFMA. It was found that although the USACE methodology likely would have identified the potential failure modes that occurred, given the service spillway's previous good performance, the low estimated likelihood of uncontrolled reservoir release, and the unlikelihood of identification of the emergency spillway headcutting as a primary risk driver, "it is unlikely that all the events that occurred at Oroville would have been envisioned by a USACE risk assessment team."

The memorandum (USACE 2017) provided preliminary conclusions, including that (1) risk assessments typically consider the risk of uncontrolled reservoir release, which may be small despite significant damage and erosion, and (2) event trees that dead-end (without reservoir breach) typically do not consider how certain events affect other failure modes (e.g., damage to the Oroville service spillway significantly changing its operation). Further statements were also provided for future consideration, including that "when Potential Failure Modes are evaluated during a risk analysis, events that can be caused by unplanned operation decisions, or due to poor or unexpected performance of another feature on the project, may not be captured."

B.4   CITED REFERENCES FOR APPENDIX B

Bonnin, G. M., D. Martin, B. Lin, T. Parzybok, M. Yekta, and D. Riley. (2006). *Precipitation-Frequency Atlas of the United States: Volume 2 Version 3.0*, National Oceanic and Atmostpheric Administration, Silver Spring, MD, 295.

DWR (California Department of Water Resources). (2018). "Oroville spillways incident background." California Department of Water Resources.

FEMA (Federal Emergency Management Agency). (2016) *South Carolina Dam Failure Assessment and Advisement*. Federal Emergency Management Agency, Washington, DC, p. 73.

Flynn, S. E. (2016). *The South Carolina Deluge: Lessons from a Watershed Disaster*. Northeastern University, Center for Resilience Studies, p. 78.

GAO (General Accounting Office). (2014). *Missouri River Flood and Drought: Experts Agree the Corps Took Appropriate Action Given the Circumstances, but Should Examine New Forecasting Techniques*, GAO-14-741 US Government Accountability Office, Washington, DC, p. 55.

IFT (Independent Forensics Team). (2018). *Independent Forensic Team Report: Oroville Dam Spillway Incident*. Independent Forensic Team.

Koczot, K. M., A. E. Jeton, B. McGurk, and M. D. Dettinger. (2005). *Precipitation-Runoff Processes in the Feather River Basin, Northeastern California, and Streamflow Predictability*, Water Years 1971-97, US Geological Survey, Sacramento, CA, p. 92.

Maximuk, L. P. and V. L. Nadolski. (2012). *The Missouri/Souris River Floods of May–August 2011*, National Weather Service, Silver Spring, MD, p. 104.

Mizzell, H., M. Malsick, and W. Tyler. (2016). "The historic South Carolina rainfall and major floods of October 1–5, 2015." *Journal of South Carolina Water Resources* 3(1), 3–7.

USACE. (2006). *Missouri River Mainstem Reservoir System Master Water Control Manual: Missouri River Basin*. US Army Corps of Engineers, Omaha, NE.

USACE. (2012a). *Post 2011 Flood Event Analysis of Missouri River Mainstem Flood Control Storage*, US Army Corps of Engineers, Portland, OR.

USACE. (2012b). *Missouri River Flood 2011 Vulnerabilities Assessment Report Volume I: Summary*, US Army Corps of Engineers, Portland, OR.

USACE. (2012c). *Missouri River Flood 2011 Vulnerabilities Assessment Report Volume II: Technical Report*, US Army Corps of Engineers, Portland, OR.

USACE. (2017). "Preliminary lessons learned from Oroville incident." US Army Corps of Engineers memorandum, G.A. Scott to E. Halpin, April 7, 2017.