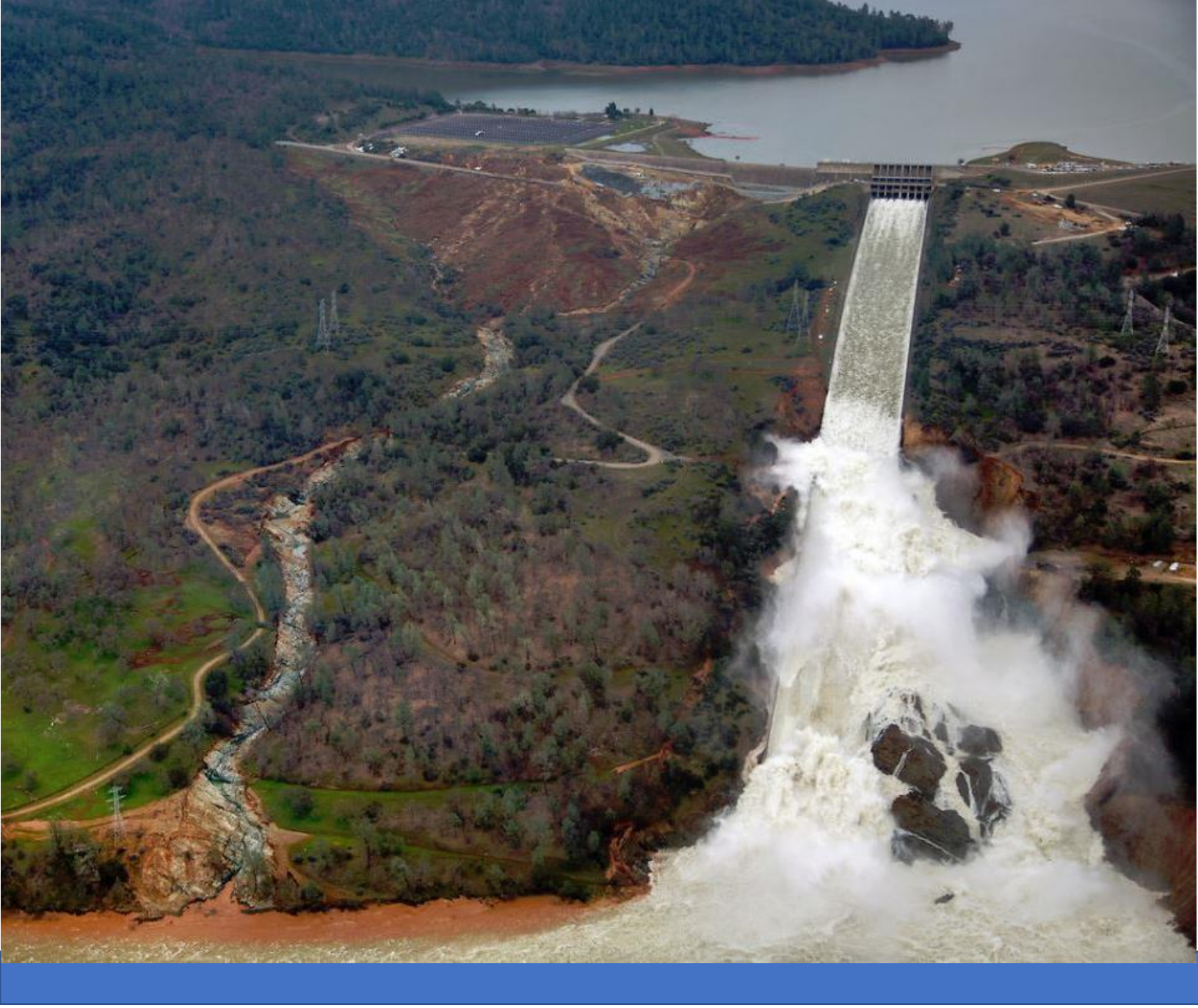


Community "Safety" Following Comprehensive Study - Oroville Dam

May 10, 2021

Safety • Risk-Reduction • Resilience • Reliability
SafeR3

Storesund Consulting

THE UNIVERSITY OF CALIFORNIA BERKELEY 1868

CCRM

PREFACE

*The question is whether dam owners, regulators, and other dam safety professionals will recognize that many of these lessons are actually **still to be** learned. 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 Report* [1]

The Oroville Dam Primary Spillway failed in February 2017 during 'under-whelming' conditions.

The challenge of safety and reliability in Socio-Technical Systems, such as Dams, is multi-faceted and complex. As a result, the appropriate 'requisite variety[1]' of expertise and management methods required to appropriately address the intended safety and reliability is much broader than currently in place for Dams, especially high-hazard dams, faced with aging issues and future climate change, that have the potential to result in catastrophic loss of lives.

In response to the 2017 February Oroville Primary Spillway incident, DWR has invested significant effort in "risk-based" methods. Risk-based methods are useful, but not foolproof and have yet to be formally established as valid and reliable. There is much untapped knowledge and best practices from other industries that can greatly enhance safety and reliability of our nation's Dams.

With respect to the recently completed "Comprehensive Needs Assessment," a focus solely on largely unvalidated risk-based methods is resulting in oversimplification of the complex Oroville Dam Socio-Technical System and results in a significant E3 error – solving the wrong problem precisely and/or only solving some of the problems and ignoring many others. Solving the wrong problem precisely, leaves the community vulnerable to the occurrence of a preventable catastrophic event.

From the California Water Code Section 6102 (*emphasis by author*)

> *(b) Globally and nationally, there is recognition that, as with all aging infrastructure, there is an unmet need regarding dam maintenance and repairs.* ***California needs to continue to lead efforts to address these unmet needs, and improve upon standards set by regulatory agencies to ensure public safety****.*
>
> *(c) …California's dam safety procedures must stay on par with, or ahead of, best practices and must continually update those procedures based on the* ***best available knowledge****.*

These directives from the California Water Code Section 6102, along with the 'call to action' by the IFT to challenge fundamental assumptions relative to the safety and reliability of Dams, are the drivers for this report. The global collective experience of the Safety and Reliability Community across all infrastructure domains, tells us we can do much better and that significant gains in reduced risk and enhanced safety and reliability are readily achievable, if we embrace a philosophy of 'continual improvement' and 'valid and reliable' management methods.

To the question, is the community downstream of Oroville Dam safe? Potentially. Are there additional unutilized/unadopted practices available, with respect to Dams, to triangulate Safety and Reliability in the spirit of "trust but verify" that would prevent future avoidable incidents – YES! Are these currently embraced? NO!

[1] Requisite Variety - in order to deal properly with the diversity of problems the world throws at you, you need to have a repertoire of responses which is (at least) as nuanced as the problems you face

About the Author

Dr. Rune Storesund is a licensed Civil (California, Louisiana, Hawaii, Washington) and Geotechnical (California) Engineer with 20 years of civil engineering experience and over 16 years of forensic engineering experience in the areas of geotechnical, water resource, and environmental engineering. He provides civil forensics support for pre-trial review, engineering standard of care, document/data review and synthesis, engineering contract review, forensic investigations and analyses, failure mode analysis, legal visual aids & animations, and expert witness services. He has a Doctorate of Engineering in Civil Systems and a Masters in Geotechnical Engineering from University of California, Berkeley.

Dr. Storesund is the Executive Director of University of California, Berkeley's Center for Catastrophic Risk Management, a group of academic researchers and practitioners who recognize the need for interdisciplinary solutions to avoid and mitigate tragic events. This group of internationally recognized experts in the fields of engineering, social science, medicine, public health, public policy, and law was formed following the tragic consequences of Hurricane Katrina to formulate ways for researchers and experts to share their lifesaving knowledge and experience with industry and government.

Dr. Storesund is the founder and director of SafeR3, a global non-profit that pioneers Risk and Crisis Management education and technology development that facilitates dissemination of "state-of-the-art" and innovative enterprise risk management to "state-of-the-practice" for daily use in organizations to reduce risk via pragmatic tools and education that increase safety, resilience, and reliability as well as the ability to quantify risk-reduction.

Dr. Storesund is a Senior Member of the National Academy of Forensic Engineers and Board-Certified Diplomate in Forensic Engineering. He serves as a technical reviewer for the National Academy of Forensic Engineers (NAFE) Journal.

Dr. Storesund is the CEO and founding member of NextGen Mapping, Inc., a software start-up company focused on leveraging big data associated with infrastructure systems to improve decision-making and connect decision-makers with real time (or near-real time) business intelligence models to enable informed and educated decisions.

Dr. Storesund is also the President of Storesund Construction, Inc. (SCI), a California General Contractor (Class A and Class B). SCI performs civil infrastructure projects, focused primarily on water resource infrastructure such as water storage and conveyance systems.

Dr. Storesund served as a Risk Management Technical Expert, as the Executive Director of UC Berkeley's Center for Catastrophic Risk Management (CCRM), on the Oroville Dam "Comprehensive Needs Assessment" Ad Hoc Committee between November 2018 and December 2020. This report is formulated as a volunteer effort through the non-profit "SafeR^3," which provides risk and crisis management education and technology development to disseminate state-of-the-art and innovative enterprise risk management to the state-of-the-practice via pragmatic tools and education that increases safety, resilience, and reliability as well as measurable risk-reduction.

Acknowledgements

The following individuals have been instrumental in the development and review of this paper. Their assistance is greatly appreciated: Prof. Karlene Roberts (UC Berkeley CCRM); Prof. Paul Schulman (Mills College); and Dr. Ian Mitroff (UC Berkeley CCRM).

CONTENTS

APPENDICES

EXECUTIVE SUMMARY

This report provides feedback on the Department of Water Resource's "Oroville Dam Comprehensive Needs Assessment," or DWR CNA for short. The purpose of the CNA was to "to assess the facilities within the Oroville Dam Complex to identify further dam safety and operational needs" [2]. This study followed findings from an Independent Forensic Team (IFT) [1] that found a number of 'lessons to be learned' following the 2017 Primary Spillway failure in order to achieve the intended degree of safety for not only Oroville Dam, but dams in general.

The feedback in this report is framed from the standpoint of the Oroville Community that was impacted by the consequences associated with the February 7, 2017 failure of the Oroville Dam Primary Spillway, rather than from a technical engineering perspective. The IFT noted [1]:

> *The question is whether dam owners, regulators, and other dam safety professionals will recognize that many of these lessons are actually still to be learned. 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.*

An overview of the Oroville Dam Complex and the 2017 failure of the primary spillway is presented. The purpose and intent of the DWR "Comprehensive Needs Assessment" (CNA) and role of the Ad Hoc Committee formulated by Senator Nielsen and Assemblyman Gallagher is discussed. Background information on Socio-Technical Systems, Safety Culture, and Valid and Reliable approaches is presented. A review of the 2018 IFT recommendations are listed as well as the reported outcomes from the DWR CNA initiative. Commentary associated with implementation of the IFT recommendations by DWR via the CNA initiative is discussed. Finally, specific recommendations are presented and discussed. The recommendations of this report are:

- Revise the California Water Code Section 6102 (Lead = CA Legislature; Timeframe – months to years)
- Perform Design Assumption Audits (Lead = CA DWR; Timeframe – months to years)
- Implement Life-Cycle-Based Management (Lead = CA DWR; Timeframe – month to years)
- DSOD Standalone Organization (Lead = CA Legislature; Timeframe – months to years)
- Utilization of a "Performance Insurance" (Lead = CA Legislature; Timeframe –years)

The safety culture literature cautions against putting all your eggs in one 'basket' when it comes to 'mindfulness of potential "preventable-irreversible" problems.' As presented, the CNA/DWR is 'following' the federal agencies into the domain of 'risk-informed decision-making' (RIDM). RIDM was used by many organizations and STILL RESULTED IN PREVENTABLE FAILURES (Boeing 737 MAX, Deepwater Horizon, PGE Wildfires, Fukushima, etc. [2]).

These recommendations are structured to not remove a basket, but to augment through additional baskets. This also puts DWR in a position of leadership as opposed to being 'followers.' The recent updates to the water code look to California to be leaders, not followers. The internal DWR working theory may be that DWR is doing 'best practice' with respect to dams because it is 'following' the regulatory minimum, but 'dams' is not doing 'best practice' with respect to safety and reliability from the 'safety culture' standpoint. DWR, if it chooses, can help the dam owner/operator community to catch up to the international 'best practice' on safety and reliability.

INTRODUCTION

This report provides feedback on the Department of Water Resource's "Oroville Dam Comprehensive Needs Assessment," or DWR CNA for short. The purpose of the CNA was to "to assess the facilities within the Oroville Dam Complex to identify further dam safety and operational needs" [3]. This study followed findings from an Independent Forensic Team (IFT) [1] that found a number of 'lessons to be learned' following the 2017 Primary Spillway failure in order to achieve the intended degree of safety for not only Oroville Dam, but dams in general.

The feedback in this report is framed from the standpoint of the Oroville Community that was impacted by the consequences associated with the February 7, 2017 failure of the Oroville Dam Primary Spillway, rather than from a technical engineering perspective. As a result of the Oroville Dam Complex being subject to the public disclosure limitations associated with "Critical Energy Infrastructure Information" (CEII), the public has very limited ability to 'verify' the accuracy and appropriateness of safety evaluations performed by most high-hazard dam owner/operators. This results in the public having to "trust" the purported degree of safety represented by the dam owner/operator without the ability to independently verify the reasonableness, appropriateness, completeness, and validity of the reported results. The IFT noted [1]:

> *The question is whether dam owners, regulators, and other dam safety professionals will recognize that many of these lessons are actually **still to be learned**. 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.*

This evaluation explores the degree to which the 'lessons to be learned' have been learned and incorporated into the management practices of dams to better ensure the represented level of safety matches the actual level of safety in aging legacy infrastructures, which are subject to enhanced hazards as a result of climate change.

Oroville Dam Complex

Oroville Dam is situated in the foothills of the eastern Sierra-Nevada mountain range in Butte County, California. The dam is located approximately 70 miles north of Sacramento and 22 miles southeast of Chico (Figure 1). The Oroville Dam Complex consists of the main dam, Hyatt powerplant, primary service spillway, and emergency overflow weir (Figure 2).

The dam is owned and operated by the California Department of Water Resources (DWR) as part of the State Water Project. The State Water Project has ongoing water supply and delivery contracts with water contractors throughout the State of California (Figure 3). The Oroville Dam project received construction cost-share contributions and technical design support from the U.S. Army Corps of Engineers in order to provide flood control and mitigation on the Feather River. Additionally, federal oversight is provided by the Federal Energy Regulatory Commission (FERC) due to the presence of the 841-MegaWatt Hyatt Power Plant [1].

Oroville Dam was designed to accommodate water storage as part of the State Water Project (SWP), a flood control reservoir, and public recreational space. The reservoir has a storage capacity of approximately 3.6 million acre-feet [1]. The Primary Spillway was rated for a maximum discharge of 296,000 cubic feet per second (cfs) [1].

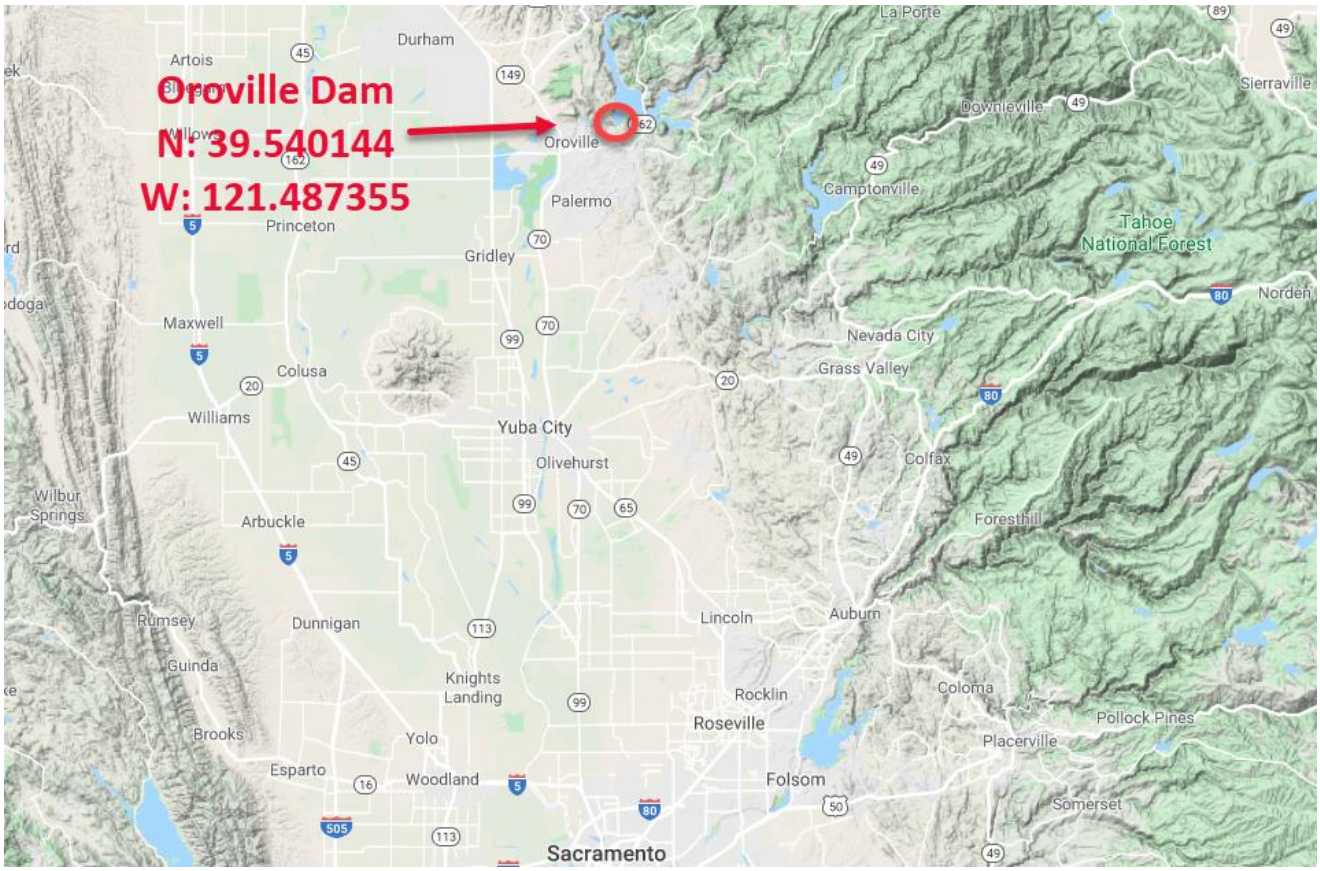


Figure 1: Oroville Dam located in Oroville, CA, southeast of Chico and north of Sacramento.

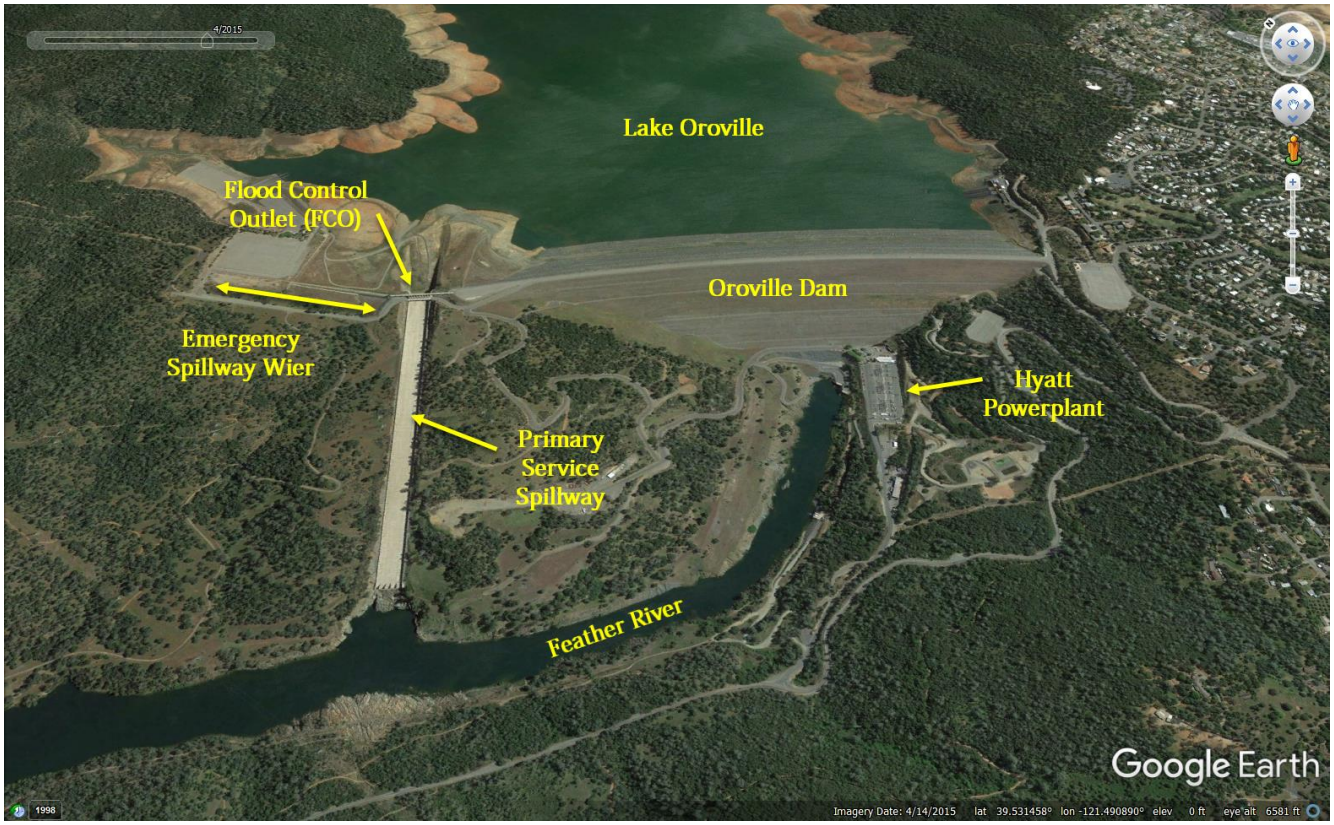


Figure 2: Overview of Oroville Dam and ancillary features.

Figure 3: Overview of the California State Water Project [4].

2017 Primary Spillway Failure

Failure of the Primary Spillway was first detected in the morning of February 7, 2017. The failure occurred about halfway down the spillway alignment (Figure 4, Figure 5). A chronology of events [1] is shown in Figure 6. After observation of the initial anomaly, the Flood Control Outlet gates were closed and discharge terminated so a more detailed visual inspection could take place. Figure 7 shows the extents of the initial failure area.

During this time, precipitation events were resulting in inflows into Lake Oroville. Various discharge rates were tested February 8 and February 9. Lake Oroville was allowed to reach El. + 901 ft, which resulted in activation of the Emergency Spillway. Flows down the Emergency Spillway resulted in visible erosion and scour of the surficial soils, which led to concerns about the integrity of the Emergency Spillway, and, subsequently the overall integrity of Oroville Dam.

An Evacuation Order was issued at 3:44 pm on February 12, 2017 and just under 200,000 community members were ordered to immediately evacuate [1]. The Evacuation Order was changed to an Evacuation Warning on February 14 and the Evacuation Warning was lifted five weeks after the Evacuation Order was first issued [1].

Figure 4: Location of initial failure of the reinforced concrete chute slab in the Primary Spillway, February 2017.

Figure 5: View looking up spillway during post-failure releases [5].

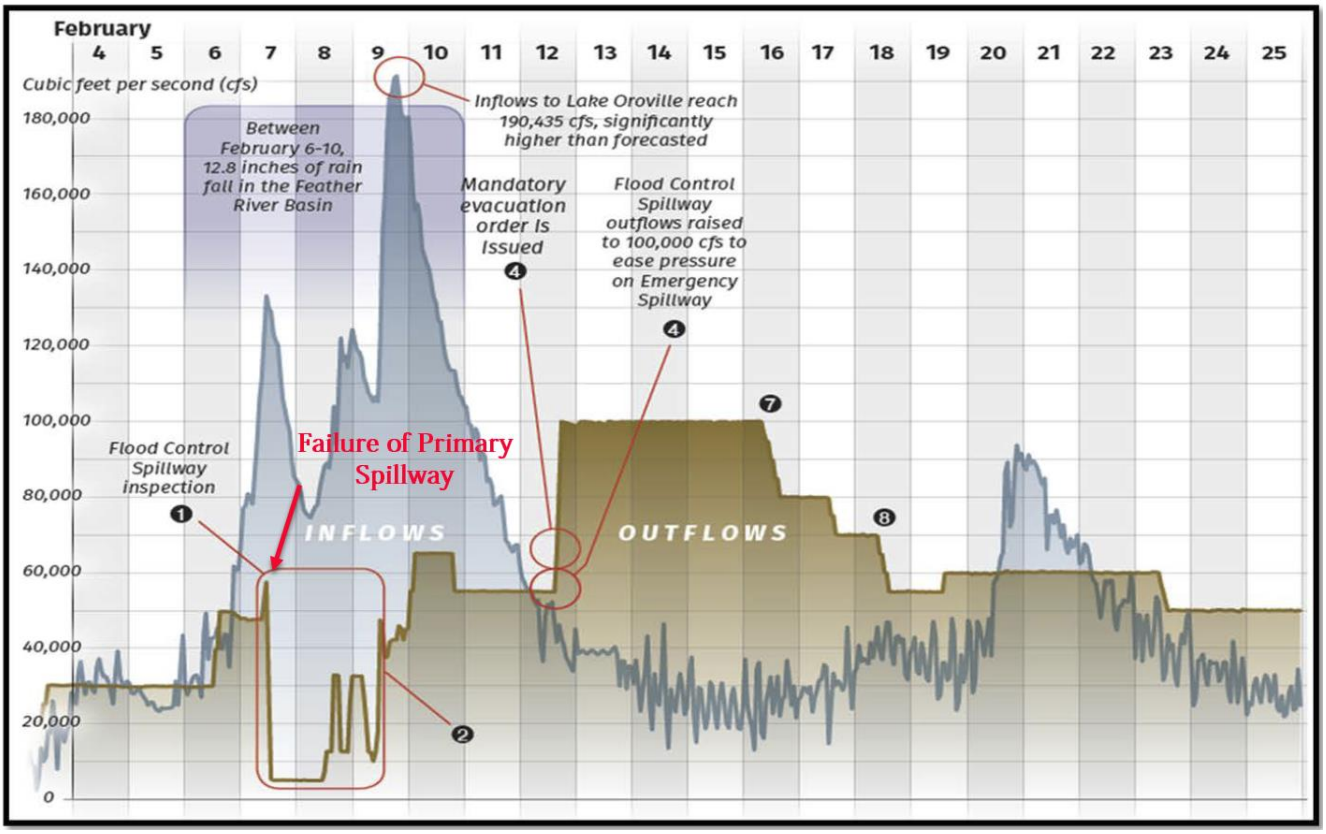


Figure 6: Chronology of reservoir inflows and outflows during February 2017 [1].

Figure 7: View of the initial failure area on February 7, 2021 [1].

Figure 8: Utilization of the Emergency Spillway resulting in downstream erosion/scour [6].

Figure 9: Community updates during the Evacuation Order period [7].

DWR Comprehensive Needs Assessment[2]

Following the 2017 Oroville Spillway Incident, DWR made commitments to the Oroville community, federal and state dam safety regulators, the Federal Energy Regulatory Commission (FERC) and the California Division of Safety of Dams (DSOD), to assess the facilities within the Oroville Dam Complex to identify further dam safety and operational needs. In addition, DWR committed to identifying potential measures to address those needs and reduce dam safety risks. In January 2018, DWR initiated the Oroville Dam Safety "Comprehensive Needs Assessment" (CNA) and the report published in November 2020.

The CNA process was led by DWR as the owner of the Dam. As part of the process, an "Independent Review Board" (IRB) of dam experts conducted technical reviews of key deliverables and documented review findings. The IRB was charged with a review and assessment on these specific topics [8]:

A. Proposed alternatives to restore the spillway design capacity

- Current design flood and combined spillway capacity needs
- Capacity of the combined spillways once emergency recovery efforts conclude
- Alternatives to provide any shortfall in spillway capacity

B. Proposed project flood operations associated with various alternatives

- Flood operations under alternatives identified in other tasks
- Post-emergency water control manual proposal

C. Proposed remedial options for the service spillway headworks

- Potential risks to the headworks
- Studies and assessments of different features of the headworks
- Testing, maintenance, and mitigation projects

D. Proposed low-level outlet alternatives

- Alternative outlet concepts
- Reservoir drawdown benefits
- Potential construction, operation, long-term maintenance risks

E. Proposed dam embankment reliability and improvements

- Current projects related to slope stability and seepage
- Seepage and stability evaluations
- Alternative additional mitigation projects

F. Proposed dam complex instrumentation and monitoring plans

- Plan for additional instrumentation for the reconstructed and new spillway structures
- Updated instrumentation data gathering, surveillance, and monitoring plan

The CNA also included engagement with an Ad Hoc Group of community stakeholders appointed by Senator Jim Nielsen and Assembly member James Gallagher. The Ad Hoc community group met intermittently with DWR and the IRB. The Ad Hoc group provided community perspectives and communicated about the CNA process and findings to the larger Oroville community.

The CNA final report includes a summary of the risk analysis process and findings and includes recommendations for future next steps and future projects. The final report has been submitted to FERC and DSOD.

Ad-Hoc Committee[2]

Senator Jim Nielsen and Assemblyman James Gallagher appointed a group of community members to represent the community during the CNA. The Ad Hoc Community group's role was primarily to communicate accurate information and context about elements of the CNA under consideration – and the final document – to the stakeholders and interest groups that they represent. The Ad Hoc Group also provided informed community and stakeholder perspectives to the IRB as the Oroville Dam CNA was developed. The Ad Hoc Group received questions about the CNA from the community and interested parties and communicated relevant questions or concerns to the IRB.

Meeting #1	Wed 18 Jul 2018
Meeting #2	Tue 30 Oct 2018
Meeting #3	Thu 10 Jan 2019
Meeting #4	Thu 4 Apr 2019

Meeting #5	Fri 9 Aug 2019 & Wed 16 Oct 2019
Meeting #6	Wed 13 Nov 2019
Meeting #7	Fri 26 Jun 2020
Meeting #8	Fri 9 Oct 2020

SOCIO-TECHNICAL SYSTEMS

Dams are a type of Socio-Technical System. The concept of socio-technical systems gained traction following WWII and stems from research on coal mining workflows in England following WWII, captures the inseparable relationship between human and organizational factors and their physical system components. The working hypothesis was that improved operational system performance would be realized by leveraging the knowledge and capabilities of workers to confront technological uncertainty, variation, and adaptation. This perspective is very important when examining the performance of 'systems' that are operated and managed by 'people.'

Socio-Technical Systems are a bit unique in that throughout their life-cycle, they are subjected to inputs and decision-points by different individuals, different organizations, and at different life-stages, where common life-cycle stages include: I will refer to this as 'organizational perspectives.' As a result of differing organizational perspectives, a system is subjected to an array of human and organizational across its life-cycle. Life-cycle stages consist of:

- Planning
- Design
- Construction
- Operations/Maintenance
- Requalification (frequently omitted because a formal 'design life' is not specified)
- Decommissioning

[2] As described by DWR [1]

Decision-making timeframes across these organizational perspectives vary greatly. At one end of the decision-making spectrum, operators frequently need to make split-second decisions. These decisions can be risk-reducing by increasing system capacity or decreasing system demands to ensure anticipated system performance. These operator-based decisions could also inadvertently increase system demands or decrease system capacity, resulting in unintended outcomes or 'failures.'

Socio-Technical Systems performance is also subjected to longer term-policy based decision-points, over the course of years to decades, that can impact investments in safety and training approaches. Examples of this include chronic deferred maintenance, under-staffing/training, and new requirements from updated engineering design codes.

It is important to recognize that human and organizational factors are just as important to system performance, if not more important, than the physical loads engineers are accustomed to addressing. To achieve the intended level of safety and reliability, one must account for all these different organizational perspectives and decision-timeframes, otherwise the evaluation will be incomplete and the wrong problem will be solved precisely (E3 error).

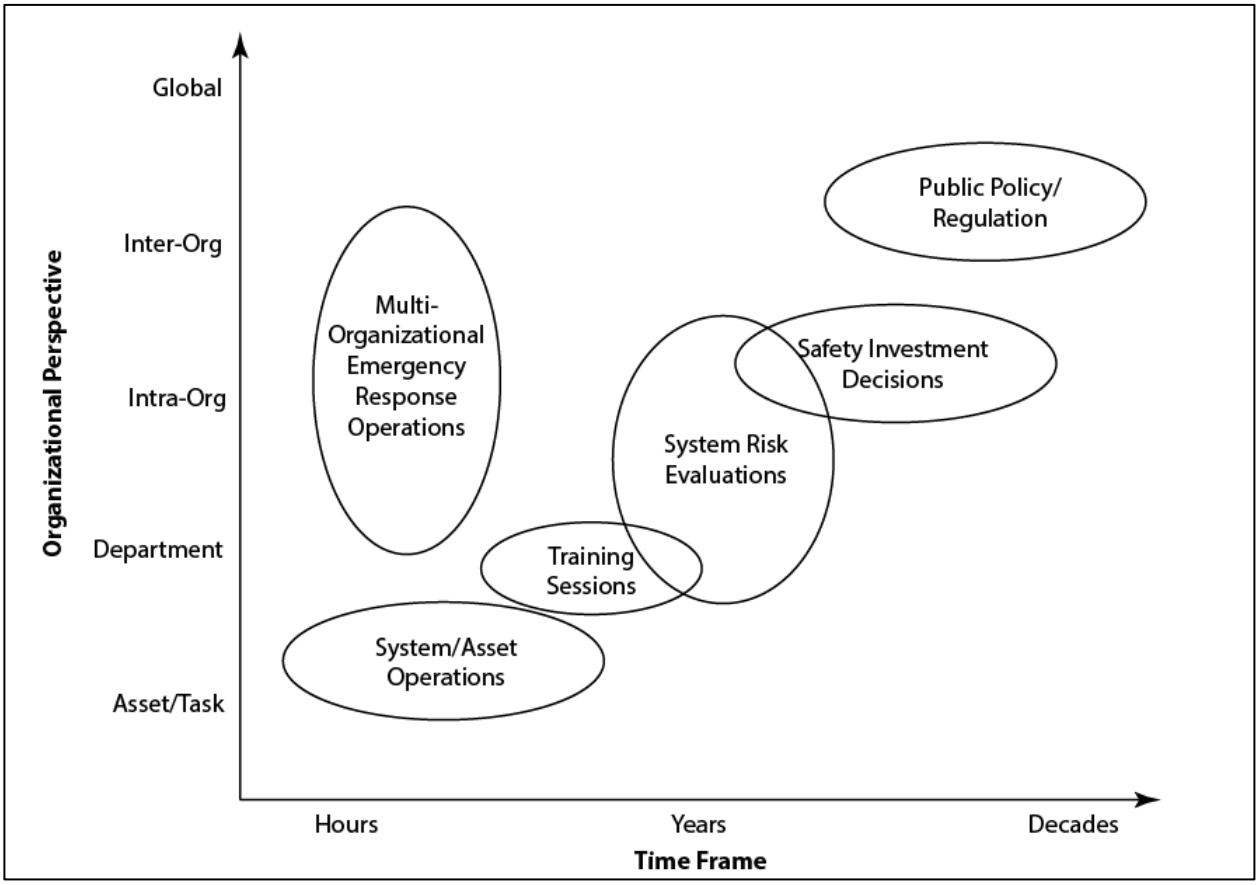


Figure 10: Organizational perspectives within generic Socio-Technical Systems.

In addition to the varying range of organizational perspectives, additional uncertainty is injected into the process at all life cycle stages just by the limitation of knowledge. Examples of these knowledge limitations include elements in Figure 11, such as simplifications, incompleteness, ambiguity, and inconsistencies. All of these factors contribute to uncertainty of safety and reliability of civil works. Many of these factors are omitted from current risk analyses. These omissions result in UNDER-SPECIFYING the "risk" and over-promising the actual level of safety and reliability of the structure. Further, under-specifying the risk, leads to over-confidence in system performance and reduced

'crisis management' capabilities/resources to interactively respond to 'surprises' by reduce the magnitude of consequences or reducing the likelihood of failure or both.

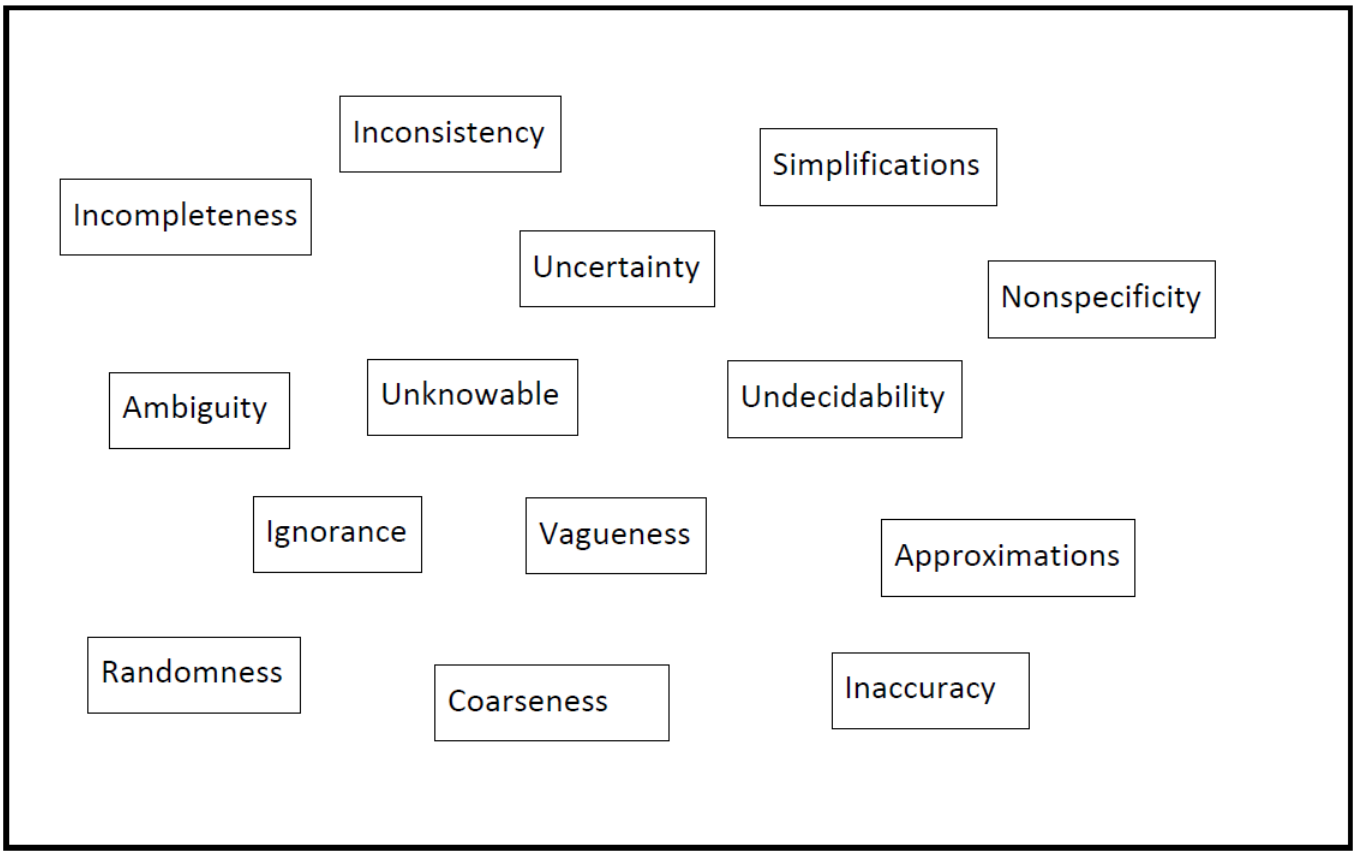


Figure 11: Select examples of knowledge limitations that preclude a full and exhaustive inventory of safety and reliability vulnerabilities.

Lastly, engineers and the engineering profession tend to shy away from social aspects of the civil works projects they design and focus primarily on the physical aspects of these systems. Dr. Ed Wenk, the first Congressional Science Advisor (1959); science advisor to Presidents Kennedy, Johnson, and Nixon; member of the National Academy of Engineering; and emeritus professor of engineering, public affairs, and social management of technology at the University of Washington in Seattle said this of the social aspects of our infrastructure systems and engineering [9]:

> *As we expose the human ingredient, we encounter properties of individual character – the noblest of creativity, altruism, compassion, the dedication to life, liberty and the pursuit of happiness. On the other hand, we confront universal weaknesses of ignorance, error, blunder, and folly, temptations from ambition, greed, envy, pride, fear, and vanity, and threats from just plain mischief.*
>
> *Engineers have long been aware of these dangers, especially from ignorance and error. History records an incalculable number of accidents attributed to human failings. Such threads led engineers – concerned with the integrity of design – to introduce concepts of safety margins. At first, these were derived empirically. The soaring Gothic cathedrals with their flying buttresses now stand because of lessons from those that fell down. The safety of pressure vessels is now assured from principles sought after explosions on steamboats wiped out hundreds of passengers.*

By such contingencies in design, engineers accommodate uncertainties in theories, in design assumptions, in loading, in quality of materials and fabrication, in use, and in abuse. These safety margins impose two people-related elements in practice. The first is recognition of potential harm to people or property from engineering failure, and social responsibility – now backed by law – to reduce risk.

…If engineering is to be practiced as a profession and not just a technical craft, attention must be focused on context as well as content. That is, the design of complex megasystems for transportation, communications, public health, or whatever must harmonize their principles from the natural sciences with an understanding of human values, their expression in cultural norms, and the role of law and of government in serving the public interest by balancing human rights with property rights.

...The human factors and social context are NOT someone else's business. To adopt this mindset, however, is more than an upgrade of aptitudes; it requires a change in attitudes.

These comments apply directly to the challenge currently faced by the US dams community and go to the charge identified by the IFT that it is time for "everyone involved in dam safety …[to] challenge current assumptions on what constitutes "best practice" in our industry is overdue."

SAFETY CULTURE CONSIDERATIONS

Safety Culture is a significant driver of a larger Safety Management System (SMS) to promote safety and mitigate risk in the operations of hazardous technical systems. In the United States several national regulatory agencies, (e.g. the Federal Aviation Administration and the Nuclear Regulatory Commission) have developed model SMSs and industry has largely implemented these. The ways in which the SMS is developed, implemented and adhered to can reinforce or undermine safety as an organizational priority. A safety culture that acknowledges the pressures and constraints on the system will distribute appropriate responsibilities across the organization.

Managing and ensuring the safety and integrity of our aging infrastructure is a major challenge for owner/operators and regulators. Not only is aging infrastructure a problem, but various degrees of knowledge about the current and projected integrity of our systems further challenges our ability to identify and appropriately prioritize infrastructure investments. Additionally, safety and integrity investments require gaining operator, regulatory, and public support to make the necessary investments for often costly and long-term upgrades, building new or more resilient infrastructure, and economic, environmental, and other policy and regulatory changes.

Following the catastrophic failure of the Deepwater Horizon incident in 2010, significant energy and focus has been given to the topic within the oil and gas industry. Attributes of a robust safety culture include (Figure 12) [10]:

- Leadership commitment to safety values and actions
- Respectful work environment
- Environment of raising concerns
- Effective safety and environmental communication
- Personal accountability
- Inquiring attitude
- Hazard identification and risk management

- Work processes
- Continuous improvement

BSEE's Safety Culture Policy Statement

According to BSEE, the following characteristics "typify a robust safety culture":[†]

1. ***Leadership Commitment to Safety Values and Actions.*** *Leaders demonstrate a commitment to safety and environmental stewardship in their decisions and behaviors;*
2. ***Hazard Identification and Risk Management.*** *Issues potentially impacting safety and environmental stewardship are promptly identified, fully evaluated, and promptly addressed or corrected commensurate with their significance;*
3. ***Personal Accountability.*** *All individuals take personal responsibility for process and personal safety, as well as environmental stewardship;*
4. ***Work Processes.*** *The process of planning and controlling work activities is implemented so that safety and environmental stewardship are maintained while ensuring the correct equipment for the correct work;*
5. ***Continuous Improvement.*** *Opportunities to learn about ways to ensure safety and environmental stewardship are sought out and implemented;*
6. ***Environment for Raising Concerns.*** *A work environment is maintained where personnel feel free to raise safety and environmental concerns without fear of retaliation, intimidation, harassment, or discrimination;*
7. ***Effective Safety and Environmental Communication.*** *Communications maintain a focus on safety and environmental stewardship;*
8. ***Respectful Work Environment.*** *Trust and respect permeate the organization with a focus on teamwork and collaboration; and*
9. ***Inquiring Attitude.*** *Individuals avoid complacency and continuously consider and review existing conditions and activities in order to identify discrepancies that might result in error or inappropriate action.*

[†] BSEE, *Safety Culture Policy Statement,* http://www.bsee.gov/Safety/Safety-Culture-Policy/ (accessed October 7, 2015).

Figure 12: Safety Culture Statement following 2010 Deepwater Horizon incident [10].

We can look to the High Reliability Organizations (HROs), Safety II; and Resilience Engineering domains for approaches and strategies to better recognize and embrace the time-dependent dynamics of safety culture in socio-technical systems. It should be noted that the cultural facets include both obvious and transparent and hidden and underlying, as depicted in Figure 13.

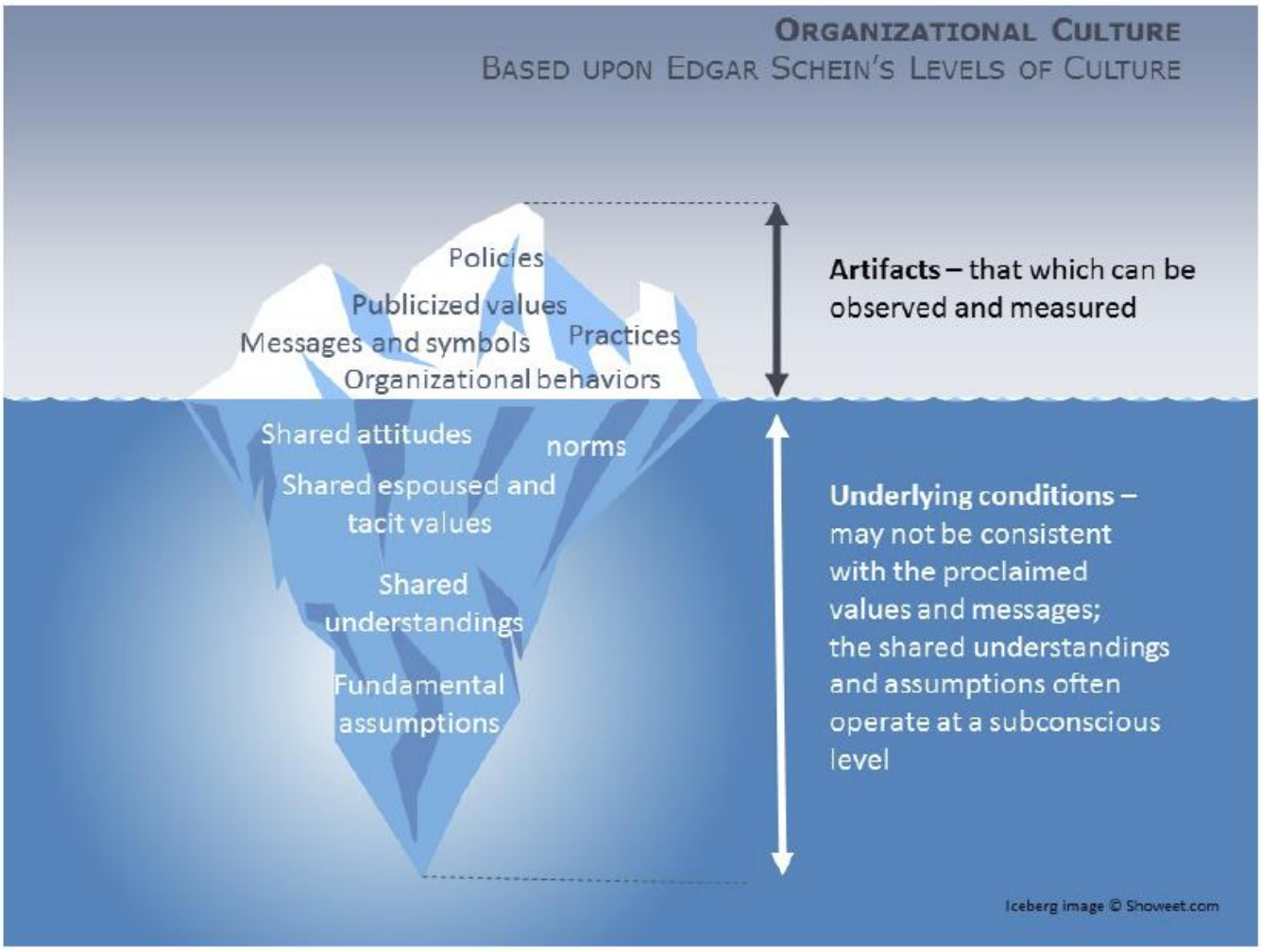


Figure 13: Visual representation of organizational culture, based on Edgar Shein's levels of culture [10].

High Reliability Organization research began in the mid-1980s and examined complex organizations that seemed to operate without failure in complex environments[3,4]. The underlying supposition of this work was that existing organizational theory concepts did not explain the processes at work in such organizations very well. The work initially focused on three organizations considered relatively exotic by critics. They were the U.S. Navy's nuclear-powered aircraft carriers, the Federal Aviation Administration's air traffic control system, and a commercial nuclear power plant.

Weick and Sutcliffe[5] identified the major components of high reliability organizations:

- Preoccupation with failure. Attention to close calls and near misses.
- Reluctance to simplify interpretations. Attention to root cause analysis.
- Sensitivity to operations. Situational awareness and carefully designed management practices.
- Commitment to resilience. Constant attention to management practices that might need to be changed.
- Deference to expertise. Listen to system experts and follow their advice.

[3] Rochlin, G. LaPorte, T., and Roberts, K. (1987) The self-designing high reliability organization. Naval War College Review, 40, 76-90.
[4] Roberts, K.H. (1990) "Managing High Reliability Organizations." California Management Review, 32, 101-113.
[5] Weick, K.E. and Sutcliffe, K. (2001) Managing the Unexpected. San Francisco: Jossey Bass.

All organizations, HRO and non-HROs, develop beliefs about the world, including susceptibility to hazards resulting in undesired outcomes. Organizations develop approaches to confront these hazards via norms, regulations, procedures, rules, guidelines, job descriptions, and training materials. During the course of operation, organizations accumulate unnoticed events that are at odds with accepted beliefs about the hazards and resulting consequences.

Unlike non-HROs, HROs develop beliefs about the world, hazards, and potential outcomes with fewer simplifications, less finality, and more process-improvement. The definition of what is 'hazardous' is continually revisited and updated. HROs tend to accumulate and more rapidly detect unnoticed smaller events that are at odds with what they expect. This gives them the ability to investigate and understand the anomalies and outline proactive responses to more rapidly restore reliable performance.

Safety II[6] is a framework presented by Erik Hollnagel, where emphasis is centered on 'humans' as a resource necessary for system flexibility and resilience. The working hypothesis is that Socio-Technical Systems are complex, which results in work situations (workflows, procedures, etc.) being underspecified, which means actual work conditions will very likely differ from what has been specified and/or described. Performance variability (the need for modifications/adjustments) by the workforce is thus not only normal and necessary, but required.

Finally, Resilience Engineering[7], is a framework that examines the ability of a system to "adjust its functioning prior to, during, or following changes and disturbances, and thereby sustain required operations under both expected and unexpected conditions." Three important terms are identified in this definition that must be underscored.

> Required operations: This term identifies the core functional outcome(s) the system is required to generate. If these outcomes are not generated, system 'failure' occurs. As mentioned previously, it is very common for these core functional outcomes to be implicit rather than explicitly defined, resulting in ambiguity across organizational divisions and personnel. The lack of specificity with respect to the core functional outcomes/required operations results in confusion within a system's organization and hinders the ability to clearly communicate the core required operations.
>
> Expected conditions: These are the anticipated operational parameters for the system and are typically delineated through a series of explicit and implicit system assumptions generated during the initial configuration of the system.
>
> Unexpected conditions: These are operational parameters that may impact a system that have not been considered or evaluated to date. Unexpected conditions also include parameters that were 'unimaginable' as well as remote scenarios that may have been originally considered, but discounted due to a perception of very low likelihood of occurrence.

There are three time-dependent qualities of resilience. First, anticipation - knowing what might be expected to occur. Second, attention – knowing what to look for. Third, response – knowing what to do and having the required resources to fully implement the response.

[6] Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management. Farnham, UK: Ashgate.
[7] Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.) (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.

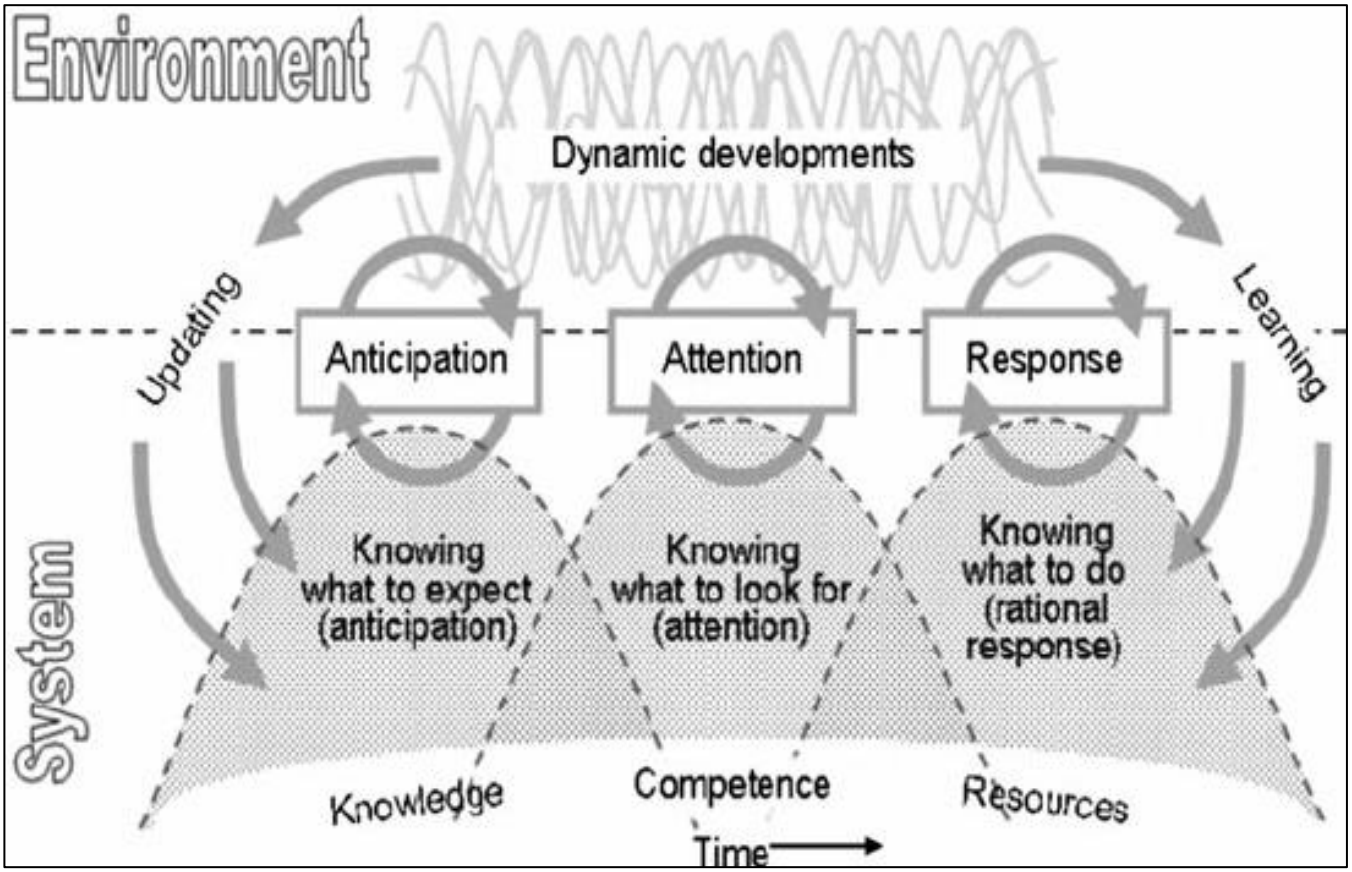


Figure 14: Resilience qualities as described by Woods and Hollnagel.

VALID AND RELIABLE

Utilization of methods to aid in management of high-hazard critical infrastructure must be valid and reliable. Following is a discussion of validity and reliability of engineering analytical methods and processes [11] [12]

Valid: *being supported by objective truth or generally accepted authority, based on flawless reasoning and solid ground, well grounded, sound, having a conclusion correctly derived from premises, cogent, convincing.*

Reliable: *suitable or fit to be relied upon, trustworthy, worthy of full confidence, dependable. Campbell and Stanley* [12] *identified approaches that can be used to establish the validity of engineering analytical methods and processes through two approaches: 1) external, and 2) internal.*

External validity *is the extent to which the method (approach) is generalizable or transferable. A method's generalizability is the degree the results of its application to a sample population can be attributed to the larger population. A method's transferability is the degree the method's results in one application can be applied in another similar application.*

Internal validity *is the basic minimum without which the method is uninterpretable. Internal validity of a method addresses the rigor with which a method is conducted - how it is designed, the care taken to conduct measurements, and decisions concerning what was and wasn't measured. There are four different types of internal validity: 1) face, 2) content, 3) criterion-related, and 4) construct.*

Face validity *is the degree to which a method appears to be appropriate for doing what it intends to do. Face validity is based on justifications provided by the state-of-art and state-of-practice knowledge and experience.*

Content validity *addresses the degree to which the method addresses the problem (issue) it is intended to address.*

Criterion validity *addresses the degree to which the method allows for assessment of an issue or problem beyond the testing situation; the generalizability of the method. Criterion validity may be concurrent or predictive; the evaluation may be either be intended to assess a criterion independently evaluated at the same time (concurrent), or to predict achieving a criterion in the future (predictive).*

Construct validity *addresses the degree to which the results of the method can be accounted for by the explanatory constructs of a sound theory. A method's construct validity can be assessed by specifying the theoretical relationships between the concepts and then examining the empirical relationships between the measures of the concepts, and then interpreting how the observed evidence clarifies the concepts being addressed. Construct validity is demonstrated when measures that are theoretically predicted to be highly interrelated are shown in practice to be highly interrelated.*

A reliable method is one that yields valid and consistent results upon repeated use*. A reliable method is suitable for its intended purposes. Reliability is established through multiple applications in prototype conditions by independent and qualified users representative of those that will use the method in practice.*

The important point made here is that methods must be applied and the outcomes of those methods compared with what 'actually happens.' While the Probabilistic Failure Mode Analysis (PFMA) method is documented and has been used by numerous individuals, the degree to which the PFMA method accurately and precisely predicts system "state" is (1) largely unknown because it is physically impossible to 'test' the predicted recurrence intervals and (2) the only 'known' likelihood of failure magnitude is 1.0 (i.e. failure has occurred). Little to no cross-checks have been documented in the scientific literature that examines the skew between anticipated failure scenarios and likelihoods with actual empirical data through back-calculation of past failures. Much work is needed in this area. For Oroville, the author is unaware of any formal back-calculation by any agency that mirrors actual events (and associated likelihoods) with the PFMA-calculated likelihood which was considered in the 2014 PFMA [13].

SUMMARY OF IFT FINDINGS

The Oroville Dam spillway incident was caused by a long-term systemic failure of the California Department of Water Resources (DWR), regulatory, and general industry practices to recognize and address inherent spillway design and construction weaknesses, poor bedrock quality, and deteriorated service spillway chute conditions.

There were many opportunities to intervene and prevent the incident, but the overall system of interconnected factors operated in a way that these opportunities were missed. Numerous human, organizational, and industry factors led to the physical factors not being recognized and properly addressed, and to the decision-making during the incident. The following are some of the key factors which are specific to DWR:

- *The dam safety culture and program within DWR, although maturing rapidly and on the right path, was still relatively immature at the time of the incident and has been too reliant on regulators and the regulatory process.*

- *Like many other large dam owners, DWR has been somewhat overconfident and complacent regarding the integrity of its civil infrastructure and has tended to emphasize shorter-term operational considerations. Combined with cost pressures, this resulted in strained internal relationships and inadequate priority for dam safety.*
- *DWR has been a somewhat insular organization, which inhibited accessing industry knowledge and developing needed technical expertise.*
- *DWR's ability to build the appropriate size, composition, and expertise of its technical staff involved in dam engineering and safety has been limited by bureaucratic constraints.*

In addition to lessons which are specific to DWR, as described in this report, the following are some of the general lessons to be learned by the broader dam safety community:

- *In order to ensure the safe management of water retention and conveyance structures, dam owners must develop and maintain mature dam safety management programs which 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 five-year reviews.*
- *Appurtenant structures associated with dams, such as spillways, outlet works, power plants, etc., 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.*

Some of these general lessons are self-evident, and have been noted by others previous to the IFT's investigation of this incident. The question is whether dam owners, regulators, and other dam safety professionals will recognize that many of these lessons are actually ***still to be*** *learned. 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.*

CNA ANALYSES AND OUTCOMES

Report Findings

The final report of the CNA process detailing the methods and findings was released on November 30, 2020.

> *To identify dam safety and operational needs associated with the facilities in the Oroville Dam Complex, the CNA project team employed the risk analysis approach. This approach consisted of each multi-disciplinary task team having workshops that used expert professional judgment to assess potential vulnerabilities of the facilities. Each task team examined potential mechanisms whereby a facility could fail, be damaged, or simply not perform as designed.* [3]
>
> *The CNA's results showed that there are no dam safety issues that exhibit a need for immediate risk-reduction actions. These results are based on the finding by the CNA project team of no unacceptable risks associated with identified potential vulnerabilities of the Oroville Dam facilities. A parallel risk study by independent experts found results in general agreement with those from the CNA.* [3]
>
> *The results of the CNA evaluations were documented in several reports that together comprise several thousand pages. These documents were submitted to both FERC and DSOD. These documents contain Critical Energy Infrastructure Information and, by federal regulation, cannot be released to the public due to homeland security concerns. This report was prepared for distribution to the public to provide a complete summary of the CNA evaluations conducted, the results of the evaluations, and the findings and recommendations prepared by the CNA project team.* [3]
>
> *Though no unacceptable risks were found, and therefore no immediate actions need to be taken, DWR concluded that there were potential vulnerabilities identified that require further consideration and examination to better estimate their actual risk. In addition, the CNA developed potential risk reduction measures for consideration to potentially reduce risks to even lower levels, and recommended implementation of these measures if they are found to be reasonably practicable. To be reasonably practicable, a risk reduction measure must be capable of being implemented and to be cost effective – that is, the cost of implementation must not be disproportionately large compared to the benefits obtained.* [3]

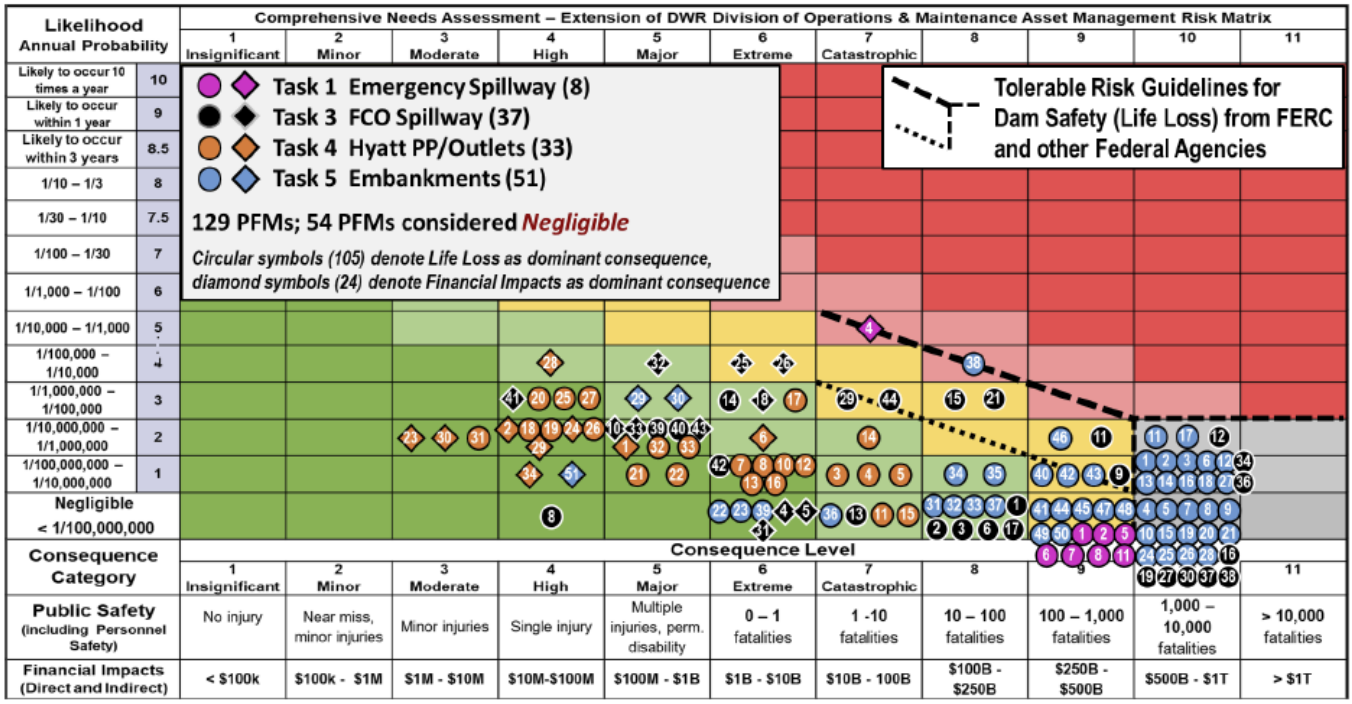
Recommended "Early Implementation Projects" that would be completed within a year or so included [3]:

- *Installation of 13 new piezometers in Oroville Dam to improve seepage monitoring (status: eight piezometer installations currently completed; awaiting regulatory approval for remaining five piezometers).*
- *Installation of four new piezometers in the rock foundation of the FCO headworks structure to monitor water pressures acting on the structure (status: installations completed).*
- *Completion of a new state-of-the art seismic stability analysis of Oroville Dam to update past evaluations on the potential performance of the dam during strong earthquake shaking (status: program and detailed scope are being developed).*

"Interim Implementation Projects" to be completed in the near term (3 to 5 years) consisted of [3]:

- *Raise Parish Camp Saddle Dam by 3 feet to reduce the risk of flood waters overtopping and breaching the dame.*
- *Line Palermo Canal to reduce seepage into the rock slope above Hyatt Powerplant and switchyard and improve stability of the rock slope. This would help reduce the likelihood of a landslide occurring in this area that would impact the switchyard and Area Control Center (ACC) for the Hyatt Powerplant.*
- *Install new remote starter and power connections to the FCO radial gates to improve their reliability. This provides another redundant power supply to operate the radial gates during a flood event, and allows operators to raise the gates locally at the FCO headworks without relying upon either external power or control communication lines.*

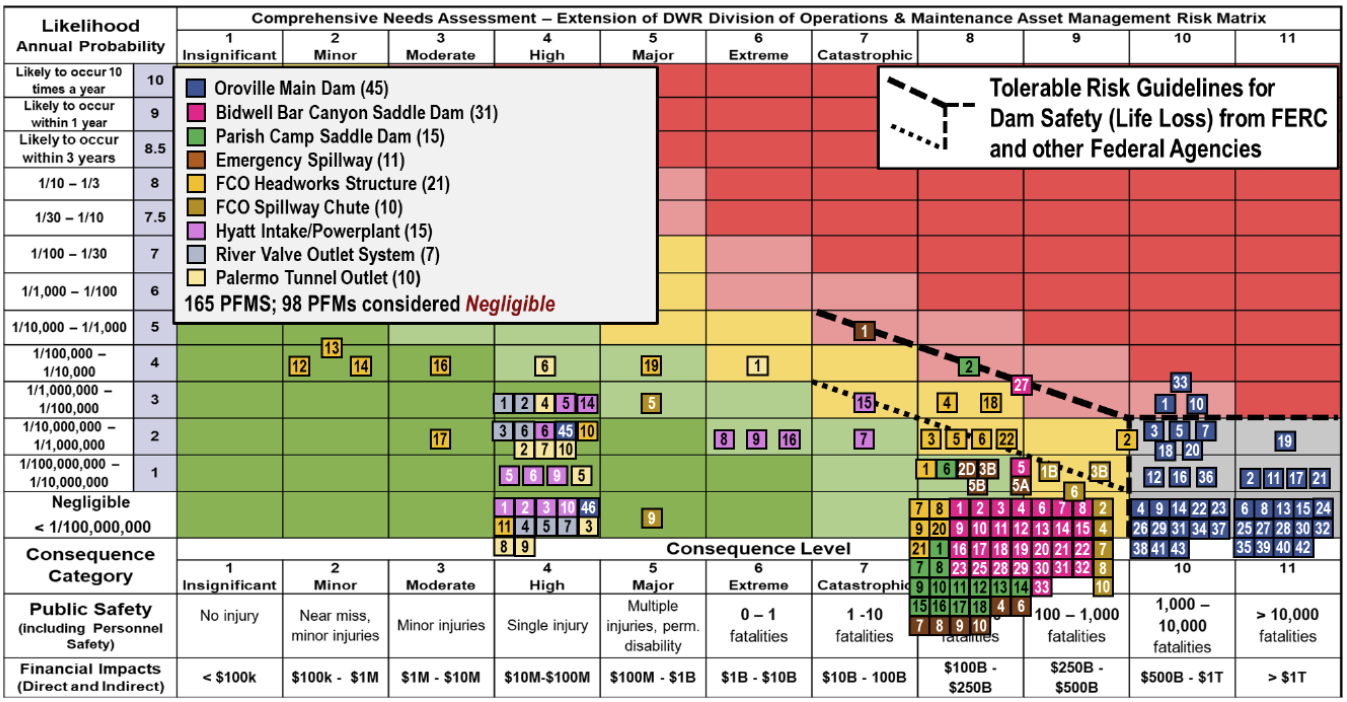
Figure 16. Risk Estimates for Critical CNA PFM Scenarios Plotted on CNA Risk Matrix



Note: the number inside each circle and diamond represents the identification number for that PFM. For example, the number 17 in the orange circle represents PFM number T4-17.

Figure 15: Risk plot showing risk estimates for CNA PFM Scenarios [3].

Figure 17. L2RA Existing Condition PFM Risk Estimates for Life-loss Plotted on the CNA Risk Matrix



Note: the number inside each square represents the identification number for that L2RA PFM. For example, the number 33 in the blue square represents L2RA PFM number ORO-33.

Figure 16: Risk plot showing risk estimates based on the Level 2 FERC risk analysis [3].

Table 5. Distribution of Most Critical CNA PFM Scenario Risk Estimates for Existing Conditions on the CNA Risk Matrix

Color/zone on the CNA risk matrix	Emergency spillway PFMs	FCO PFMs	Outlet PFMs	Embankment dam PFMs	Total PFMs
Upper red	0	0	0	0	0
Lower red	1	0	0	1	2
Amber	7	8	0	11	26
Gray	0	9	0	26	35
Upper green	0	9	9	9	27
Lower green	0	11	24	14	39
Total	8	37	33	51	129
Above PFMs plotting below the matrix: "*Negligible Risk*" – Annual Probability of Failure < 10^{-8}	7	16	2	29	54

Figure 17: Reported summary of scenarios by dam region [3].

Comments on the DWR CNA Report

Firstly, and most importantly, the completed CNA report is not 'comprehensive' with regards to the scope of the examination that needs to be completed to responsibly address the 'safety and reliability' of the Oroville Dam Complex. The Ad Hoc Committee immediately commented on the misrepresentation and suggested an alternative label. The IRB concurred with the Ad Hoc Committee (see Figure 18), but DWR continued to use the term "Comprehensive," which the Ad Hoc Committee continues to assert misleads the public on the depth and rigor of the evaluation. It is appreciated that the public has the ability to review the report and conclude for themselves what content is/is not addressed, but a general public individual likely does not have the technical background to ferret out the difference between 'comprehensive' and non-comprehensive.

Table 1: SUMMARY OF AD HOC COMMITTEE MEETING NO. 1 COMMENTS

Comment No.	Comment	Significance	IRB Comments
1	The use of the term "Comprehensive Needs Assessment" implies a more thorough examination of needs than currently proposed via the identified six (6) tasks and may be interpreted by the public as misleading.	Medium/ High	The IRB agrees that the title of the study (taken alone) could lead many stakeholders to expect a more expansive scope than currently envisioned. Expectations surrounding a "Comprehensive Needs Assessment" will vary widely according to the perspective of the reader of the final report. A significant risk in not addressing the comment would be the ability for detractors to discount or dismiss the study as not being comprehensive. This comment is closely related to IRB recommendation M1-22. It would seem that recommendation 1c from the Ad Hoc committee would be a reasonable approach to addressing this concern. The introduction of the final report could define the scope of the CNA effort, and it could identify other items not addressed in the scope of the CNA along with how those issues are being addressed by DWR. To implement recommendation 1a of the Ad Hoc Committee, consider renaming the study "Facility Needs Assessment". This would eliminate potential criticism surrounding the term "comprehensive" and would help focus expectations that the study is mainly about assessing the physical features of the facility and not the human or organizational factors within DWR or the operation of the facility. DWR may also consider providing the Ad Hoc Committee a briefing on some of the other efforts that DWR has completed and continues to undertake to address other issues of concern to the Ad Hoc Committee such as site security, terrorism, etc.

Figure 18: Concurrence by the IRB that the use of the term "Comprehensive" may mislead the public.

The CNA summary report noted that the documents contained "Critical Energy Infrastructure Information" (CEII), which is not information that is available to the public. The CNA summary report does not provide any means by which to independently verify the assumptions used in the calculations nor the reasonableness of parameters. There is no communication of uncertainties associated with the anticipated likelihood of failure or the consequences of failure. It is, from the public's standpoint, a black box. The public is forced to 'trust' the work by DWR and its consultants without the benefit of any checks or audits.

It should be noted that FERC does provide guidance on preparing Comprehensive Assessments (Figure 19) as part of the Part12D reporting [14]. This list includes a number of items that were not considered as part of DWR's "Comprehensive Needs Assessment." One substantial omitted item was "Review and evaluation of dam and public safety programs." Two evacuations have been executed at Oroville Dam, yet no evaluation of the effectiveness or required enhancements to achieve the intended evacuation effectiveness (i.e. durations, number of people).

Also, of note, FERC identifies limitations of the Level 2 Risk Analysis and explicitly states that these types of risk analyses are insufficient to determine if existing dam safety risks are tolerable (Figure 20). FERC states that "Higher level risk analyses (typically Level 3 and Level 4 risk analyses) will be required to demonstrate risk tolerability" [14].

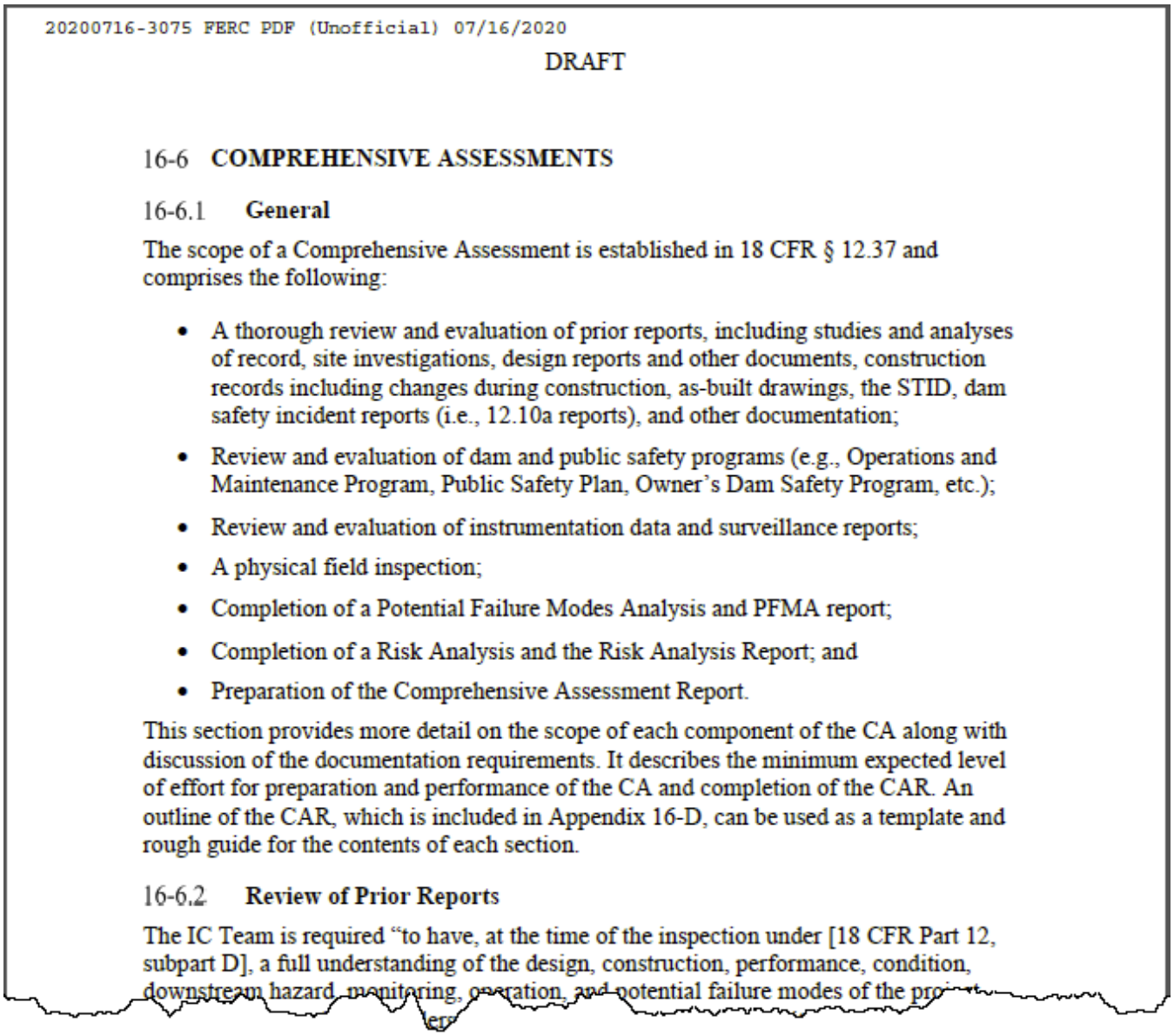
Finally, the selected 'acceptable risk' thresholds used by DWR were not developed in conjunction with the community. The risk thresholds were unilaterally imposed on the community without the benefit of a structured discussion or any form of informed consent.

Guidance on the assumptions for establishing "tolerable risk" is presented in the U.S. Army Corps of Engineers (USACE) manual on "Engineering and Design, Safety of Dams – Policy and Procedures" [15]. These assumptions/requirements include (Figure 21 and Figure 22):

- Risks that society is willing to live with so as to secure certain benefits
- Risks that society does not regard as negligible or something it might ignore
- Risks that society is confident are being managed by the owner
- Risks that the owner keeps under review and reduces still further if and as practicable

If we account for the nuances associated with Oroville Dam and apply an adjustment factor of say two-orders of magnitude (which is likely conservative) to the "tolerable risk" threshold to acknowledge mistrust and past erroneous and incorrect 'likelihood of failure' determinations, we may find that many failure scenarios DWR 'believes' to be acceptable are in fact 'unacceptable.' Layered on this are the many uncertainties that are included in the PFMA scenarios that are not carried forward and communicated. The 'confidence' of the risk plot position can be graphically portrayed on these risk plots to give the audience some sense of uncertainty and confidence about the estimate. As currently depicted, all scenarios are shown to have the same 'certainty.' This most certainly is not the case.

Figure 23 shows a conceptual example of how the calculated risk positions for the various failure scenarios plot relative to an adjusted 'acceptable risk' threshold that has been lowered by two-orders of magnitude. The calculated positions do not change, just the threshold with regards to what is ok and what is not ok. What we see from this hypothetical example is that our system goes from largely 'acceptable,' to largely 'unacceptable,' with numerous scenarios falling outside the acceptable threshold. Appropriate and responsible development of these thresholds is required if they are to be used as part of decision-making where the lives of tens of thousands to hundreds of thousands of individuals are at stake.



20200716-3075 FERC PDF (Unofficial) 07/16/2020

DRAFT

16-6 COMPREHENSIVE ASSESSMENTS

16-6.1 General

The scope of a Comprehensive Assessment is established in 18 CFR § 12.37 and comprises the following:

- A thorough review and evaluation of prior reports, including studies and analyses of record, site investigations, design reports and other documents, construction records including changes during construction, as-built drawings, the STID, dam safety incident reports (i.e., 12.10a reports), and other documentation;
- Review and evaluation of dam and public safety programs (e.g., Operations and Maintenance Program, Public Safety Plan, Owner's Dam Safety Program, etc.);
- Review and evaluation of instrumentation data and surveillance reports;
- A physical field inspection;
- Completion of a Potential Failure Modes Analysis and PFMA report;
- Completion of a Risk Analysis and the Risk Analysis Report; and
- Preparation of the Comprehensive Assessment Report.

This section provides more detail on the scope of each component of the CA along with discussion of the documentation requirements. It describes the minimum expected level of effort for preparation and performance of the CA and completion of the CAR. An outline of the CAR, which is included in Appendix 16-D, can be used as a template and rough guide for the contents of each section.

16-6.2 Review of Prior Reports

The IC Team is required "to have, at the time of the inspection under [18 CFR Part 12, subpart D], a full understanding of the design, construction, performance, condition, downstream hazard, monitoring, operation, and potential failure modes of the pro-

Figure 19: FERC guidance on 'comprehensive assessments' [14].

Additional information on RIDM and how Level 2 risk analyses fit into the overall risk management framework in FERC's dam safety program is included in Risk-Informed Decision Making Risk Guidelines (FERC, 2016), available at:

http://www.ferc.gov/industries/hydropower/safety/guidelines/ridm.asp

18-1.4 Limitations

For all the benefits provided by a Level 2 risk analysis, typically the results will not be suitable for determining if the existing dam safety risks are tolerable. Higher level risk analyses (typically Level 3 and Level 4 risk analyses) will be required to demonstrate risk tolerability. More information on Level 3 and 4 risk analyses is provided in Chapter 2 of the FERC Risk-Informed Decision Making Risk Guidelines (FERC, 2016).

This document describes the process and procedures for performing a Level 2 risk analysis. This document does not present information on risk analysis methodology. Risk analysis methodology references are included in Best Practices for Dam and Levee Safety Risk Analysis (BOR/USACE, 2018).

18-3

Figure 20: FERC direction related to concluding risks are tolerable or not [14].

ER 1110-2-1156
31 Mar 14

CHAPTER 5

Tolerable Risk Guidelines

5.1 Introduction.

5.1.1 Role of Tolerable Risk Guidelines in Risk Assessment and Risk Management. Tolerable risk guidelines are used in risk management to guide the process of examining and judging the significance of estimated risks obtained using risk assessment. The outcomes of risk assessment are inputs, along with other considerations, to the risk management decision process. Tolerable risk guidelines should not be used alone to prescribe decisions on "How safe is safe enough?" Meeting or achieving the tolerable risk guidelines is the goal for all risk reduction measures, including permanent and interim measures. The available options for IRRM may be limited by time, available funding, and potential negative effects on public health and safety due to the IRRM. The loss of project benefits should not override the need to reduce life safety risk.

5.1.2 Development of Tolerable Risk Guidelines USACE. USACE is working with the Bureau of Reclamation (USBR) and the Federal Energy Regulatory Commission (FERC), to craft common risk management guidelines. Reclamation had been using "Guidelines for Achieving Public Protection in Dam Safety Decision Making" (reference A.111), which were originally issued as interim guidance in 1997 and subsequently in final form in 2003. USBR revised the 2003 guideline and issued an interim document in August 2011 titled, "Interim Dam Safety Public Protection Guidelines - A Risk Framework to Support Dam Safety Decision-Making" (reference A.112). Guidelines are also being used in other countries, such as the Australian National Committee on Large Dams (ANCOLD) - Guidelines on Risk Assessment (2003) (reference A.130). Although these guidelines have some fundamental common characteristics, there are some subtle and important differences.

5.1.3 Continued Development of Guidelines. As USACE works with Reclamation and FERC to achieve a common risk management framework and guidelines, USACE will use an adaptation of the 2011 Reclamation public protection guidelines, the risk evaluation guidelines published by Australian National Committee On Larger Dams (ANCOLD) in 2003 (reference A.130) and some adaptations of the ANCOLD guidance implemented by the New South Wales Government Dam Safety Committee (NSW DSC) Risk Management Policy Framework for Dam Safety, 2006 (reference A.147).

5.2 Background on Tolerable Risk Guidelines.

5.2.1 Definition of Tolerable Risk. Tolerable risks are:

5.2.1.1 Risks that society is willing to live with so as to secure certain benefits;

5.2.1.2 Risks that society does not regard as negligible or something it might ignore (i.e. the risk is not considered a broadly acceptable risk - see definition below);

5-1

Figure 21: Excerpt from USACE Dam Safety manual that describes assumptions associated with "Tolerable Risk" [15].

ER 1110-2-1156
31 Mar 14

5.2.1.3 Risks that society is confident are being properly managed by the owner; and

5.2.1.4 Risks that the owner keeps under review and reduces still further if and as practicable (Adapted from HSE, 2001 reference A.146).

5.2.2 Definition of Broadly Acceptable Risk. "Broadly acceptable risk" is contrasted with tolerable risk. "Risks falling into this (broadly acceptable risk) region are generally regarded as insignificant and adequately controlled. The levels of risk characterising this region are comparable to those that people regard as insignificant or trivial in their daily lives. They are typical of the risk from activities that are inherently not very hazardous or from hazardous activities that can be, and are, readily controlled to produce very low risks" (HSE, 2001 reference A.146). By the nature of the hazard that USACE dams pose it is inappropriate to attempt to manage them as posing a broadly acceptable risk and therefore the concept of the broadly acceptable risk level or limit does not apply to USACE dams.

5.2.3 Definition of Tolerable Risk Range. Figure 5.1 shows how in general tolerable risk is a range between unacceptable, where the risk cannot be justified except in exceptional circumstances, and broadly acceptable, where the risk is regarded as negligible (Adapted from HSE, 2001 reference A.146). This figure illustrates the point at which the incremental risk for a specific dam is tolerable within the general range of tolerability as defined by the definition in 5.2.1 and the incremental risk being reduced as informed by the as-low-as-reasonably-practicable (ALARP) considerations.

5.2.4 Equity and Efficiency.

5.2.4.1 Two fundamental principles, from which tolerable risk guidelines are derived, are described as follows in ICOLD, 2005 (reference A.143):

5.2.4.1.1 Equity. The right of individuals and society to be protected, and the right that the interests of all are treated with fairness, with the goal of placing all members of society on an essentially equal footing in terms of levels of risk that they face. (See Section 2.2.4.3 for additional definition.)

5.2.4.1.2 Efficiency. Efficiency is the need for society to distribute and us e available resources so as to achieve the greatest benefit. (See Section 2.2.4.4 for additional definition.)

5.2.4.2 The Conflict between Equity and Efficiency. There can be conflict in achieving equity and efficiency. Achieving equity justifies the establishment of maximum tolerable risk limits for individual and societal risk. Efficiency is defined by the risk level where

5-2

Figure 22: Excerpt from USACE Dam Safety manual that describes assumptions associated with "Tolerable Risk" [10].

Figure 23 presents a conceptual example of delineation 'tolerable risk' thresholds based on context-specific adjustments, rather than blindly using very generic thresholds across infrastructure domains. The lack of trust of the community to the dam owner/operator to "get it right" requires more 'safety' by lowering the line between 'acceptable' and 'unacceptable' risk positions.

Also shown in Figure 23 is the inclusion of uncertainty about the estimated risk position. There is uncertainty both in the likelihood of failure (y-axis) as well as the magnitude of consequences (x-axis). Confidence intervals should be communicated for all of the scenarios as many of them likely have uncertainty magnitudes that plot into 'unacceptable' regions, whereas the 'best guess' may plot right on, or slightly below, the 'acceptable'/'unacceptable' threshold.

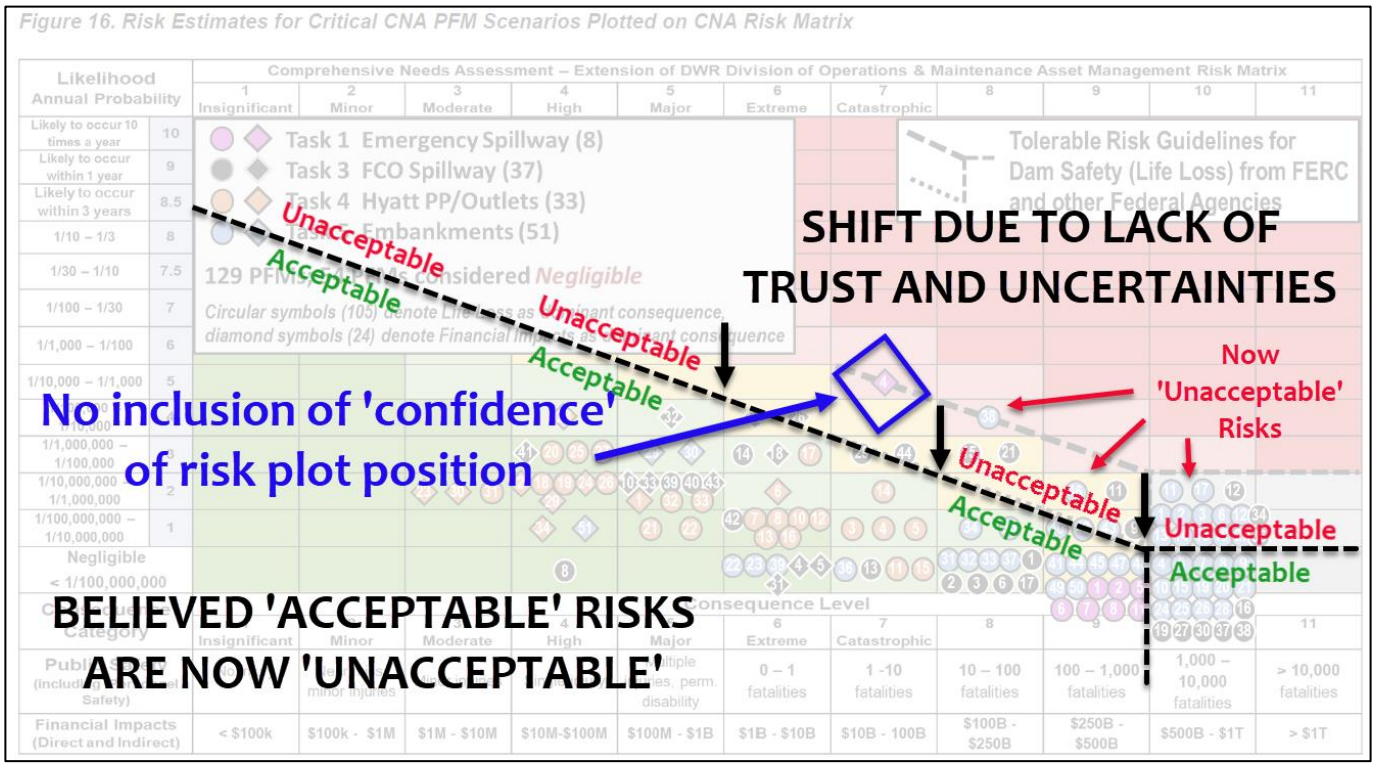


Figure 23: A conceptual example of updating "tolerable risk" threshold to account for Oroville-specific context as well as confidence intervals for the uncertainties associated with the estimated 'likelihood of failure' and 'consequences of failure.'

Figure 24 shows a cartoon that graphically illustrates the challenge associated with subjective risk-based methods that allow 'potential' issues to linger. First, there is some recognition or perception of a potential 'risk.' In the case of the cartoon, we have a boulder that may or may not fall onto the two individuals at the base of the hill. There is deliberation between the individuals as to the 'likelihood' that the boulder will actually fall on them. Meanwhile, and quite separate from the outcomes of their deliberations, the boulder starts to move and the parties evacuate the area, which then is referred to as "risk management." Having the situation require action vs. proactive measures implemented before action is required is preferred because it is 'safe' for the decision-maker…there was no question, action was required.

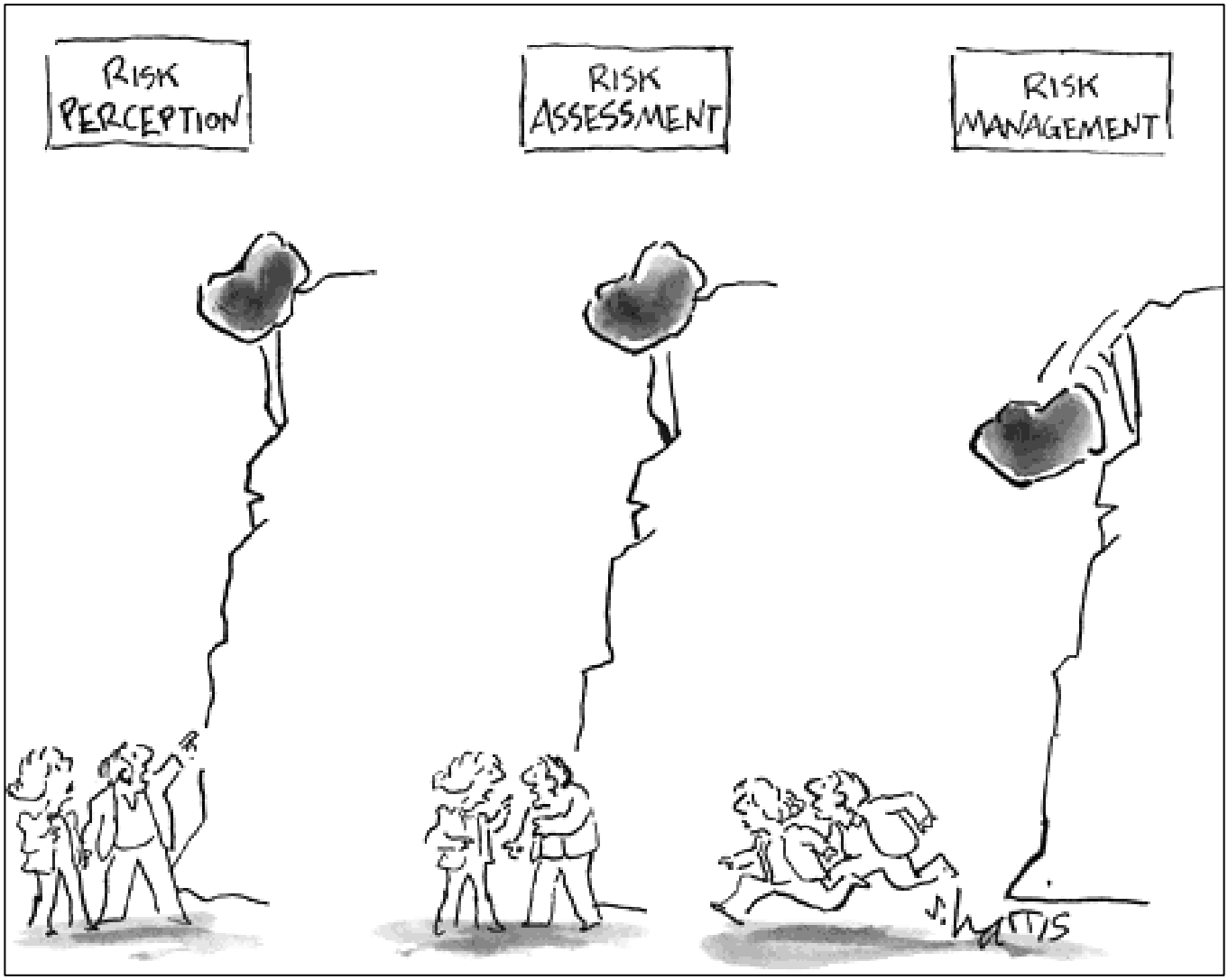


Figure 24: Cartoon by S. Hattis illustrating risk perception, risk assessment, and risk management. From: http://www.sciencecartoonsplus.com/

Further compounding the subjective challenge of conventional risk analyses are cognitive constraints related to rare events. Cognitively, humans, even Subject Matter Expert humans, have a hard time distinguishing rare events that occur less frequently than about the 100-year event. Research by Fischoff et al [16], shown in Figure 25, reveals that individuals have a hard time distinguishing between a 100-year event and the 1,000-year or 10,000-year, or 100,000-year events. These events with less than a 100-year frequency are essentially perceived to be equally 'un'likely.

Thus, we have probable events that occur up to a recurrence interval of 1 in 100 years. We then have possible events, which occur less frequently than 1 in 100 years. We should approach possible events with much more scrutiny than probable events due to the overconfidence bias phenomenon. This situation arises in conventional risk analyses where multiple multiplications result in the calculated likelihood values of 10 to the -6, -7, -8, and smaller.

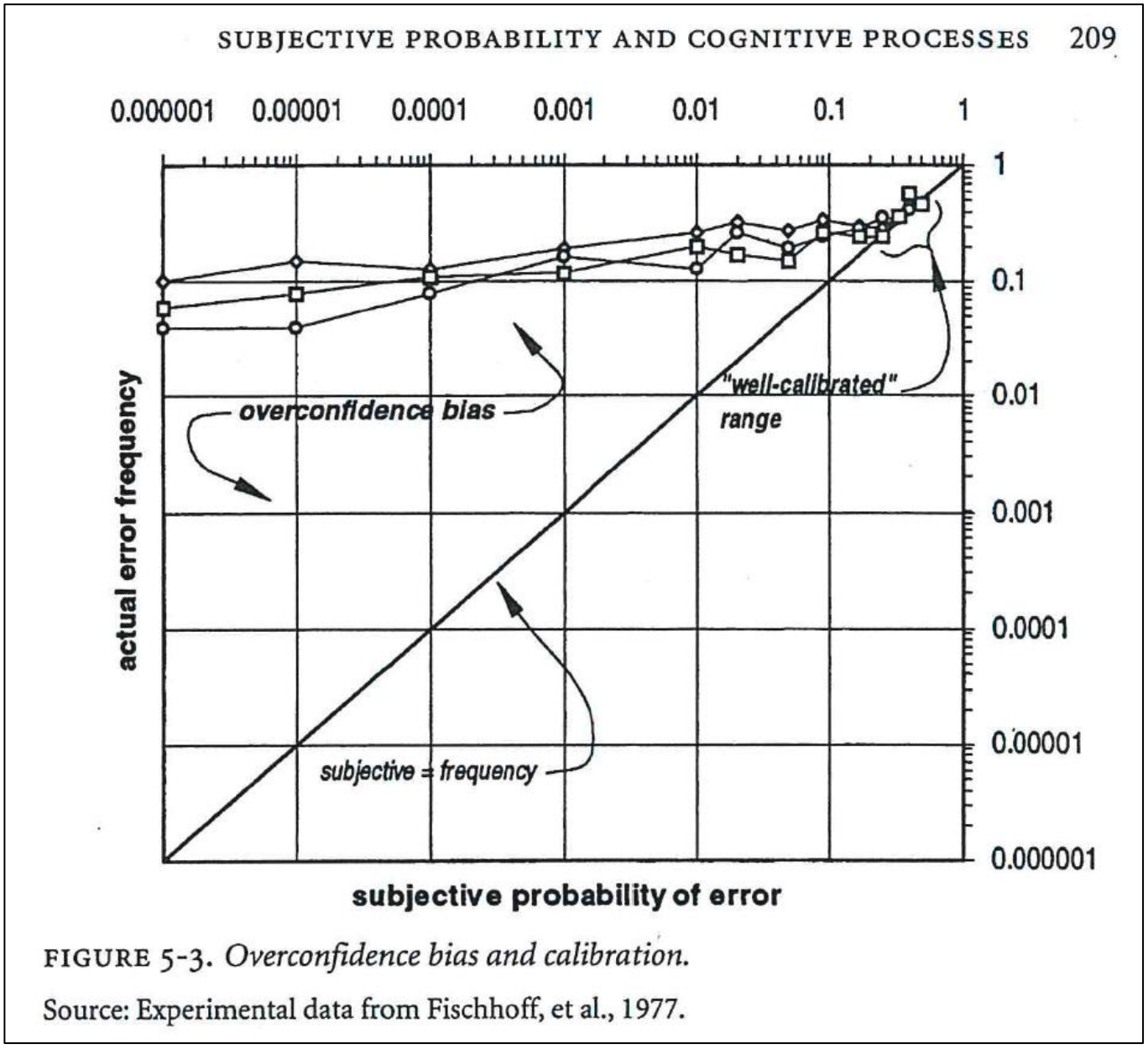


Figure 25: Overconfidence bias for very rare events.

Analogies or stories are another mode of past occurrences that influences the 'belief' in the likelihood that something may or may not happen. If something has happened in your lifetime, your parents' lifetime, or grandparents' lifetimes, one tends to deem that more probable than had that event not occurred, which makes sense. It is essentially empirically-based. However, when we are talking about innovation and new and emerging technologies, no such empirical history exists and 'belief' is constrained to individual imagination.

At some point, an event is deemed 'too remote' and is not actively addressed. It is omitted. While this is ok, there should be a formal delineation of events considered and events not considered as this enables future managers to clearly understand what is 'anticipated' vs 'unanticipated' operational situations.

If we apply a conceptual adjustment factor to the results of the CNA risk plot that accounts for the 'overconfidence bias' (as shown in Figure 26), we find risks that were anticipated to be 'acceptable,' may very well be 'unacceptable'

and more 'likely,' resulting in unanticipated number of "unacceptable' scenarios than hoped for. Due to the inherent challenge of these risk-based methods, there is no pragmatic way one can 'double check' that the risk plot position calculated is fully representative of the actual system state. One must 'hope' that the answer has been calculated correct. Reliance on a technique that cannot be independently substantiated is not a sound approach to ensure high-levels of safety and reliability for high-hazard critical infrastructure systems.

This conceptual example that examines 'what happens' if the estimated risk positions are incorrect illustrates that 'problems' can quickly 'pile up' for the unprepared organization. If the phenomenon illustrated in Figure 26 were to occur, would the organization have the Resilience to (a) know what to expect (i.e., is the organization mindful of the potential occurrence of a large number of 'unacceptable' scenarios); (b) know what to look for (i.e., measurable monitoring metrics and leading indicators that enables an organization to proactively identify); and (c) know what to do (i.e., having resources available and appropriately deploying to mitigate and reduce the 'unacceptable' risk down to 'acceptable' limits).

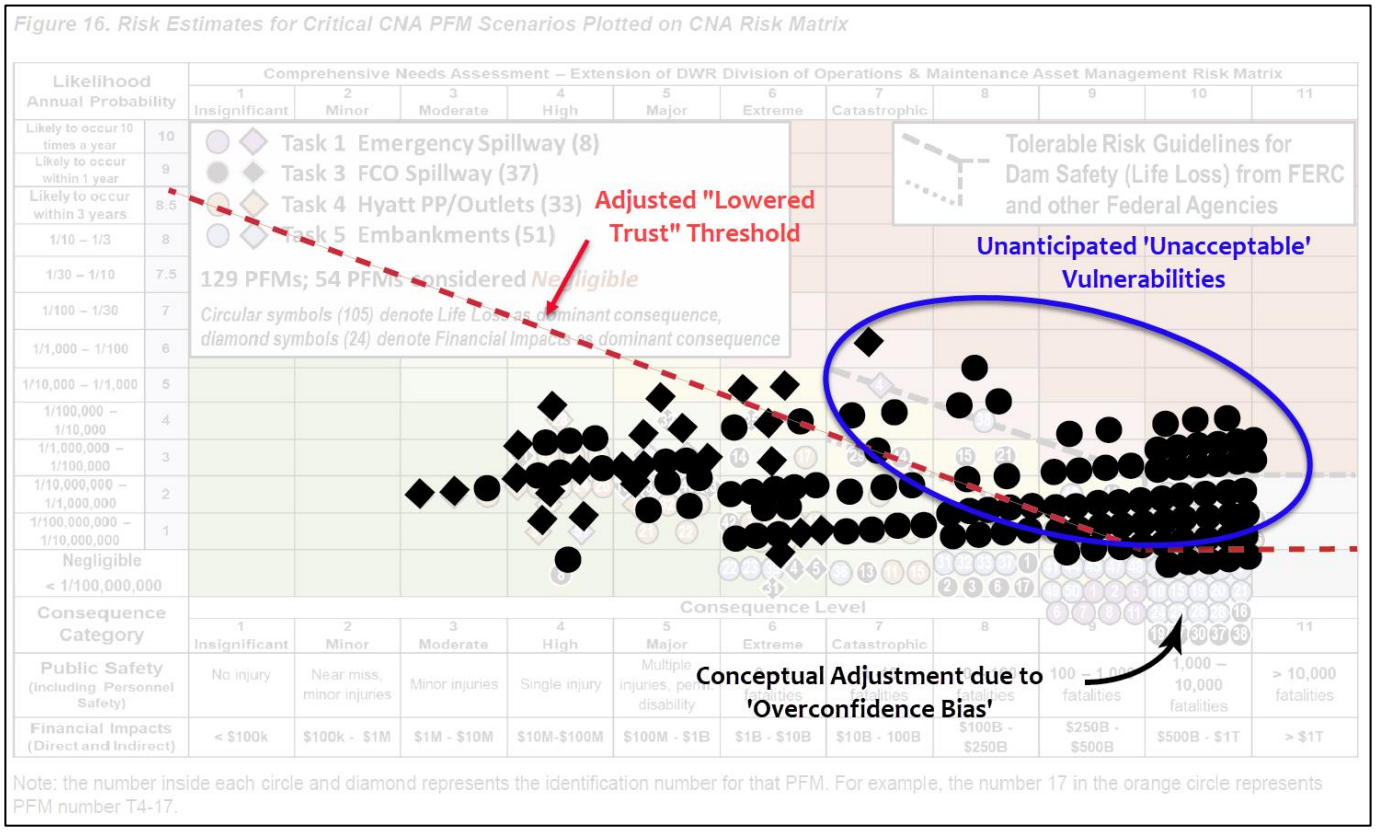


Figure 26: Conceptual risk plot accounting for degraded 'trust' and overconfidence bias, resulting in significantly greater vulnerability than 'hoped for.'

INCORPORATION OF IFT "LESSONS TO BE LEARNED"

A discussion is presented that reflects on the updates and modifications incorporated into DWR's "Comprehensive Needs Assessment" relative to the recommendations made by the IFT. It should be noted that some of the IFT recommendations were targeted directly to DWR, while others were aimed at the larger dam industry. Also, some IFT recommendations may not be wholly applicable to the DWR's "Comprehensive Needs Assessment." In such instances, it has been so noted.

Industry-Level Lessons to be Learned for US Dam Safety Practice

The IFT presented some lessons that they felt applied not just to DWR, but to the industry as a whole. These lessons have been included because they also apply to DWR.

Physical Inspections

OVERALL COMMENT: NOT APPLICABLE TO CNA INITIATIVE

The IFT noted that physical inspection, in themselves, are not necessarily impactful at identifying latent issues. As reported in the CNA report, physical inspections were not a substantial element of the evaluation and it is unclear if any targeted physical inspections were performed during the course of the CNA work.

Comprehensive Facility Reviews

OVERALL COMMENT: APPLICABLE TO CNA - LESSON NOT FULLY IMPLEMENTED

The IFT noted that 'Comprehensive Facility Reviews' consist of the following [1]:

> *Periodic comprehensive reviews of original design and construction, performance, maintenance, and repairs are needed for all features of dam projects. These reviews should compare the various features of the project with the current state of practice to answer the following questions:*
>
> - *Is the feature consistent with current design and construction practice?*
> - *If there are variations from current practice, do they compromise the structure and present a risk of failure or unsatisfactory performance?*
> - *If there is not enough information available to make those judgments, is the potential risk sufficient to justify further study or evaluation?*

The CNA completed by DWR did not satisfy these criteria, thus the CNA cannot be considered a 'Comprehensive Facility Review," as recommended by the IFT. No documentation has been provided to date that substantiates DWR has completed a "Comprehensive Facility Review" as recommended by the IFT.

Regulatory Compliance

OVERALL COMMENT: APPLICABLE TO CNA - LESSON POTENTIALLY REPEATED

The IFT noted that [1]:

> *Compliance with regulatory requirements is not sufficient to manage dam owners' and public risk.*

In general, it must be recognized that regulators have an essential role in management of dam safety, but do not have the resources nor the primary responsibility for managing dam safety. That responsibility, both legally and ethically, rests with dam owners.

In conducting the CNA and related Level 2 Risk Analysis (L2RA), DWR fully and solely relied on regulatory compliance and the associated evaluation protocols. There is no regulatory constraint that precludes DWR from performing additional analyses (such as best practices from other high-hazard industries). Extending beyond the minimum required by regulators and exploring additional techniques to substantiate that the intended level of safety and reliability is actually being realized is critical to responsible safety and reliability management. Use of triangulation (comparing the outcomes of multiple independent analysis methods) is an extremely effective means to identify analytic bias and converge upon a representative understanding of safety and reliability. Use of a single method/technique, regardless of the number of times or different 'teams,' that single exercise fails to detect inherent bias.

To illustrate this concept, Johari's Window is used. The Johari Window is a technique that shows and helps people/organizations better understand their relationship with themselves and others. It was created by psychologists Joseph Luft and Harrington Ingham in the mid-1950s. There are two columns and two rows (a 2x2 matrix). The left column are things known to the 'self'. These are thing the individual/organization are directly aware of. The right column are things not known by the individual/organization but known by others. This includes 'best practices' in other industries. The table has two rows. The top row are things known to others and the bottom row are things not known to others.

Figure 27 shows a Johari Window with respect to various management approaches one could take, for example, to ensure maximum safety and reliability of US dams. As outlined in the FERC engineering manual, the primary management approach consists of risk-based methods (PFMAs and RIDM). This approach is shown in the "known to self" column and "known to others" row. There are other 'best practices' techniques used in other industries (such as reliability-centered maintenance, Total Quality Management, and Life-Cycle management) that enhance safety and reliability, but are not currently included part of the U.S. Dams 'best practices.'

Consistent with the IFT recommendations, this report strongly encourages review of the large portfolio of existing 'best practices' in other industries to aid in triangulating and 'convincing ourselves' that the intended level of safety and reliability in our dams is actually being achieved. Utilization of multiple models and multiple techniques to cross-check (i.e. triangulation) is a very effective means to ferret out 'groupthink' and inherent skew between intended level of safety and reliability and the actual level of safety and reliability.

Figure 28 presents the intended outcome of the recommendations in this report; augment and enhance the current practices within U.S. Dams to bolster the actual level of safety and reliability of these aging infrastructures. It is impossible for any one individual or group of external experts to 'know' the actual system state of the dam based on periodic 'reviews' of limited system data. Use of a wide-ranging portfolio of management techniques that are continually in practice, is utilized by High Reliability Organizations. U.S. Dams should be High Reliability Organizations.

	Known to self (i.e. US Dams)	Not known to self (i.e. US Dams)
Known to others	PFMA/RIDM	PFMA/RIDM Triangulation Leading Indicators Reliability-Centered Maintenance Resilience Engineering High Reliability Organizations Life-Cycle Management Total Quality Management Crisis Management Preparedness
Not known to others	Detailed design calculations Design assumptions Performance characteristics	"Surprises" New Technologies

Figure 27: Use of Johari Window to illustrate known techniques but not currently accounted for in dams 'best practice.'

	Known to self	Not known to self
Known to others	PFMA/RIDM Triangulation Leading Indicators Reliability-Centered Maintenance Resilience Engineering High Reliability Organizations Life-Cycle Management Total Quality Management Crisis Management Preparedness	PFMA/RIDM Triangulation Reliability-Centered Maintenance Resilience Engineering High Reliability Organizations Life-Cycle Management Total Quality Management Crisis Management Preparedness
Not known to others	Detailed design calculations Design assumptions Performance characteristics	"Surprises" New Technologies

Figure 28: Augmenting the current US Dams risk management practices to bolster safety and reliability by leveraging 'best practices' by other industries.

Potential Failure Mode Analyses (PFMAs)

OVERALL COMMENT: APPLICABLE TO CNA - LESSON NOT FULLY IMPLEMENTED

The IFT noted that:

> *In general, although a very useful tool, which is likely quite adequate for a majority of dams, the current PFMA process can have difficulties in properly characterizing risks for large or complex systems, including accounting for human and operational aspects in failures. By defining failure modes as a linear chain of events, there can be a tendency to oversimplify complex failure modes involving multiple interactions of system components. Knowledge of the full range of dam safety risks resulting from all operational aspects is required for an organization's managers to decide on appropriate actions to manage those risks.*

For this effort, the Department has elected to utilize a "new for them" method referred to as "risk-informed" analysis and decision making. Having worked extensively in this area and across many different infrastructure types, I wanted to quickly point out some challenges with this approach.

The first challenge that must be acknowledged is that these annual likelihoods of occurrences do not preclude an event from happening in any given year. In fact, it is conceivable that any of these events could possibly happen twice or more in any given year. This annual likelihood of occurrence is based on a long-term perspective, say across hundreds of years. Therefore, the concept of risk as used in risk analysis and risk management cannot be a foundational framework for managing for safety and high reliability. As an analogy, right now, California has and is experiencing some catastrophic wildfires. Firefighters talk about "Career Fires." These are large fires one would see once in their career. We are now hearing reports that firefighters are seeing multiple 'career fires' and sometimes even multiple 'career fires' in the same year.

The second challenge is that it is near impossible to independently verify the risk position estimates. The far majority of these evaluations rely on subjective interpretations rather than verifiable facts. This means you have to 'trust' the analyst. There are many problems with this, but one problem that is not easily overcome is the lack of information and the need to make basic assumptions. For example, the Center for Catastrophic Risk Management investigated the 2010 Deepwater Horizon incident. I personally reviewed the risk register and associated risk analysis for the blowout preventer. One could argue that the assumptions made in the original evaluation were reasonable. However, there were a series of unconsidered factors that unfolded during the actual event. These unconsidered factors were never accounted for, never made the risk register, and thus were never recognized as potential failure mode scenarios.

Lastly, and piggy backing off the last point, these identified scenarios are just a sub-set of the full portfolio of failure scenarios that exist in reality. I will make the argument that the "risk-informed" approach is useful, but even more useful are the sets of assumptions by which the evaluations were completed. We need to inventory those and vigilantly monitor actual system performance and hazards to ensure we are not deviating outside the limits of those assumptions. If we do, we'll have problems. My concern here is the focus on these identified scenarios, which may or may not be correct, but little to no focus on what I will call "uncaptured" scenarios that are just as likely or probably even more likely than what is captured in the current risk plots.

For example, the PFMA performed in 2014 directly 'analyzed' the potential for spillway failure and erosion/scour as a result of discharge over the Emergency Spillway. Both scenarios were discounted by the PFMA team and concluded as posing 'no problem' for the dam. Both the premise for the conclusion as well as the conclusions themselves were incorrect. This incorrect finding highlights a fundamental problem with PFMAs and RIDM. Full

reliance on 'experts' without cross-checking will lead to the wrong decision and yield 'surprises' down the road. We know better!

Table 6.4 Adverse and Positive Factors for Candidate F4

Candidate F4: PMF Event Occurring, the Left Spillway Chute Wall is Overtopped and Impacts the Dam Embankment	
Adverse Factors	**Positive Factors**
	Design of the overflow section and spillway channel should prevent this.

Rationale for Not Carrying PFM forward: The spillway chute is designed to accommodate flows in excess of the operational requirements of the flood control regulation plan (150,000 cfs). The FCO has passed 150,000 cfs in the past without overtopping the wall. The emergency spillway can pass sufficient flow such that the FCO would not need to pass more than 150,000 cfs during the PMF.

6.1.5 Candidate F5: Loss of the Spillway Channel Lining Results in Erosion of the Rock Underlying the Spillway

Candidate Description: Cavitation or slabjacking results in loss of the concrete lining in the spillway chute downstream of the FCO. The rock in the spillway chute erodes and the FCO is undermined and lost.

The adverse and positive factors related to Candidate F5 are provided in Table 6.5.

Table 6.5 Adverse and Positive Factors for Candidate F5

Candidate F5: Loss of the Spillway Channel Lining Results in Erosion of the Rock Underlining the Spillway	
Adverse Factors	**Positive Factors**
	The spillway channel concrete is in good condition and there is no evidence of significant erosion or stress resulting from flows experienced to date.
	The rock is fresh and hard and resistant to erosion.
	The duration of large flows through the FCO is not sufficient to develop significant erosion of the rock.
	DWR has performed minor repairs to the spillway concrete as recently as 2009.

Figure 29: Excerpt from redacted 2014 PFMA report summarizing the 'analysis' associated with potential spillway failure.

Rationale for Not Carrying PFM forward: The spillway chute is in good condition and the underlying rock is very competent. Many spillways are constructed of rock with no concrete lining. It is seen as highly unlikely that the concrete lining will fail and highly unlikely that significant erosion of the rock will occur during one spilling event.

6.1.6 Candidate F6: Scour of Soil and Debris During Flow Over the Emergency Spillway Blocks the Feather River

Candidate Description: Flow over the emergency spillway during a large flood scours soil and trees from the slope as water flows over the emergency spillway to the Feather River. This blocks the river and causes the river to backup.

The adverse and positive factors related to Candidate F6 are provided in Table 6.6.

Table 6.6 Adverse and Positive Factors for Candidate F6

Candidate F6: Scour of Soil and Debris During Flow Over the Emergency Spillway Blocks the Feather River	
Adverse Factors	**Positive Factors**
Creates adverse condition downstream.	The large flows would prevent damming of the river with debris.
	This would not result in a dam failure.
	The slope below the emergency spillway has relatively little vegetation and surficial cover and the underlying bedrock is not subject to significant erosion.

Rationale for Not Carrying PFM forward: Damming of the Feather River is seen as highly unlikely under the heavy flows that would be occurring if the emergency spillway is activated. Even if this did occur, and there was no scenario that would result in failure of the dam or an uncontrolled release.

6.2 Static Loading Candidate PFMs Not Carried Forward

6.2.1 Candidate S1: Clogging of Downstream Pervious Zones leading to Elevated Phreatic Surface and Slope Instability

Candidate Description: Downstream internal drain zones, Zones 5a (Blanket) or 5b (Chimney) and/or shell Zone 3 become clogged and do not adequately drain and convey seepage from the dam core Zone 1 and under-seepage from the foundation; a phreatic line (elevated pore pressures) develops in the downstream zones and a seepage face emerges on

Figure 30: Rationale for not considering primary spillway failure in yellow highlight. "Analysis" of Emergency Spillway erosion/scour show in green highlight.

Consideration of Appurtenant Structures

OVERALL COMMENT: APPLICABLE TO CNA - INSUFFICIENT INFORMATION

The IFT noted that historically, DWR allocated disproportionate attention towards certain features of the dam complex, rather than a more balanced portfolio of attention relative to structure importance and associated risks. As a result of the limited scope of the CNA (see ***DWR Comprehensive Needs Assessment2*** that outlines the six tasks), disproportionate attention to differing elements of the Oroville Dam Complex is continued. It is unclear how other 'appurtenant structures' were included or excluded as no overarching summary of assets was presented.

Owner's Dam Safety Program and Dam Safety Culture

OVERALL COMMENT: APPLICABLE TO CNA – INSUFFICIENT INFORMATION

Safety culture aspects were not addressed in the CNA report. The intent of the 'risk-informed decision-making' (RIDM) approach is aligned with the IFT recommendation, but this particular RIDM only considered a sub-set of the larger system.

Specific Lessons to be Learned for DWR

In addition to the industry-wide recommendations, the IFT also had specific and targeted recommendations for the California Department of Water Resources. These recommendations are more 'organizational' in nature and thus are a bit challenging to fully evaluate in the limited interactions as part of the CNA and Ad Hoc meetings. However, high-level observations are noted. A formal audit by an outside 'independent' qualified organization with experience is recommended.

Organizational Culture and Internal Working Relationships

OVERALL COMMENT: APPLICABLE TO CNA - INSUFFICIENT INFORMATION

Limited insight was gained during the CNA process. However, compared with attributes from Safety II and HROs, there appears great opportunity for advancement on this IFT recommendation.

Appropriate Staffing for Technical Positions

OVERALL COMMENT: APPLICABLE TO CNA - INSUFFICIENT INFORMATION

Limited insight was gained during the CNA process. Much of the content developed and shared was by outside consultants rather than internal DWR personnel. It should be noted that the US Bureau of Reclamation predominantly uses internal staff, rather than outside consultants, for their risk analyses. This has many benefits, the most evident is internal staff having familiarity with scenarios, assumptions and the ability to rapidly leverage insights from past scenarios during actual unfolding events.

Technical Expertise Related to Dam Engineering and Safety

OVERALL COMMENT: APPLICABLE TO CNA - INSUFFICIENT INFORMATION

It appears that significant effort has been expended by DWR to increase exposure to and training in risk-informed decision-making. As previously described, this is useful, but not exhaustive. Additional techniques and trainings are needed. There is an extensive body of literature and many methods and techniques available that could be extended to dam safety. Exploration of these concepts, along with validation studies of the extended techniques would greatly advance dam safety for not just DWR, but the dam safety community as a whole. This is an

opportunity for DWR to be a leader (as required by Water Code Section 6102) to expand the portfolio of techniques and methods to ensure the highest degree of safety and reliability.

Dam Safety Program and Risk Management

OVERALL COMMENT: APPLICABLE TO CNA - INSUFFICIENT INFORMATION

The IFT noted that consideration should be given to restricting and possibly relocating the "Dam Safety Branch." It was also to consider how to advance dam safety "over and above simple regulatory requirements." The "risk-informed decision-making" process is a regulatory requirement. It is unclear that any additional methods, outside those required by regulation, have been pioneered by DWR. This is an opportunity for DWR to be a leader (as required by Water Code Section 6102) to expand the portfolio of techniques and methods to ensure the highest degree of safety and reliability.

RECOMMENDATIONS

The safety culture literature cautions against putting all your eggs in one 'basket' when it comes to 'mindfulness of potential "preventable-irreversible" problems.' As presented, the CNA/DWR is 'following' the federal agencies into the domain of 'risk-informed decision-making' (RIDM). RIDM was used by many organizations and STILL RESULTED IN PREVENTABLE FAILURES (Boeing 737 MAX, Deepwater Horizon, PGE Wildfires, Fukushima, etc.).

The "Rasmussen Study" published in October of 1975 [17] was a seminal paper/study that embraced a risk-based approach to the challenge of nuclear power plant failure.

> *The Reactor Safety Study was sponsored by the U.S. Atomic Energy Commission to estimate the public risks that could be involved in potential accidents in commercial nuclear power plants of the type now in use. It was performed under the independent direction of Professor Norman C. Rasmussen of the Massachusetts Institute of Technology. The risks had to be estimated, rather than measured, because although there are about 50 such plants now operating, there have been no nuclear accidents to date resulting in significant release of radioactivity in U.S. commercial nuclear power plants. Many of the methods used to develop these estimates are based on those that were developed by the Department of Defense and the National Aeronautics and Space Administration in the last 10 years and are coming into increasing use in recent years.*
>
> *The objective of the study was to make a realistic estimate of these risks and, to provide perspective, to compare them with non-nuclear risks to which our society and its individuals are already exposed. This information may be of help in determining the future reliance by society on nuclear power as a source of electricity.*

The outcomes of the Nuclear Safety Study [17] were highly scrutinized. A review and commentary report was issued in 1978 [2]. This report highlighted some challenges associated with the risk-based approaches (), that are still challenges to this day:

> *We have found a number of sources of both conservatism and non-conservatism in the probability calculations in WASH-1400, which are very difficult to balance. Among the former are inability to quantify human adaptability during the course of an accident, and a pervasive regulatory influence in the choice of certain parameters, while among the latter are nagging issues about completeness, and an inadequate treatment of common cause failure. We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated. We cannot say by how much. Reasons for this include an inadequate data base, a poor statistical treatment, an inconsistent propagation of uncertainties throughout the calculation, etc.*

SUMMARY

The Risk Assessment Review Group was organized by the U.S. Nuclear Regulatory Commission on July 1, 1977, with four elements to its charter:

(1) Clarify the achievements and limitations of WASH-1400, the "Rasmussen Report."*

(2) Assess the peer comments thereon, and responses to those comments.

(3) Study the present state of such risk assessment methodology.

(4) Recommend to the Commission how (and whether) such methodology can be used in the regulatory and licensing process.

The group was formed to represent a wide spectrum of views about nuclear safety, though each member was chosen for his technical expertise. We have profited from a year of study and testimony, and wish to acknowledge the outstanding cooperation we have received from the staff of the Nuclear Regulatory Commission, the nuclear industry, and concerned scientists and citizens.

We find that WASH-1400 was a conscientious and honest effort to apply the methods of fault-tree/event-tree analysis to an extremely complex system, a nuclear reactor, in order to determine the overall probability and consequences of an accident. We have reviewed the methodology, the data base, the statistical procedures, and the results.

We have found a number of sources of both conservatism and nonconservatism in the probability calculations in WASH-1400, which are very difficult to balance. Among the former are inabilit to quantify human adaptability during the course of an accident, and a pervasive regulatory influence in the choice of uncertain parameters, while among the latter are nagging issues about completeness, and an inadequate treatment of common cause failure. We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated. We cannot say by how much. Reasons for this include an inadequate data base, a poor statistical treatment, an inconsistent propagation of uncertainties throughout the calculation, etc.

Also, both the dispersion model for radioactive material and the biological effects model should be improved and updated before they are applied in the regulatory and licensing process.

*U.S. Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975. Available from National Technical Information Service, Springfield, VA 22161.

Figure 31: Identification of 'challenges' associated with risk-based methods used in Reactor Safety Study.

Essentially, all the "DWR safety and reliability" eggs are being knowingly placed in this very flawed and problematic basket. The nuclear industry, perhaps, has the most extensive knowledge and experience with risk-based methods and have invested orders of magnitude more time, energy, and effort than the entire 'dam safety and risk management' community combined. We still suffer 'unintended' catastrophic incidents to this day across the industry. The following considerations are presented with respect to risk-based methods:

- Understanding the magnitude of uncertainty is fundamentally essential to risk management
- All risk analyses are wrong, but can be useful
- Risk analyses performed by 'outside' experts (not system-related) are even more wrong due to lack of system knowledge
- Failure modes associated with incorrect design or procedures are frequently omitted, while these constitute the majority of system failures
- Risk analyses facilitate sensitivity studies, which are very useful to confirm/refute design assumptions and uncertainty magnitudes of system 'components'
- Risk-based approaches are useful to distinguish between known high-likelihood/high-consequence events from low-likelihood/low-consequence
- Being aware of 'expected' conditions can allow for rapid detection of divergence into 'unexpected' conditions (interactive risk/crisis management)

These recommendations are structured to not remove a basket, but to augment through additional baskets. This also puts DWR in a position of leadership as opposed to being 'followers.' The recent updates to the water code look to California to be leaders, not followers. The internal DWR working theory may be that DWR is doing 'best practice' with respect to dams because it is 'following' the regulatory minimum, but 'dams' is not doing 'best practice' with respect to safety and reliability from the 'safety culture' standpoint. DWR, if it chooses, can help 'dams' to catch up to the international 'best practice' on safety and reliability.

Five recommendations are presented in this report that will improve the current 'standards' in use by DWR, as related to the safety and reliability of DWR's dams, as well as all other dams in California. These recommendations are currently, as of this report, outlines/concepts and additional work will be required to structure pragmatic valid and reliable approaches. This additional work is beyond any one organization. It will take the collective efforts from the State of California, Academia, Non-Profits/NGOs, and Industry. However, we can initiate this journey and help organize the efforts so we achieve the intended outcomes as quickly and efficiently as possible.

(1) Revise the California Water Code Section 6102

From the California Water Code Section 6102

> *(b) Globally and nationally, there is recognition that, as with all aging infrastructure, there is an unmet need regarding dam maintenance and repairs.* ***California needs to continue to lead efforts to address these unmet needs, and improve upon standards set by regulatory agencies to ensure public safety****.*
>
> *(c) …California's dam safety procedures must stay on par with, or ahead of, best practices and must continually update those procedures based on the* ***best available knowledge****.*
>
> *(d) In order to ensure that the practices of the Division of Safety of Dams continue to reflect the best available knowledge, and in light of recommendations arising from the independent Forensic Team's review of the Oroville*

Dam spillway incident, ***the Division must consult with independent dam safety and dam safety risk management organizations to propose additions*** *to the Division's existing dam safety program in order to incorporate updated best practices to ensure public safety, as set forth in 6102.*

The guidance provided in this section of the water code is on point. Accountability, however, is missing. Consideration should be given to establishing a 5-year 'state of the practice' "Dam Safety & Reliability Workshop" (with formal documented proceedings) that highlights 'state of the art' and 'emerging technologies' relative to dam safety in California. These workshops can be hosted by various academic institutions within California, perhaps on a rotating basis. This structured approach would allow explicit feedback to all dam owner/operators in California on new and emerging techniques that can potentially be implemented to enhance dam safety and reliability.

For 6102(d) it is recommended that the language be modified to expand from 'dam safety' to safety 'best practices' from all types of industries/sectors, not just in the United States, but internationally as well. Section d would be modified as follows:

d) In order to ensure that the practices of the Division of Safety of Dams continue to reflect the best available knowledge, and in light of recommendations arising from the independent Forensic Team's review of the Oroville Dam spillway incident, ***the Division must consult with independent ~~dam~~ safety and ~~dam safety~~ risk management organizations to propose additions*** *to the Division's existing dam safety program in order to incorporate updated best practices to ensure public safety, as set forth in 6102.*

The "Dam Safety & Reliability Workshop" could be a formal process to identify proposed additions and updated manuals/policies.

The Center for Catastrophic Risk Management (CCRM) at UC Berkeley would be happy to organize and host the initial workshop.

Estimated configuration and implementation timeframe: months to years

(2) Perform Design Assumption Audits

Formal audits of all infrastructure components should be initiated that locate the original design documentation and inventories the design assumptions. These critical documents become the basis for safety and reliability analyses. FERC currently requires (as stipulated in Chapter 14 of their Engineering Manual [14]) The design intent and associated design assumptions should be established for all of the dam features. In cases where the design intent is unclear or not established, the dam owner/operator would need to re-establish or create formal designs along with stated design assumptions. This approach, results in a full and complete characterization of the system and serves as a basis by which to delineate the 'expected' performance.

The current process delineated by FERC for US dams can be further bolstered by reviews of these design assumption audits by external unaffiliated and non-conflicted experts, similar to the USACE Independent External Peer Review (IEPR) process. The USACE IEPR process entails a third-party facilitator (such as Battelle Corporation) to assemble a team of qualified experts who have been cleared of all potential 'conflict of interest' as well as active consulting contracts. A proposed modification to the USACE IEPR would be to make the assumption audit 'blind,' where the names and affiliations of the experts are not disclosed to the dam owner/operator. This 'blind' review maximizes the ability of the expert reviewers to challenge incomplete/inadequate work without fear of retaliation personally or toward their employer.

The intended outcomes of the design assumption audit include: (1) collate original design information to establish the 'intended performance' attributes of the dam; (2) conduct a gap analysis to identify missing design information

where new analyses are required to re-calculate and establish design assumptions; (3) list all original design assumptions so they can be compared with current requirements and serve as a 'leading indicators' that upgrades/replacements are required in order be compliant with current knowledge and the intended performance levels.

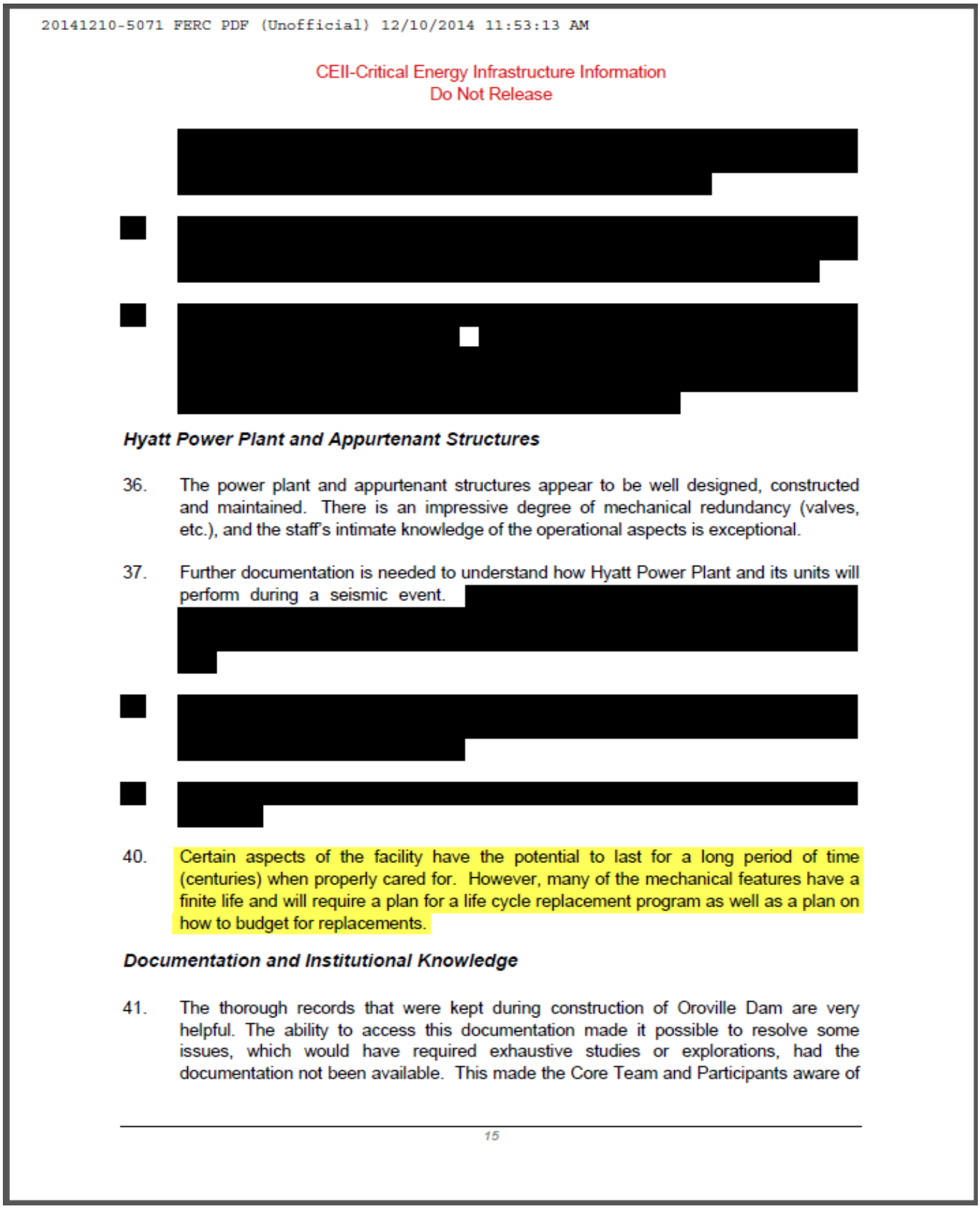
Estimated configuration and implementation timeframe: months to years

(3) Implement Life-Cycle-Based Management

Life-Cycle-Based Management approaches system components with the perspective that there are anticipated serviceability timeframes. These time-frames are variable depending on the attributes and characteristics of the actual system component. Discussion of life-cycle based perspectives were first documented in the 2014 PFMA by the 'risk' expert team, relative to the Hyatt Power Plant (Figure 32).

The Life-Cycle-Based Management approach establishes a system-based management approach whereby anticipated annual operation and maintenance costs are established along with a replacement schedule and cost. This allows appropriate management and capital replacement budgets and funding to be established to ensure that the required funding is available when needed. It replaces a 'year-by-year' budgeting approach that typically results in deferred maintenance due to the ability to quickly generate large magnitude budget increases. The deferred maintenance then leads to incremental degradation in the safety and reliability of the high-hazard, endangering the down-stream community.

Extensive knowledge exists on this topic and numerous consultants can get DWR functional in this area very quickly.



20141210-5071 FERC PDF (Unofficial) 12/10/2014 11:53:13 AM

CEII-Critical Energy Infrastructure Information
Do Not Release

[redacted]

Hyatt Power Plant and Appurtenant Structures

36. The power plant and appurtenant structures appear to be well designed, constructed and maintained. There is an impressive degree of mechanical redundancy (valves, etc.), and the staff's intimate knowledge of the operational aspects is exceptional.

37. Further documentation is needed to understand how Hyatt Power Plant and its units will perform during a seismic event. [redacted]

[redacted]

40. Certain aspects of the facility have the potential to last for a long period of time (centuries) when properly cared for. However, many of the mechanical features have a finite life and will require a plan for a life cycle replacement program as well as a plan on how to budget for replacements.

Documentation and Institutional Knowledge

41. The thorough records that were kept during construction of Oroville Dam are very helpful. The ability to access this documentation made it possible to resolve some issues, which would have required exhaustive studies or explorations, had the documentation not been available. This made the Core Team and Participants aware of

15

Figure 32: Acknowledgement of need for life-cycle considerations within the Hyatt Power Plant in the 2014 PFMA.

Estimated configuration and implementation timeframe: months to years

(4) DSOD Standalone Organization

The Department of Safety of Dams (DSOD) is currently a sub-organization within the Department of Water Resources. This means that the fiscal budget, personnel selection, organizational culture is controlled by DWR. DWR also owns and operates numerous dams that are subject to regulatory oversight by DSOD. DWR being regulated by itself is a clear conflict of interest and greatly reduces the 'trust' the community has in the integrity of the reported safety and reliability of California dams. This conflict of interest between DWR and DSOD must be mitigated in order to minimize the potential for 'going easy' or not thoroughly challenging and vetting the management and operational aspects of our high-hazard dams

DSOD was formed in response to the failure of St. Francis Dam in 1929. The intent of the organization was to ensure the safety and reliability of California dams so that no future 'unacceptable' dam failures would occur. The failure of the Oroville Dam spillway in February 2017 occurred under the oversight of DSOD. As the IFT noted, we must challenge what constitutes 'best practice' with respect to safety and reliability of our dams. Eliminating obvious and potentially lethal conflicts of interest between regulators and the regulated is an evident starting point to enhance the safety and reliability of our dams and is consistent in challenging the current 'best practice' of having our regulator 'report to' and be 'beholden to' a dam owner/operator.

Estimated configuration and implementation timeframe: months to years

(5) Utilization of a "Performance Insurance"

Finally, a financial accountability instrument, which I'll refer to as "Performance Insurance" should be considered by the California Legislature to be mandated for all California high-hazard dam owners. The premise of this recommendation is that as part of the design and construction process of a dam, a certain level of performance is 'promised' to the community via the design. The dam, for example, is formally designed to (see also Figure 33):

- convey a certain amount of water out the primary spillway (Oroville dam: 296,000 cfs [1] [13])
- convey a certain amount of water out the emergency spillway (Oroville dam: 350,000 [1] [13])
- receive a certain amount of inflow water over a period of time (Oroville dam: PMF of 725,000 cfs [13])
- tolerate a seismic event (Oroville dam: [13])

High-hazard dam owner/operators would need to carry insurance or bond or maintain a fund to cover potential financial obligations should actual performance fall short of intended If failure in the dam system occurs at a level below these stated and 'promised' performance levels, the impacted community is financially compensated based on a 'parametric payout' schedule. This has a number of benefits:

(1) There would be immediate and direct financial accountability, based on the parametric payout parameters, for the actual performance of the high-hazard dam decoupled from the current approach of litigation, which typically takes decades and results in fractional restitution for the individual community member;

(2) A secondary organization would 'peek behind the curtain' of the operation and management practices of the high-hazard dam owner/operator to ensure the purported level of safety and reliability matches the 'known' and 'documented' evaluations within the owner/operator organization. This secondary organization also has the benefit of comparing/contrasting approaches across different owner/operators and financially incentivizing approaches based on premiums;

(3) Finally, if these dams are as 'safe and reliable' as reported by the owner/operators, the 'risk' to the insurance/bonding organizations would be very low and have correspondingly low premiums. If the insurance/bonding organizations find (with the assistance of their technical evaluation and modeling support team(s)) the purported safety and reliability levels do not coincide with their internal findings and/or the magnitude of uncertainty associated with the safety and reliability is sufficiently great, then very high premiums may be assessed. In cases where the assessed premiums are much greater than anticipated, meaningful discussions would likely occur to bridge the gap between what the dam owner/operator 'hopes' the level of safety and reliability is compared with the assessed level of safety and reliability by the insurance/bonding organization. This assumes there is a large enough 'market' in California for open competition amongst the global insurance/bonding marketplace.

Much work would be required to configure this sort of approach, but the utility of this tool is it ensures the financial risk of failing to meet the promised performance level of the high-hazard dam remains with the dam owner/operator rather than being transferred (unknowingly) to the community. Further, the need for the community to 'trust' that the dam owner/operator is appropriately managing their risk is eliminated. Full accountability rests with the dam owner/operator and their insurer/bonding organization.

[redacted]. A brief summary of the pertinent data on Oroville Dam is provided on Table 2.1.

Table 2.1 Oroville Dam Summary of Pertinent Data

Pertinent Data	
Location	5 miles northeast of Oroville, CA
Stream/River	Feather River
Type	Zoned earth and rockfill embankment
Hazard Class	High
Construction Date	1968
Dam Height	770 feet
Dam Crest Length	5,420 feet
[redacted]	[redacted]
Normal Max. Reservoir Elev.	900 feet
Normal Reservoir Elev.	875 feet (the reservoir level can vary by several hundred feet, for the purposes of the PFMA, El. 875 feet was used as the normal reservoir level)
Drainage Basin	3,607 square miles
Reservoir Capacity	3,537,577 acre-feet

4

20141210-5071 FERC PDF (Unofficial) 12/10/2014 11:53:13 AM

CEII-Critical Energy Infrastructure Information
Do Not Release

Pertinent Data	
Reservoir Area	15,800 acres
Spillway Type	Gated flood control outlet (FCO) structure. Emergency spillway (two sections: 800-ft long broad crested weir, 930-ft long gravity ogee weir).
Emergency Spillway Elev.	901 feet
PMF/IDF	PMF (2003 study) based on HMR 59, inflow 725,000cfs / outflow 671,000 cfs, starting at elevation 901 feet.
Max. PMF Water Surface Elev.	917.5 feet (2003 study)
Minimum PMF Freeboard	4.5 feet (2003 study)
Controlling Fault & Peak Ground Acceleration	Cleveland Hill Fault – Mw 6.5 earthquake. 50th percentile horizontal ground motion estimate of PGA is 0.57g.

2.2 Dam

Oroville [redacted] is [redacted] zoned earth [redacted] with a maximum height of 770

Figure 33: Reported 'design' performance levels of Oroville Dam [13].

This ‘performance insurance’ would differ from other approaches, such as the Price-Anderson Act of 1957. The Price-Anderson Act became law in 1957 as part of amendments to the Atomic Energy Act of 1954. The Act sets a limit on the monetary liability of companies for a nuclear accident, and defines the procedural mechanisms for the industry’s insurance coverage. Complaints [18] on this Act include (1) that the financial compensation limits are well below the full magnitude of anticipated financial costs associated with triggering events; (2) Price-Anderson is blind to comparative differences in and arbitrarily treats the whole industry uniformly. Higher-risk reactors - including older, relicensed reactors with aging parts - are not required to carry correspondingly higher levels of insurance coverage. Moreover, the Price-Anderson Act does not stipulate security requirements to protect against terrorism at insured reactors; and (3) Act has no fault liability for reactor operators, and injured victims are precluded from directly suing vendors or manufacturers responsible for the accident. These types of issues would need to be addressed in the responsible formulation of a ‘performance insurance.’

Estimated configuration and implementation timeframe: years

WORKS CITED

[1] I. F. T. (IFT), "Independent Forensic Team Report Oroville Dam Spillway Incident," 2018.

[2] U. N. R. Commission, "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission NUREG/CR-0400," U.S. Nuclear Regulatory Commission, 1978.

[3] C. D. o. W. R. (DWR), "Oroville Dam Safety Comprehensive Needs Assessment," [Online]. Available: https://water.ca.gov/Programs/State-Water-Project/SWP-Facilities/Oroville/Oroville-Dam-Safety-Comprehensive-Needs-Assessment. [Accessed 08 01 2021].

[4] C. D. o. W. R. (DWR), "Bulletin 132-17 MANAGEMENT OF THE CALIFORNIA STATE WATER PROJECT," 2017.

[5] C. D. o. W. R. (DWR), "KG_oro_spillway_damage_11232_02_12_2017.jpg," [Online]. Available: https://pixel-ca-dwr.photoshelter.com/galleries/C0000OxvlgXg3yfg/G00003YCcmDTx48Y/I0000v5.YzdNCf1I/KG-oro-spillway-damage-11232-02-12-2017-jpg. [Accessed 08 01 2021].

[6] C. D. o. W. R. (DWR), "FL_Oroville-1299_02_11_2017.jpg".

[7] C. D. o. W. R. (DWR), "FL_Oroville-1481_02_13_2017.jpg".

[8] C. D. o. W. R. (DWR), "Charter or Oroville Dam Safety Comprehensive Needs Assessment - Public Ad Hoc Group," 2018.

[9] E. W. Jr., "Teaching Engineering as a Social Science," *ASEE PRISM,* 1996.

[10] U. C. S. A. H. I. BOARD, "INVESTIGATION REPORT VOLUME 3 DRILLING RIG EXPLOSION AND FIRE AT THE MACONDO WELL".

[11] R. Bea, "Human and Organizational Factors: Quality and Reliability of Engineered Systems, Volume 2, Course Lecture Illustrations & Notes," 2008.

[12] D. a. J. C. S. Campbell, Experimental and Quasi-Experimental Designs for Research, Boston: Houghton Mifflin, Co., 1963.

[13] G. Fleming, "Potential Failure Mode Analysis Report, Oroville Dam, FERC Project No. 2100-CA, Oroville California, November 14, 2014," 2014.

[14] F. E. R. C. (FERC), "Engineering Guidelines for the Evaluation of Hydropower Projects".

[15] U. A. C. o. E. (USACE), "Engineering and Design - Safety of Dams - Policy and Procedures, ER 1110-2-1156".

[16] B. S. P. a. L. S. Fischoff, "Knowing with Certainty: The approxpriateness of extreme confidence," *J. Exp. Psychology Human Perception adn Performance,* vol. 3, no. 4, pp. 552-564, 1977.

[17] U. N. R. Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG 75/014)," 1975.

[18] P. Citizen, "Price-Anderson Act: The Billion Dollar Bailout for Nuclear Power Mishaps," 2004.

APPENDIX A

CNA Meeting #1 Materials

APPENDIX B

CNA Meeting #2 Materials

APPENDIX C

CNA Meeting #3 Materials

APPENDIX D

CNA Meeting #4 Materials

APPENDIX E

CNA Meeting #5 Materials

APPENDIX F

CNA Meeting #6 Materials

APPENDIX G

CNA Meeting #7 Materials

APPENDIX H

CNA Meeting #8 Materials

APPENDIX I

DWR Final CNA Report

APPENDIX J

IFT Final Report

APPENDIX K

2004 Oroville Dam PFMA (Redacted)

APPENDIX L

2009 Oroville Dam PFMA (Redacted)

APPENDIX M

2014 Oroville Dam PFMA (Redacted)

APPENDIX N

2018 Oroville Dam PFMA (Redacted)

APPENDIX O

DWR/DSOD Comments

APPENDIX P

IFT Comments