## Case Study with Supporting Media and Simulation Exercise

**Title: Cybersecurity in Water and Hydropower Dams**

---

## Real World Inspiration

Across the United States, you can find around 92,000 dams, dotting rivers and canyons all throughout the country. Dams serve many purposes, whether it be flood risk reduction, irrigation, water supply, or hydroelectricity, among many others. As it stands, “Dams Sector assets irrigate at least 10 percent of U.S. cropland, help protect more than 43 percent of the U.S. population from flooding, and generate about 60 percent of electricity in the Pacific Northwest.” [1] An attack can mean insufficient water supply or irrigation, with the severest of consequences being possible drought and/or famine. When considering floods or blackouts, consequences can become fatal. The continuous maintenance and security of the Dams Sector is extremely important, as it has an impact on multiple industries in the United States’ critical infrastructure, as well as the lives of all citizens.

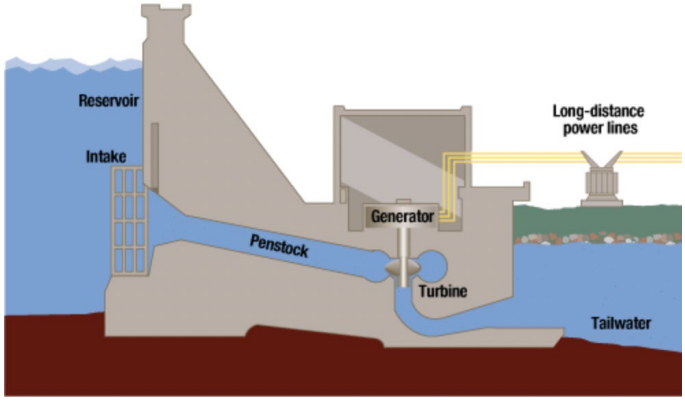


Figure 1: diagram of a dam that generates hydroelectricity [2].

With the large amount of dams in the U.S., there comes quite a variety of dam sizes, purposes, and complexity. Oftentimes, the more importance a dam’s purpose has, the more complex its design will be. For example, a dam that generates hydroelectricity will include turbines and generators, which you can see in Figure 1. The dam holds water in a reservoir, and when water is released, it spins a turbine that is connected to a generator [2]. Now what if the turbine is stopped, or the generator is turned off? This is what can lead to a blackout. Aside from certain dam components that pose greater risks if attacked, dams in general share some characteristics that are cause for concern in cybersecurity. The average age of a dam in the US is 61 years old [3]. This means that most dams are operating on decades-old infrastructure, utilizing inadequate security controls and outdated patches [4]. Because of the age concerns, dams are undergoing a modernization effort. With the added cyber changes, “... systems are modernized and adopt digital technology, which can introduce new vectors of attack if not secured properly” [5]. These new vectors of attack are what need attention, as the aforementioned security controls and patches will be the first to be targeted in cyberattacks. These attacks could allow the attacker to gain access and control to critical control systems and allow them to disrupt physical processes [4]. Beyond the aging infrastructure, there are also vulnerabilities in the designs of some dams. The large majority of dam failures occur due to flooding or overtopping [3]. This happens when the amount of heavy rainfall is simply too high and exceeds the storage and discharge capacities that the dam was designed for. Design issues can go as far as the operational design of a dam. Many dams are managed remotely over the internet. While companies save money by not

requiring on-site operators, the risks of cyber attacks increase greatly [6]. Moreover, workplace policies can create issues as well. Currently, only 81% of high-hazard potential dams have an Emergency Action Plan [3]. Without an Emergency Action Plan, workers are left without an answer for attacks that do happen.

With so many vulnerabilities and the risks involved with those, it is crucial to think of countermeasures against those. This is where Cyber Informed Engineering principles come in. CIE encourages engineers to consider cybersecurity at every step of the design process, rather than just as an afterthought thrown on at the end. Many principles might apply to any one problem. For example, **CIE principle #2, Engineered Controls**, can apply to the dam scenario by asking the question *How do I select and implement controls to reduce avenues for attack or the damage that could result?* Dam designers could use this principle to consider certain design elements that could help keep a dam from overtopping if an attacker were to take control of water levels. Another principle that could greatly help is **CIE principle #4, Design Simplification,** which asks *How do I determine what features of my system are not absolutely necessary to achieve the critical functions?* This could be helpful to keep in mind if looking to specialize between reservoir and hydropower dams. Another countermeasure that dams are already implementing focuses on **CIE principle #6. This principle is Active Defense**, which asks the question *How do I proactively prepare to defend my system from any threat?* This is being implemented in the form of a reservoir water level alarm that does not allow for remote shut-off. This means that if the water levels in a dam get dangerously high, an alarm will alert all workers to the issue. And because there is no remote shut-off, a worker would have to turn it off in-person, ensuring that the emergency has been seen and acknowledged.

## Media Feature for the General Audience

For a custom media clip designed by faculty and students of the University of Pittsburgh, please click on the video file found here: **https://youtu.be/p9aawDaO3gU**

The linked video is an information piece on cybersecurity of dams as well as the implementation of cyber-informed engineering in that context. It begins in a narrative setting to get the audience invested in the unnamed person we see, so that when they suffer the severe consequences of the dam hack, it is upsetting for the audience, and therefore draws them into the issues at hand.

The video then goes into more detail on cyberattacks on dams, and how they are particularly vulnerable. It then introduces cyber-informed engineering and poses questions to challenge the viewers on what they have learned.

## Future Policy Implications

The organizational policy decisions made by dam owners and managers in the United States mostly reflect mandatory regulation rather than internal preferences. However, no single regulatory entity has jurisdiction over all of the approximately 97 percent of American dams that do not support hydroelectric generators [13]. Instead, roughly 70 percent of facilities are regulated by state agencies, with the remainder under the authority of the federal government or unregulated due to exemptions [14]. Those few institutions whose recommendations indeed apply to the dams sector in its entirety generally lack the capacity to issue binding mandates. For instance, the Department of Homeland Security (DHS), which serves as the Dams Sector-Specific Agency, may only provide domain expertise and help implement federal partnerships with the private sector [15]. One of the operational components of the DHS, the Cybersecurity & Infrastructure Security Agency (CISA), acts as the Dams Sector Risk Management Agency and bears a similar inability to issue regulation [16].

CISA guidance, however optional, represents likely the most substantive basis for the improvement of cybersecurity for dams without the capability to generate electricity. The organization's advice, following the intentions articulated in the 2015 Dams Sector-Specific Plan, has been distilled into the Cybersecurity Framework Implementation Guidance, published in 2020 [17]. This document works to provide dam management professionals with a policy scheme that is simultaneously mindful of the organizational structures particular to the dam sector and capable of implementing more general cybersecurity frameworks—namely those developed by the National Institute of Standards and Technology, or NIST. While more abstract than technical, the Implementation Guidance functions to assist dams with creating their own threat identification procedures, protective technology, detection processes, and response and recovery planning [17].

For dams with hydroelectric capabilities, CISA recommendations still apply. However, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Standards prove a much more prominent cybersecurity resource. This position stems mainly from the Standards' status as mandatory for all components of the Bulk Electric System in the United States [18]. Unlike the Cybersecurity Framework Implementation Guidance, NERC CIP promotes cybersecurity from a tangible, somewhat technical perspective. The Standards, each with their own set of suggested measures that qualify as compliance, address security management controls, electronic security perimeters, supply chain risk management, and several other pillars relevant to cyber-informed engineering [18].

In the future, dams without responsibility for power generation may benefit from optional internal adoption of those NERC CIP Standards dealing with organizational culture and policy. For instance, consider CIP-004, the Standard pertaining to personnel and training. This document offers direction for the creation of internal programs for security awareness, cybersecurity training, personnel risk assessment, access management, and access revocation [19]—all of which are vital initiatives regardless of whether a dam supports hydroelectric generators. Even the specific measures suggested, such as the reverification of all user accounts and their associated privileges every 15 months or less [19], mostly appear to constitute universal best practices for the dam sector. Other NERC CIP Standards, including those which dictate internal governance and policy surrounding security management controls, enjoy a similar degree of breadth in applicability. (Note that this latter Standard, CIP-003, may require some adjustment for use within non-hydroelectric dams due to its reliance on the verbiage of a "CIP Senior Manager" [20].)

## Part 1: Expand Your Understanding with the Following Exercise

Hypothetical Scenario 1:

The Hamburger Dam straddles a river canyon five miles upstream of the coastal Herbert City and supplies most of the city's 200,000 human population with 400 MW of electricity through a pumped-storage hydropower system. To avoid generator explosions similar to Russia's 2009 Sayano-Shushenskaya power station incident, where an improperly balanced turbine was overstressed and broke apart, the Hamburger Dam air gaps the generator control system to maintain tight control over generator water intake. This reduces the ability of attackers to program intake gate controls in a manner that induces turbine-destabilizing fluid flow fluctuations. However, the gate control system for a series of Tainter gates on the dam spillway operates through internet protocols to a centralized control station 150 miles away.

Outside attackers from Fairyland attempt to gain remote access to the Hamburger Dam. Although they are unable to access the power plant controls, they exploit zero-day vulnerabilities in the communication protocols of an old internet browser used by the central control station to access Hamburger Dam's floodgate controls and successfully drain a tenth of

the dam's reservoir, sending Herbert City two feet under water. Once the hackers had access to controls for the floodgates, there were no limits, or need for confirmation of their commands.

For the following questions: choose the best answer(s) then justify.

1. Question 1: Which one of the following potential vulnerabilities in the dam's security system most contributed to this attack's success?
    a. Too many people had keycard access to the dam controls
    b. Lack of digital command confirmation through secondary controllers
    c. The dam was built too close to residential neighborhoods
    d. No authentication of devices physically plugged into the control system
2. Question 2 : How could you use CIE principle #5, "Layered Defenses", to best defend from the Fairyland attack?
    a. Require a physical key and a key card to access the controls
    b. Require on-site confirmation of extreme remote commands
    c. Build another dam to protect nearby neighborhoods
    d. Implement a port block to confirm the safety of plugged-in devices
3. Question 3: Given the specific mode of attack Fairyland utilized, which of the following organizational entities bears some responsibility for failing to prevent this incident? Multiple answers may apply.
    a. Governmental agencies that issue non-binding cybersecurity guidance for the dams sector
    b. The manufacturing company that produced the concrete used in the dam's construction
    c. The information technology department that designed and implemented the facility's authorization and authentication procedures
    d. The maintenance personnel who clean and repair the dam's physical components

Hypothetical Scenario 2:

Tania is a highly skilled process engineer in good professional standing at Hamburger Dam. She is one of three engineers on-duty during the night shift and possesses emergency access to the generator controls. One sweltering August evening, Tania overhears her spouse's infidelity and the couple's plan for a late-night dip in the ocean. Tania hurries away to her shift and "accidentally" shuts all of the dam's generator intake valves, crashing the local electrical grid. The blackout includes every streetlight near the ocean coast, and the next morning two corpses wash up onto a lighthouse island a kilometer offshore. Tania testifies that her error was induced by the proximity between the controls for the pump-generators between the Hamburger Dam's upper (battery) and lower (main) reservoirs and the controls for the Hamburger Dam generators. Supposedly, she had been attempting to switch the pump-generators from generation into pumping mode to prepare for the expected decrease in power demand associated with nighttime electrical grid conditions.

For the following questions: choose the best answer(s) then justify.

A. Question 1: What was one vulnerability in the dam's system that led to the outage?
    a. Lack of an air gap allowed access to the controls via internet
    b. The employee should be able to leave their personal troubles at the door
    c. The generator automatically turns on when it receives the command
    d. The controls, one with major consequences and one used daily, exist on the same panel

B. Question 2 : How could you use CIE principle #2, “Engineered Controls”, to defend the dam from this attack?
    a. Create a single access point for communication via internet
    b. Mandate therapy to teach compartmentalization
    c. Adding some additional mechanical controls or require multiple people to perform the same action for it to go through
    d. Require a lock and key for controls that are not used daily
C. Question 3 : Assume Tania’s testimony about her error really is true. Which one of the following organizational entities bears some responsibility for the failure to prevent this particular accident?
    a. The recruiter who hired Tania
    b. The manufacturer that created the plastics used in the panel’s buttons
    c. Tania’s spouse
    d. The procurement department that allowed the purchase of a poorly designed control panel

## Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience.

[1] “Dams Sector.” *Dams Sector | Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectos/dams-sector.

[2] *How Hydroelectric Power Works*, Tennessee Valley Authority, www.tva.com/energy/our-power-system/hydroelectric/how-hydroelectric-power-works.

[3] Bowers, W Sharkey. *The Vulnerability of Dams: A Rising Threat to Life & Property*, J.S. Held, www.jsheld.com/insights/articles/the-vulnerability-of-dams-a-rising-threat-to-life-property.

[4] *Introduction to the Dams Sector Risk Management Agency*, Cybersecurity & Infrastructure Security Agency, www.cisa.gov/sites/default/files/publications/Dams%20SRMA%20Fact%20Sheet_508.pdf.

[5] Vasquez, Christian. “Congress Sounds Alarm on Lax Dam Cybersecurity.” *CyberScoop*, 10 Apr. 2024, cyberscoop.com/dam-cybersecurity-ferc-congress/.

[6] Riotta, Chris, and Ron Ross. “Hacking the Floodgates: US Dams Face Growing Cyber Threats.” *Bank Information Security*, 18 Apr. 2024, www.bankinfosecurity.com/hacking-floodgates-us-dams-face-growing-cyber-threats-a-24894

[7] Wikipedia contributors. “Dam.” *Wikipedia, The Free Encyclopedia*, May 2024, https://en.wikipedia.org/w/index.php?title=Dam&oldid=1226212836

[8] Wikipedia contributors. “Johnstown Flood.” *Wikipedia, The Free Encyclopedia*, Jun 2024, https://en.wikipedia.org/w/index.php?title=Johnstown_Flood&oldid=1229864704

[9] Wikipedia contributors. “Floodgate.” *Wikipedia, The Free Encyclopedia*, May 2024, https://en.wikipedia.org/w/index.php?title=Floodgate&oldid=1221784453

[10] Mauney, Lee. “Lesson Learned: Downstream flooding can be caused by spillway flows that exceed channel capacity or as a result of reservoir misoperation.” *Association of State Dam Safety Officials*, https://damfailures.org/lessons-learned/downstream-flooding-can-be-caused-by-spillway-flows-that-exceed-channel-capacity-or-as-a-result-of-reservoir-misoperation/

[11] Greenshields, Chris. “OpenFOAM v12 User Guide - 2.2 Breaking of a dam.” OpenFOAM v12 User Guide*, CFD Direct Ltd*, Jul 2024, https://doc.cfd.direct/openfoam/user-guide-v12/dambreak#x6-230002.2

[12] craigloewen-msft, et. al. “How to install Linux on Windows with WSL.” *Microsoft Learn*, Aug 2023, https://learn.microsoft.com/en-us/windows/wsl/install

[13] A. Mey. “Nonpowered dams can be converted to hydroelectric dams for electricity generation.” EIA.gov. Accessed: Jul. 14, 2024. [Online.] Available: https://www.eia.gov/todayinenergy/detail.php?id=39552#

[14] Association of State Dam Safety Officials. “Frequently Asked Questions.” DamSafety.org. Accessed: Jul. 14, 2024. [Online.] Available: https://damsafety.org/media/faq

[15] U.S. Department of Homeland Security. “Introduction to the Dams Sector-Specific Agency.” DamSafety.org. Accessed: Jul. 14, 2024. [Online.] Available: https://damsafety.org/sites/default/files/files/dams-ssa-fact-sheet-2016-508.pdf

[16] Cybersecurity & Infrastructure Security Agency. “Introduction to the Dams Sector Risk Management Agency.” CISA.gov. Accessed: Jul. 14, 2024. [Online.] Available: https://www.cisa.gov/sites/default/files/2023-01/dams-srma-fact-sheet-2022-508.pdf

[17] Cybersecurity & Infrastructure Security Agency. “Dams Sector: Cybersecurity Framework Implementation Guidance.” CISA.gov. Accessed: Jul. 14, 2024. [Online.] Available: https://www.cisa.gov/sites/default/files/publications/Dams_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf

[18] North American Electric Reliability Corporation. “Reliability Standards.” NERC.com. Accessed: Jul. 14, 2024. [Online.] Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[19] *Cyber Security — Personnel & Training*, NERC Reliability Standard CIP-004-7, Dec. 2021. [Online.] Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-7.pdf

[20] *Cyber Security — Security Management Controls*, NERC Reliability Standard CIP-003-9, Mar. 2023. [Online.] Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-9.pdf

## Authors

Karlynn Riccitelli, University of Pittsburgh Class of 2026. Interests include the intersection of English and Computer Science, in combination with Digital Media and User Experience Design.

Naomi Yamawaki Taylor is a rising senior at the University of Pittsburgh studying Film Production and Japanese Language. She has a background in documentary film and an interest in portrait photography.

Casey Withers, University of Pittsburgh Class of 2025. Interests include applied statistics, comparative politics, and data science.

Lambert Zhang is an engineering science major at the University of Pittsburgh with a concentration in engineering physics. He is expected to graduate in Spring 2025 and appreciates the feeling of accomplishment associated with assembling devices.