Dam Sector Analysis Report

Kaden Salzar

kadens

95-565 Homework 1

Category	Details
Dam Sector	This sector includes dams, levees, locks, and other infrastructure that manage water retention and control, and as such, has close ties with many other critical infrastructure sectors, including energy and water. The damn sectors mission is to manage water resources for agriculture, flood control, energy, navigation, and recreation and does so though partnerships “with both the private and public sector to develop industry practices that build a culture of safety and security”. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/dams-sector
Organizations	**1. U.S. Army Corps of Engineers (USACE):** Manages arond 740 dams for water resource control, public safety, and national defense. The USACE has a Dam Safety Program, which is designed to allow the USACE to be able to repair dams safely and efficiently. https://www.usace.army.mil/Missions/Civil-Works/Dam-Safety-Program/ **2. Tennessee Valley Authority (TVA):** Operates 49 dams, 29 of which generate hydroelectric power across seven Southeastern states. TVA’s mission includes hydropower generation, flood control, water quality management, navigation, and recreation, all of which align with CISA’s definition of the Dams Sector. TVA provides electricity to approximately 10 million people, making it

	the nation's largest public power utility and a key player in dam sector security and resilience. https://www.tva.com/environment/managing-the-river https://www.tva.com/
Assets	**1. SCADA Systems** - ***Cyber***, **High Criticality**: Supervisory Control and Data Acquisition Systems monitor and control dam operations in real time. SCADA systems are vital tools for dam operators to optimize performance, enhance safety, and ensure efficient management of water resources. https://damtoolbox.org/wiki/SCADA_/_ADAS https://www.sciencedirect.com/science/article/pii/S0167404822004205 **2. Dam Structure** - ***Physical***, **High Criticality**: The dam structure is the backbone of the facility, providing the physical means to regulate water flow for hydropower generation, irrigation, navigation, and public safety. Its integrity is critical to preventing catastrophic downstream impacts and is necessary for other sectors to thrive.
Security Regulations	**1. DAM SAFETY AND ENCROACHMENTS ACT** A majority of dams are regulated at the state level, with PAs Dam Safety and Encroachemnt being one example. This Pennsylvania law regulates dams, reservoirs, water obstructions, and encroachments to protect public health, safety, and property. It ensures the safe planning, design, construction, maintenance, and monitoring of these structures, with a focus on preventing failures and safeguarding natural resources. https://www.palegis.us/statutes/unconsolidated/law-information/view-statute?SESSYR=1978&SESSIND=0&ACTNUM=325&SMTHLWIND=&CHPT=&SCTN=2&SUBSCTN=

	2. The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience: While not a law, PPD-21 establishes U.S. policy to identify and strengthen the security and resilience of critical infrastructure, including dams, against both physical and cyber threats. The directive specifically tasks the Department of Homeland Security with coordinating national efforts to reduce vulnerabilities, minimize consequences, and improve response and recovery related to critical infrastructure threats. https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and
Threats	**1. Cyberattack on SCADA systems:** Attackers could exploit vulnerabilities in dam control systems to disrupt operations, manipulate water flow, or deny operator access. **2. Insider or External Physical Sabotage:** Adversaries attempt to physically breach or sabotage dam facilities, potentially damaging floodgates, intake structures, or control rooms. These actions may be motivated by terrorism, activism, or geopolitical conflict.
Threat Intel Sources	**1. WaterISAC:** Sector-specific information sharing and threat alerting. WaterISAC also provides guides to improve the physical and cybersecurity of the dam sector. https://www.waterisac.org/portal/tlpclear-cisa-%E2%80%93-dams-sector-waterside-barriers-guide https://www.waterisac.org/portal/exercise-opportunity-%E2%80%93-2024-dams-sector-information-sharing-drill **2. InfraGard:** InfraGard membership offers direct FBI engagement, 24/7 access to threat intelligence, exclusive training and events, valuable networking, and collaborative information sharing to enhance security and situational awareness for critical infrastructure owners. https://www.fbi.gov/file-repository/reports-and-publications/infragard_factsheet.pdf/view

Frameworks	**1. NIST Cybersecurity Framework (CSF):** Provides structured guidance for managing cybersecurity risks through five core functions: Identify, Protect, Detect, Respond, and Recover. It can help organizations in the dam sector prioritize and improve their cybersecurity based on risk. https://www.nist.gov/cyberframework **2. National Infrastructure Protection Plan (NIPP):** The National Infrastructure Protection Plan (NIPP) outlines how government and private sector partners collaborate to manage risks and strengthen the security and resilience of critical infrastructure. It uses an all-hazards risk management framework that addresses both physical and cyber threats. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf
Vulnerabilities	**1. CVE-2020-15368 - ASRock Motherboard AsrDrv103.sys Driver Vulnerability** https://nvd.nist.gov/vuln/detail/CVE-2020-15368 **2. OPC Unified Architecture Servers:** Known tools exist that can connect to OPC UA servers using default or compromised credentials. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a
Controls	**Preventative - Network Segmentation of SCADA Systems:** Organizations in the Dam Sector, such as the Tennessee Valley Authority, implement network segmentation to isolate SCADA networks from enterprise IT systems and the internet. This prevents unauthorized access, limits the spread of malware, and

	reduces attack surfaces for cyber intrusions. https://www.gao.gov/assets/gao-08-526.pdf **Detective - IDS:** IDS integrated into OT/ICS networks monitor dam operations in real time, detecting anomalies and potential cyber threats without disrupting critical processes. These systems enhance visibility and support secure, segmented network environments. https://industrialcyber.co/features/integrating-intrusion-detection-into-ot-ics-frameworks-can-build-network-activity-visibility-detect-potential-risks/
Incident Response	Organizations in the dam sector should regularly update their incident response capabilities using tools like CISA's Dams Sector Tabletop Exercise Toolbox, which offers customizable scenarios and planning resources tailored to sector-specific threats. In the event of an incident, CISA should be the first point of contact, along with WaterISAC, for coordination, intelligence sharing, and response support. https://www.cisa.gov/resources-tools/resources/dams-sector-tabletop-exercise-toolbox
Recent Incidents	**1. Bowman Avenue Dam, New York, 2013:** Iranian hackers obtained unauthorized access to the dam's SCADA systems. The attackers were able to monitor water levels, temperatures, and flow rates. Luckily, the control systems were offline at the time for maintenance, preventing physical damage. The cost of remediating the attack was over $30,000. https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged **2. Oroville Dam Spillway Failure – California, 2017** This is a physical incident where the spillway of the tallest dam in the U.S. suffered a structural failure due to poor design and maintenance issues, forcing the evacuation of around 188,000

	people downstream after a series of rainstorms. While not cyber-related, the incident does underscore the importance of physical asset monitoring and real-time communication systems in dam operations. https://damfailures.org/case-study/oroville-dam-california-2017/