Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 12| 2025

Review Article **Received:** 15-11-2025| **Accepted:** 10-12-2025 | **Published:** 23-12-2025

Cyber-Physical Systems Under Threat: A Case-Study Review of Recent SCADA Attacks in the U.S. Utility Sector

Benjamin Panful [1]***, Barnabas Apaflo*** [2] ***and Nasiru Hutchful*** [3]

[1] *Lake Land College, USA*
[2] *Texas A&M University*
[3]*Department of Computer Science and Engineering, University of Mines and Technology, Ghana*

Abstract: The case-study review focuses on United States-based breaches of supervisory control and data acquisition (SCADA) and operational-technology (OT) of utility systems, particularly of water and wastewater systems. We integrate four exemplary incidences which are Oldsmar, 2021; Aliquippa/Unitronics, 2023; rural Texas overflows, 2024 and Bowman Avenue Dam, 2013 based on technical advisories, peer and industry assessments, and authoritative reporting. A formal evidence hierarchy/extraction schema allows initial access vectors, SCADA/PLC touchpoints, process-level impacts, detection/response actions, and government communications to be coded uniformly. Cross-case findings reveal three pathways to OT impact recurrently: first is internet-exposed Human Machine Interfaces/Programmable Logic Controllers (HMIs/PLCs), commonly using default or weak credentials. Second is misuse of remote-access, such as vendor channels without multifactor authentication (MFA) and the last is Information Technology (IT) to OT interdependence that transforms enterprise intrusions into operational risk. Effects included near-miss chemical setpoint manipulation and local overflows; operators and manual fallback were important in detection and containment. Federal guidance translated into practice, we suggest a realistic control stack of small and mid-size utilities, zero external exposure, credential hygiene and MFA, segment IT/OT, vendor access hardened PLCs/HMIs, operator-focused monitoring and incident response, and simple readiness metrics. Weaknesses are uneven reporting to the public and attribution opaqueness. In general, the reported cases attest to the fact that utilities in the U.S. face credible SCADA-layer risk, and that prioritized, implementable controls can significantly decrease the probability of unsafe change of processes.

Keywords: SCADA, ICS/OT, Human–Machine Interface (HMI), Programmable Logic Controllers (PLC), Incident Response.

INTRODUCTION

In the U.S. utilities, cyber physical risk has become not just a theoretical issue but a trend of reported SCADA/OT intrusions with likely or near-miss process impacts. In February of 2021, an attacker remotely operated an operator control at a small Florida water utility and tried to raise a setpoint of sodium hydroxide using the HMI. The operator observed an abnormal cursor control and undid the switch and found out that thin staffing and remote-access equipment can be turned into a direct operation on the treatment procedures (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Kaufman *et al.*, 2023). Later technical and academic works present another point that small differences in attacker persistence or alarm spoofing would lead to materially bad results, highlighting why access administration and operator consciousness are significant (Cervini *et al.*, 2022; Kaufman *et al.*, 2023)

Getting to the end of 2023, several United States water and wastewater utilities that utilized Unitronics PLCs were breached, and federal warnings outlined exploitation vectors that included internet exposed devices that were default-protected or not password-protected and poor remote-access hygiene (CISA, 2023, 2024a). The timeline information and indicators provided by open-source incident reports related to the Aliquippa, Pennsylvania incident can help visualize how misconfigurations of commodities may leave PLCs and HMIs vulnerable to direct manipulation (SecurityScorecard, 2023; Steinbrecher, 2024). There were HMI manipulations in rural Texas water systems in early 2024, such as an overflow in Muleshoe and attempted compromise in towns that are close, an incident that highlights both the operational salience of such events and the dependency of the sector on manual fallback to control the deviation of processes (Miller, 2024). The historical timeline that prosecutors and media tend to use when discussing the topic is typically a longer one that traces back to the 2013 Bowman Avenue Dam intrusion, which proved that remote-access to small, municipally managed industrial assets have been a long-standing target, although the methods and intensity have changed (U.S. Attorney's Office, 2016; DFS, 2016; Yadron, 2015; Lach, 2016).

These were not the only incidents. Federal warnings highlight the rising rate of ill intent against critical infrastructure and, particularly, the

***Corresponding Author:** Benjamin Panful

DOI- https://doi.org/10.5281/zenodo.18030630

Water and Wastewater Systems (WWS) sector. The sector page developed by CISA also consolidates risks and resources specific to utility operators (CISA, 2025). Their 2021 joint advisory lists common tactics in spear phishing and ransomware staging in IT networks to abuse vendor and remote-access rings of entry into OT, and prioritized mitigations to resource constrained utilities (CISA, 2021). Living-off-the-land tradecraft, latent access, and a desire to target U.S. infrastructure have been highlighted by multi agency alerts on state sponsored pre-positioning (e.g., the "Volt Typhoon" campaign) and intelligence community reporting further highlights this (CISA, 2024b; CTIIC, 2024). This position was reinforced in 2024 with federal officials calling an attack on the water systems disruptive and encouraging utilities to act swiftly (Satter, 2024; CBS, 2024).

The concerns are reflected in industry and practitioner analysis. The Multiyear Operational Control system/Industrial Control Systems (OT/ICS) cybersecurity reports reveal a common exposure, internet accessible HMIs/PLCs, default credentials, flat or lax IT/OT segmentation, and brittle remote-access habits and report an increase in OT relevant incidents and attempted process manipulation (Dragos, 2025, 2021). Vendor case notes and sector blogs have further details of attacker activity and defender failures (Forescout Research, 2023); (OT Security News, 2024); (Caws, 2024). Simultaneously, peer reviewed literature demonstrates the overlap of structural vulnerabilities in SCADA spaces with detection gaps, and how water sector anomaly detection is currently developing towards processes capable of localizing and indicating process level deviations. Syntheses by Alanazi *et al.,* (2023) bring together the prevalence of insecure remote-access, default credentials and lack of network isolation in legacy deployments, and studies in water distribution anomaly detection show methods of detecting cyber instigated anomalies in hydraulic signals. These water sector findings are put in a wider critical infrastructure context by cross sector studies reminding us that utilities have suppliers, architectural patterns, and adversaries with other sectors, despite process physics differences (Glenn *et al.,* 2016; Sikder *et al.,* 2023). The same trends are evident in the energy sector, as digitalization of distributed assets has increased the attack site in a manner that is closely related to the challenges of water-sector SCADA integration (Chen *et al.,* 2025). Though most of the utilities continue to suffer mainly IT side of disruption, the above U.S. examples indicate that direct OT disruption, realized or narrowly escaped, is now publicly reported. The combination of legacy equipment, remote-access to vendors, and thin staffing common in small local entities and special districts fits the description of advisories and incident reports well and provides a broad attack surface that can be easily traversed with a reasonable amount of expertise. This paper is intended to present a case study review of SCADA/OT cases in U.S. utilities, triangulating technical advisories, peer reviewed analysis, and well-known press to reconstruct the attack unfolding, describe the impacted assets and process level effects in OT, analyze how it was detected, responded to, and communicated to the public and to derive practice ready controls and governance implications that are aligned to federal guidance on Water and Water Systems (WWS) operation (CISA , 2021, 2023, 2025; CISA *et al.,* 2024)

We examine four of the main cases, Oldsmar (2021), Aliquippa/Unitronics compromises (2023), Texas HMI manipulations (2024), and Bowman Avenue Dam (2013) that were chosen based on the reported OT touchpoints and evidence that can be triangulated. We uniformly code tactics and impacts, highlighting when evidence demonstrates SCADA/HMI/PLC-level interaction, but not IT only effects, and transform recurrent pathways, exposed devices, credential weaknesses, and remote-access abuse into a prioritized control stack which small utilities can realistically implement (Dragos, 2025; CISA *et al.,* 2024).

BACKGROUND & RELATED WORK

SCADA/OT in U.S. utilities

Water and wastewater systems (WWS) are based on supervisory control and data acquisition (SCADA) to oversee and activate treatment and distribution processes using field sensors/actuators, programmable logic controllers (PLCs) or remote terminal units (RTUs), local human machine interfaces (HMIs), SCADA servers and historians, and engineering workstations. These operational technology (OT) resources are becoming increasingly connected to information technology (IT) networks to report data, remotely operate, maintain their vendors and become interdependent (Hassanzadeh *et al.,* 2020). The sector guidance of CISA lays out this landscape and enumerates the exposure points that are typically common to plant managers and municipal leaders (CISA, 2025). Practitioner articles tail the same structure and

Publisher: SARC Publisher

highlight how governance, access control, and monitoring should grow as utilities become able to connect outside of plant walls (Stone, 2022; Goldstein, 2021).

Threat landscape and recurring attack pathways

Recent U.S. incidences and federal warnings all tend to converge on some few common initial access points. First, uncovered control equipment and HMIs over the internet can still be found and in far too many instances are secured with factory default or weak credentials. According to the CISA cybersecurity advisory, certain devices were accessible using default passwords or no passwords, and this fails to provide a security barrier between opportunistic scanning and process level tampering (CISA, 2023, 2024a).

Second, abuse of remote desktops by remote-access tools into persistent vendor channels offers adversaries HMI level control in case of weak or single factor authentication. The Oldsmar case demonstrates how the ability to remotely control an operator console can be directly translated into attempted setpoint changes despite operators reversing the change. The episode demonstrated how inadequate staffing and careless access can increase the risk (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021). Sector case notes explain similar mishaps that are misconfigured remote services, shared accounts, and restricted surveillance that is exploited by adversaries (OT Security News, 2024; Caws, 2024).

Third, state-sponsored pre-positioning uses living-off-the-land methods to merge into legitimate administration activity and create latent access. Although it is not water-focused, federal sources have clarified that this tradecraft is directed at U.S. critical infrastructure and may overlap with utilities through shared service providers and remote connectivity (CISA, 2024a; CTIIC, 2024). In 2024, the public warnings stated that disruptive attacks on water systems were still ongoing, which translated the technical risk into clear calls to action on the part of the operators and state partners (Satter, 2024; CBS, 2024).

Lastly, IT to OT pivot risks make it difficult to contain an incident since ransomware or credential theft in enterprise networks may slow down operations, ruin trust in data, or cause indirect pressure on OT. The cross-sector cases, like the Colonial Pipeline outage, show how outages in business systems can cause material impacts on energy services without necessarily having direct PLC manipulation (Olorunlana and Mohammed, 2025; Garden State Cyber Threat Highlight, 2021). This interdependence is important to utilities that outsource IT or cross-source identity infrastructure between IT and OT.

Standards and guidance shaping utility defenses

The water sector-focused CISA alert AA21 287A provides concatenated noted Tactics, Techniques and Procedures (TTPs) and offers prioritized mitigations, reduce the external exposure, eliminate default credentials, implement multi factor authentication (MFA) on all remote pathways, segregate networks to limit lateral movement, and enhance logging with OT context (CISA, 2021). The Unitronics alert and AA23 335A add targeted actions that involve eliminating devices off the public internet, altering defaults and tracking unauthorized configuration changes (CISA, 2023, 2024a). To prepare in case of an incident, the WWS Sector Incident Response Guide offers a utility-specific playbook that balances ICS forensics-related concerns and the needs of communicating with the community (CISA *et al.,* 2024). These materials are combined with assessment tools and contacts on sector pages that are available to assist municipal operators. Simultaneously, the strategic basis of the need to expedite base level controls is provided by intelligence and multi-agency material on state sponsored campaigns (CISA, 2024b, 2025; CTIIC, 2024).

Evidence base of academic and industry

Peer reviewed and industry research are also useful to supplement the advisories as they quantify the exposure patterns and suggest detection methods specific to water processes. An extensive survey of SCADA vulnerabilities emphasizes the prevalence of insecure remote-access, default passwords, and lack of network isolation in old systems (Alanazi *et al.,* 2023). Simultaneously, an article titled Cyber Attacks Detection in Water Distribution Systems shows anomaly detection methods that localize the cyber induced anomalies on the hydraulic signals, which are applicable in utilities that require process aware monitoring, and not perimeter only notifications (Sikder *et al.,* 2023). Studies on the U.S. electric industry indicate almost the same exposure patterns, insecure vendor networks, inadequate segmentation, and outdated equipment, indicating that cyber risk in the water sector belongs to a wider country-infrastructure issue, and not a isolated vulnerability

(Glenn *et al.,* 2016). Past water-utility intrusions empirical reviews indicate that most of them were exploited through the same structural vulnerabilities, demonstrating the persistence of these vulnerabilities over the past decade (Hassanzadeh *et al.,* 2020).

According to the practitioner perspective, the multi-year OT/ICS reports record an increasing number of OT related incidents and list the same systematic vulnerabilities: internet reachable HMIs/PLCs, poor credential hygiene, flat or permissive segmentation, and fragile remote-access routes (Dragos, 2025, 2021). Technical notes and sector blogs provide additional hardness with regard to attacks by hacktivist or patriotic groups that opportunistically exploit water facilities (Forescourt Research, 2023; Ribeiro, 2025; Perez, 2025). Although the technical quality of these sources differs, they all drive the same message as federal guidance and academic surveys, therefore exposure reduction, credential hygiene, MFA, segmentation, PLC/HMI hardening, and process aware monitoring are the ultimate near term priorities to focus on in small utilities.

Synthesis and implications to our case review

This is the background that drives our case study protocol design. Since both advisories and empirical reporting are dominated by exposed devices, credential weaknesses, and remote-access misuse, our extraction schema specifically captures access vectors and authentication posture, the specific OT assets accessed (HMI, PLC, engineering workstation), process level effects (setpoints, valves, pumps), the role of human operators in detection and the role of human operators in post incident communications and government actions. Mapping such elements between cases allows us to trace how such weaknesses appear in small and larger utilities and transform recurring TTPs into a prioritized control stack consistent with the mentioned sector guidance.

CASE-STUDY METHODOLOGY

Research questions and logic design

We aim at an organized review of case studies that would recreate the process by which U.S. utility incidents got to the SCADA/HMI/PLC assets, the effects of the process level that was attempted or achieved, and the response of the operators and agencies. According to federal recommendations, which list repetitive routes, exposed devices, weak credentials, and remote-access abuse (CISA, 2021, 2023, 2024a), we pose the following question:

RQ1: What are common access vectors and methodologies across incidents, and what is their intra-OT penetration?

RQ2: What OT components (HMI, PLC, engineering workstation, historian) were manipulated and by what process level intentions (e.g., setpoint manipulation) did they do it?

RQ3: Which intrusions were detected and contained and what operator actions (manual overrides, shutdowns) were decisive?

RQ4: What is the development of public communication and government response (alerts, enforcement, guidance) during and after the incidents?

Case selection and scope

We encompass incidents that meets the following criteria; (i) U.S. utility (with a specific focus on water/wastewater systems); (ii) reported SCADA/OT touchpoints (HMI/PLC interaction or configuration effects) but not IT only effects; and (iii) triangulated by at least two types of sources among government advisories/official statements, reputable media, peer reviewed or industry/forensic reports. The Oldsmar intrusion fits the requirements by means of the contemporary media and the case material in detail (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Kaufman *et al.,* 2023). The compromised Unitronics/PLC fulfill them through federal alerts and independent reporting (CISA, 2023, 2024a; SecurityScorecard, 2023). National wire reporting applies to the Texas HMI manipulations (Miller, 2024). We consider Bowman Avenue Dam intrusion of 2013 as one of the historical comparators with primary documentation (U.S. Attorney's Office, 2016) and secondary press (Yadron, 2015).

We skip both incidents that are exclusively IT side and have no plausible route to OT found in the literature, and those that are paywalled media but not primary unless substantiated by official or technical documents (e.g. WSJ and DOJ SDNY).

The cases covered a time between 2013-2025. This window encapsulates the Bowman precedent through the most recent warnings issued by the water sector such as state sponsored pre-positioning campaigns (CISA, 2024b; CTIIC, 2024).

Typology of sources and evidence hierarchy.

To control credibility and specificity in the process of synthesis, we categorize sources into four levels:
Tier 1 (Primary/Official): Government recommendations and official announcements containing technical or legal details, CISA sectoral and incident-related sources, collective notices and press (CISA, DOJ, DFS CTIIC, etc.).

Tier 2 (Peer reviewed / formal studies): Scholarly articles and cross sector analyses that extrapolate vulnerabilities or suggest ways to detect them.

Tier 3 (Industry/practitioner): Year in review and technical briefs that provide counts of incidents, patterns of exposure, and practitioner controls.

Tier 4 (Reputable media): AP, Reuters, CBS, WIRED, etc. to get the timeline of incidents and the story of their impact on the population.

In case there is a clash in claims, the Tier 1 sources prevail, then Tier 2. Tier 3 and 4 gives context, color and corroboration but are not utilized to override primary documentation.

Data extraction schema

For each case we extract variables that map directly to observe failure modes and operator actions in our sources. We concentrate on the context of the system, events, the initial access/authentication position, the OT components accessed, process level impacts, detection and response, impact, government and public communications and the strength of the evidence.

Reliability, limitations and dealing with uncertainty

Public reporting differs when it comes to technicalities. We reduce this by cross-tiering, giving preference to primary technical documentation with respect to OT specific claims, and being conservative in the case of OT interaction that is implied, but not demonstrated. The enrichment of context is done by using narrative media (e.g., WSJ; The New Yorker) only when it is backed by official releases or technical advisories. The cross-sector events with a robust IT side impact, but indirect OT, (e.g., Colonial Pipeline) can inform our concept of IT to OT interdependence without overemphasizing process manipulation (Olorunlana and Mohammed, 2025; Garden State Cyber Threat Highlight, 2021).

CASE PROFILES

Oldsmar Water Treatment (Florida, Feb. 2021)

This is a small municipal treatment plant, complete with Operator work stands/HMIs. You can access these machines remotely and adjust the settings, like chemical dosing and other setpoints. One operator observed his cursor being taken over remotely, then lost control of his local setup for a short interval. The next moment there was a rapid change in sodium hydroxide (NaOH) setpoint to an unsafe level, he was able to get it back to its previous value. Public release followed within days, while local hardening was implemented (Greenberg 2021; Kaufman et al. 2023). Reporting points to misuse of remote-access tooling and permissive access practice that let an adversary interact with an HMI session. The case illustrates weak authentication, common passwords, and limited monitoring as amplifiers of risk (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Cervini *et al.*, 2022). In controlling chemical injections, the adversary manipulated an HMI remotely. He tried to raise the setpoint for NaOH (lye). The operator fixed this immediately with no downstream damage resulted (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Kaufman *et al.*, 2023).

Decisive human detection (observed cursor movement, setpoint change) was involved. The plant reportedly disabled or restricted remote-access, reviewed credentials, and increased local supervision (Kaufman *et al.*, 2023). With no physical harm reported, the incident remained a near-miss event. The episode has now become characteristic of small utility exposure and operator-centric last line defense (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021). The case drove nationwide attention, as well as subsequent sector advisories emphasizing credential hygiene, exposure reduction, and MFA on all remote pathways (CISA, 2021, 2025). The evidence of this event is high since multiple contemporaneous media and detailed teaching materials concur on HMI manipulation, operator detection, and rapid reversal (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Kaufman *et al.*, 2023).

Aliquippa Water Authority / Unitronics PLC Compromise (Pennsylvania, Nov. 2023)

This is a facility that uses Unitronics PLCs for water treatment and distribution. Some devices were accessible from the internet with default or weak credentials, according to federal advisories

Publisher: SARC Publisher

(CISA, 2023, 2024a). In late November 2023, a breach was reported at a booster station by the Aliquippa Water Authority. Federal and state entities issued alerts with mitigations. Open-source reporting summarizes indicators and the sequence of events. (Steinbrecher, 2024; SecurityScorecard, 2023).

Advisories describe enemies scanning for internet-reachable Unitronics PLCs/HMIs and logging in with default or no passwords, followed by defacement or configuration access. So, in this case also, weak remote-access hygiene (no MFA, shared credentials) created the problem and exposure (CISA 2023, 2024a). Thus, reporting is primarily centered on PLC-level access and interface defacements. While widespread physical damage has not been confirmed, the ability to access a zone full of PLCs to change logic or setpoints directly poses a process risk (CISA 2023; SecurityScorecard 2023).

The local operators isolated affected equipment, where necessary and reverted to manual operations. Against this sort of attack, advisories call for immediate removal of devices from public networks, password changes, and where possible, enabling MFA (CISA, 2023, 2024a). Service disruptions were limited but the reputational and regulatory impacts were not trivial. The incident triggered a series of sector-wide hygiene actions across similarly configured utilities (SecurityScorecard, 2023; CISA 2023). This occurrence is part of a larger trend toward state-aligned campaigns against America's critical infrastructure. It is a timely reminder that even small utilities can be nation-state target (Christello 2024).

A rapid publications, alerts and broader joint advisory listed these mitigations and reenforced controls over credentials and exposure reappearance (CISA, 2024a). The evidence on this was strong for exposure conditions and countermeasures due to the official reports but also moderate in degree for detailed OT manipulation because of varying open-source materials. This evidence was collected over official advisories and various independents incidents notes.

Rural Texas HMI Manipulations and Overflow (Jan. 2024)

This is a small municipal system using HMI for controlling storage tank levels and pump switches. Because of inadequate staffing, remote monitoring of equipment is common here (Miller, 2024). In January 2024, Muleshoe Municipal Water District reported that an unauthorized HMI manipulation caused an overflow, and nearby towns (Hale Center and Lockney) reported attempted compromise. Operators immediately switched to manual control while inspections were made (Miller, 2024).

Reports from the public indicate the use of remote manipulation of HMI. The technicalities are vague, but the pattern aligns with themes from federal advisories like exposed services or credentials (CISA, 2021). Changes to HMI resulted in wrong tank/pump states and Muleshoe Overflow. At that point, it took manual intervention to stop further effects (Miller, 2024). Operators then used manual operations to handle any changes in tank levels or alarms until cleanup and reinforcement could begin. Public announcements and consultations with state and federal personalities followed (Miller, 2024).

No poisoning or danger reported. The focus was coping with the aftermath and informing the public about what had happened (Miller, 2024). National news compounded warnings already issued by federal agencies about harmful internet attacks on public utility systems (Satter, 2024; CBS, 2024). AP gave strong news on the overflow, and subsequent need for manual action. The technical vectors suggested in AP news fits advisories report (Miller, 2024).

Bowman Avenue Dam Intrusion (Rye Brook, NY; 2013)

The Bowman Avenue Dam is a small facility designed to control flooding, its supervisory control and data acquisition (SCADA) system allowed keep and monitor conditions remotely over a sluice gate, which is common to most municipality-based industrial control systems (ICS). It leans heavily on remote connections to gain efficiency and outsource routine maintenance (U.S. Attorney's Office, 2016; DFS, 2016). According to the federal charging papers unsealed in March 2016, some actors got unauthorized access to the dam's SCADA system in 2013. Later, this was spotlighted as part of a broader campaign that included disruptions to the financial sector (U.S. Attorney's Office, 2016). Subsequent reports clarified that for the period of intrusion, the dam's sluice gate actuator was offline undergoing maintenance which diminished possibility for moving from screen level access into physical activity (Yadron, 2015; Lach, 2016).

Publicly available documents agree that a remote connection to the control interface exists, but don't detail the exact access weakness or boundary exposure (U.S. Attorney's Office, 2016). Nevertheless, this episode illustrates a typical municipal risk for ICS. When endpoints are reachable over the internet or remote channels are poorly governed, motivated actors can find out and probe them easily when there is weak credential hygiene and network boundaries (DFS, 2016; (Yadron, 2015). The target was the sluicegate control via the dam's SCADA/HMI. As the motor control circuitry for the gate was cut off due to maintenance, touching the screen did not result in any movement of the gate or changes to water level (Yadron, 2015). As summarized by the New York Department of Justice (DOJ), the actor who carried out the Rye Brook cyber-attack acquired unauthorized access to remote control systems in Bowman Avenue Dam New York (U.S. Attorney's Office, 2016). This determined a way of manipulating physical processes under normal conditions. A federal investigation eventually revealed how intruders had gained access to the dam and how it was just one part of a broader operation. Local officials worked with their federal partners to examine remote-access and monitoring policies (U.S. Attorney's Office, 2016; DFS, 2016). Also, news reports on this incident encouraged city managers to reassess their vendor channels, modem exposure, and minimum authentication standards (Lach, 2016).

There weren't any physical effects reported at the dam because the gate was offline during the intrusion. Nevertheless, the case had broad legal symbolic and policy consequences. It became an early concrete instance of remote-access to a local ICS in the USA which helped to frame subsequent risk communications about small-asset exposure (U.S. Attorney's Office, 2016; DFS, 2016). DOJ charging statements and regulator linkage both presented Bowman as a cautionary account of how cities were at risk from external points. They insisted that the essentials must be strengthened, limiting outside probing and maintaining strict authentication for any remote entry (U.S. Attorney's Office, 2016); DFS, 2016). The evidence of this case is strong for the facts of remote SCADA access and lack of physical consequences according to official pronouncements. The exact access method and technical specifics are not public. Separate sources tell the same story. (U.S. Attorney's Office, 2016; DFS, 2016; Yadron, 2015; Lach, 2016).

CROSS-CASE PATTERNS & IMPACTS

Attack pathways that repeatedly enabled SCADA/OT reach

In Oldsmar (2021), Aliquippa/Unitronics (2023), rural-Texas (2024), and Bowman Dam (2013), access conditions repeat. First, HMIs and PLCs exposed to the Internet were accessible or became accessible via simple remote-access routines. According to federal warnings about Unitronics, there was compromise exploited devices online with default or no passwords, hence collapsing the barrier between opportunistic scanning and process-level interaction (CISA, 2023: 2024a). Second is the improper use of remote-access to controls at the HMI level precisely the same thing that was observed in Oldsmar, where an operator saw a remote cursor move and a NaOH setpoint rapidly increased before he reversed it (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021). Thirdly, state-sponsored pre-positioning relied on living-off-the-land techniques to blend into administrative activity and hold critical infrastructure at risk (CISA, 2024b; CTIIC, 2024). Finally, the IT/OT interconnection made business-system hacks or credential thefts possible to undermine operations or set conditions for OT access even where direct PLC manipulation was not confirmed (Garden State Cyber Threat Highlight, 2021; Olorunlana & Mohammed, 2025).

OT targets and process-level effects

The first observable point of manipulation in Oldsmar was the HMI (setpoint change for sodium hydroxide). The same applies with Texas incidents (tank/pump states leading to an overflow). It illustrates how display/control surfaces can become the effective point of insertion for an assailant when there are weak credentials and too much exposure (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Miller, 2024). In Aliquippa and related events involving Unitronics, PLC-level access and defacement of the interface were reported. Even lacking a strong confirmation, sustained logic changes, to modify setpoints or ladder logic is a direct path for process deviation (SecurityScorecard, 2023; CISA, 2023). At Bowman Dam, there was SCADA reach to a sluicegate control but no physical actuator for it because the actuator was off-line. It serves as an important reminder that physical state can mitigate cyber reach within specific windows (U.S. Attorney's Office, 2016; Yadron, 2015). Industry trend studies reinforce that attempts at process manipulation, not just IT outages, have taken up more of the recent accounts (Dragos, 2025; 2021).

Detection and response patterns

Detection was highly reliant upon human operators and manual backups. At Oldsmar the rogue cursor and unusual set point had to be detected by the operator, the system had no ability to defend itself. Texas depended on operators becoming aware of abnormal tank-level states and reverting to manual procedures (The Consortium of Cybersecurity Clinics, 2025; Miller, 2024). Post-event activities concentrated on ways to decrease exposure (unplugging devices from the public internet), resetting passwords (eliminating defaults), and turning multifactor authentication on all remote-access lines, which was prioritized by various U.S. federal advisories (CISA, 2021, 2023, 2024a). The WWS Sector Incident-Response Guide provides specific guidance for utility-craft audiences that involves containment, forensic preservation in an ICS networked environment, and a unified message during public communications (CISA *et al.*, 2024).

Observed impacts across incidents

In the classification of these events by their impacts, we come to see four general types of situations. First are process deviations or near-misses. Oldsmar eliminated the NaOH spike before any customer was given contaminated water; Muleshoe reported an overflow but managed to contain it (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Miller, 2024).

Second is operational disruption and manual mode. Both Aliquippa and Texas shut down to manually manage the situation (SecurityScorecard, 2023; Miller, 2024).

Reconnaissance and public relations were another impact in consequence. Events brought out advisories and increased awareness from federal and local safety partners (CISA, 2021, 2022, 2024a; U.S. Attorney's Office, 2016; DFS, 2016).

Finally, there was sector level risk signaling. Alerts emphasized ongoing attacks against water systems, transitioning technical hazards into a demand for policy priorities (Satter, 2024; CBS, 2024).

Research and engineering implications

According to the recent peer-reviewed survey, there's a high likelihood at many local resource-constrained utility companies that there are still vulnerable remote-access, default credentials and weak isolation (Alanazi *et al.*, 2023). Process-aware detection is still a promising complement to perimeter hygiene. Sikder et al. (2023) show how hydraulic signals can be examined to localize cyber-induced anomalies which offer a way to spot subtle process drifts before they become incidents. A cross-sector analysis of US electric power systems suggests that remote-access, vendor ecosystems, and legacy constraints are sources of common risk. This shows that the remedies for utilities can be used across various sectors of the industry (Glenn *et al.*, 2016).

CONTROLS, MEASUREMENT & PRACTICE

A prioritized control stack for small and mid-size utilities

The four U.S. case studies together with the federal advisories converge on a concise set of high leverage controls that, can significantly reduce the chances of HMI or PLC access escalating into unsafe process changes if consistently applied. Each measure has an implementation order priority and alignment with national guidance.

The first of the top priorities is to prevent external exposure of control assets. Many incidents begin with internet-reachable HMIs, PLCs, or unprotected remote services. The utilities have the first task of cataloging every public-facing endpoint, disconnect them out of direct internet connectivity, and channel any remaining connection by using brokered gateways which are highly authenticated and has activity logging (CISA, 2023, 2024a). Devices have been documented in federal advisories severally about their exposure on the internet with defaults or no passwords, which depicts how weak barriers can enable the control logic to be manipulated by adversaries. Sector analysis by SecurityScorecard (2023) and CISA (2025) repeat this exposure pattern in various utilities.

It is also essential to have a high level of credential hygiene and multifactor authentication (MFA) on every remote pathway. The Oldsmar incident proved the ability of permissive remote-access to move from screen control to chemical process manipulation. The same remedial actions are emphasized by the Consortium of Cybersecurity Clinics (2025), Greenberg (2021) and CISA (2024a), delete default credentials, use individual logins, and enable MFA in all remote channels, including vendor and maintenance access.

The third control priority will be to separate IT and OT and reduce inter-zone trust. In the case where attacks are initiated in enterprise IT systems, they may put operational pressure on OT or facilitate the horizontal movement towards key assets. Segmentation with defined conduits, allow-listed flow of data to historians and engineering workstations and explicit cross-zone authentication monitoring requests are fundamental protection mechanisms (CISA, 2021; Garden State Cyber Threat Highlight, 2021; Olorunlana and Mohammed, 2025).

Utilities need to also harden the PLCs, HMIs and pathways vendors use to access their systems. Any unnecessary services should be disabled, configuration interfaces restricted, and alarm set up to trigger upon change the ladder logic on programs. Vendor accounts should have time limits and be closely watched. These measures address the vulnerabilities shown in Oldsmar and Unitronics compromise (CISA, 2023, 2024a; Consortium of Cybersecurity Clinics, 2025; SecurityScorecard, 2023).

Another part of the control stack is producing an operator-focused monitoring and incidence response framework. In smaller utilities, operators often serve as the best detection layer. Alarms should be configured to flag unrealistic setpoints or errors that show in tank levels, while staff periodically practice manual fallback operations and evidence retention procedures specifically for ICS systems (CISA *et al.,* 2024). Examples from Texas and Oldsmar show how humans identifying problems and decisive manual intervention rounded off potential harm (Miller, 2024; Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021).

Lastly, utilities must have continuous exposure management as well as trend tracking. OT/ICS cybersecurity year-in-review analysis report reveal both the growing frequency of OT-relevant attacks and the re-use of characteristic exposure motifs. Steady comparison against such trend data lets you proactively prioritize and validate controls in place (Dragos, 2025, 2021). In practical terms, one can follow the journey from a fresh start to full maturity by detailing the trajectory as good to better to best. This pathway is shown in the table below;

Table 1 Progressive OT Security Maturity for Small and Mid-Size Utilities

Maturity Model	Focus	Practices and Capabilities
Good	Establish immediate defenses and basic operator awareness	Eliminate all public internet exposure of HMIs/PLCs. Change all default credentials. Enforce multifactor authentication (MFA) on remote desktops and VPNs. Conduct regular operator tabletop exercises for incident recognition and response.
Better	Strengthening access control and operational resilience	Implement brokered vendor access with time-bound permissions. Enable active configuration-change alarms on HMIs and PLCs. Introduce basic IT/OT network segmentation. Verify and periodically test backup-and-restore procedures for all control equipment.
Best	Integrate proactive monitoring and adaptive protection	Conduct continuous external attack-surface monitoring. Deploy privileged-access management for all OT accounts. Engineer strict allow-lists governing inter-zone communication. Adopt process-aware anomaly-detection and analytics tools for real-time visibility.

Scientific analyses of the SCADA firewall configuration show that strict use of conduits and monitoring for any changes will greatly reduce the opportunities for intruders to move around within the environment (Ranathunga *et al.*, 2016)

In summary, all these measures translate national advisory warnings into steps that are both actionable and scalable at levels of control which small- to medium-sized utilities can handle and afford, attacking the very areas of vulnerability exposed by recent SCADA/OT incidents.

Implementation constraints and workable paths
In the small utilities, lack of dedicated OT safety staff means vendors are responsible for security and integrators handle their maintenance. This can be handled by prioritizing access governance (unique identifiers, limited windows for vendor access, MFA) and insisting on basic safety standards from vendors (CISA, 2024). We also examine older equipment and the consequent risks of downtime. Older PLCs and HMIs often won't interface with modern controls. Make up for this with network-level security (segmentation, firewalls), human operators constantly monitoring and validating backups rigorously (CISA, 2021; CISA et al, 2021).

Another constraint on implementation is signal-to-noise in alarms. A high nuisance alarms ladder drowns weak signals. Set up a small number of process-plausibility rules (e.g. step-change caps on dosing setpoints) and accompany them with operator training. Oldsmar and Texas show such cues trigger manual fallback (The Consortium of Cybersecurity Clinics, 2025; Miller, 2024; CISA et al 2024). Shared risk with other industry sectors also exists. Nation-state adversaries that preposition in U.S. critical infrastructure raise the baseline threat and may exploit common providers (CISA, 2024b). Anticipate TTPs through industrial sector initiatives and federal outreach (Satter, 2024; CBS, 2024).

Engineering and Research Directions
Peer-reviewed syntheses confirm that insecure remote-access, default credentials, and weak isolation are systemic across SCADA deployments (Alanazi *et al.*, 2023). There are two directions that stand out. One of which is process-aware detection and operator decision support. Papers such as Cyber Attacks Detection in Water Distribution Systems Using Deep Learning explain how hydraulic signals can reveal cyber-induced anomalies ahead of any cascade (Sikder *et al.*, 2023). By embedding those analytics in HMIs, coupled with clear operator prompts and playbooks from the CISA et al. 2024 team, mean time to identity (MTTI) can be reduced. Still on the horizon are studies showing how the digital twin can be mobilized to simulate attack scenarios as well as train operators, a tactic that may strengthen readiness amongst small utilities (Ta, 2025).

The other direction is secure remote-access patterns for PLC/HMI maintenance. Trust patterns that are coming up trust (brokered access, ephemeral credentials, out-of-band approval) directly addresses the Unitronics vulnerabilities seen in practice while remaining sensitive to the realities of small utilities (CISA, 2023, 2024a).

Trends can change from year to year so continuous review of OT cybersecurity trend data is essential for planning. Each year, utilities should be ready to direct remediation efforts at the most pressing vulnerabilities by understanding which attack patterns are growing more common (Dragos, 2021; Dragos, 2025).

POLICY & GOVERNANCE RESPONSES

Federal posture after recent incidents
As published breaches in water utilities continued to grow outwardly, U.S. federal advisories and alerts focused more on this sector. CISA's water and wastewater sector page (WWS) is leading content for WWS operators, municipalities who face cyber challenges, an entry point to assessments, advisories, and response coordination (CISA. 2025). In the aftermath of Oldsmar and later events, a joint advisory for WWS aggregated common tactics like phishing into enterprise IT, misuse of remote-access, and weak vendor links; mitigation methods ideal for resource-constrained water systems were thus identified as well (CISA, 2021). When multiple U.S. facilities using the Unitronics controllers were hit in the latter part of 2023, CISA issued a focused alert and practical steps (remove internet exposure, change defaults, enable MFA, log and monitor configuration changes), and a cross-agency advisory pointed out that some devices were reachable with default or no passwords reducing the gap from discovery to action (CISA, 2023, 2024). In parallel, pre-positioning campaigns sponsored by nation-states (e.g., Volt Typhoon) were identified as having strategic objectives which could blend with administrative activity and maintain hidden access to infrastructure (CISA, 2024b; CTIIC, 2024). In 2024, senior officials publicly warned that certain attacks targeting water would be disruptive and urged collective action hence technical advisories became directly relevant to policy urgency (Satter, 2024; CBS, 2024).

Publisher: SARC Publisher

Incident Response, Disclosure, and Communications

CISA, FBI and EPA's WWS Sector Incident-Response Guide tailors incident response to this particular area (Water sector). It pairs ICS-aware evidence collection along with a task list that includes isolation, manual backups, restoration and public communication, all of which can be difficult in small utilities (CISA *et al.*, 2024). Legal framing from Bowman Avenue Dam, public charging documents and regulator statements of account show how official reparations define jurisprudence and define the Municipal OT attack landscape (U.S. Attorney's Office, 2016; DFS, 2016). Media accounts amplify these signals for political audiences (Yadron, 2015; Lach, 2016).

Post-incident threat-specific briefings enable public sector operators to contextualize observed tactics and reinforce baseline controls that have immediate policy implications (Forescout Research, 2023). Sector commentary surveys (e.g., WISDIAM, CloudRange) also raise public-aware leadership and governing professionals' awareness of system-specific mistakes (Caws, 2024); (OT Security News, 2024).

Governance: translating advisories into implementable policy

At the utility governance level, the advisories are divided into four areas of policy domain. Policy on exposure management: Perform routine inventories of the public-facing services, plus discarding off any chance the internet interfaces of HMIs/PLCs unless brokered through an authenticated, logged gateway. It is reviewed at every security update (CISA, 2023, 2024).

Identity & access governance: Make sure default credentials are discarded and demand that MFA always be used on every remote path, including vendor and integrator access, with time-boxed approvals and account ownership clarity (CISA, 2021, 2023, 2024a).

Network trust and change control: Demand documented IT/OT segmentation and allow-lists for inter-zone communications; also govern change type it's alarmed and reviews any modification made to the configurations of a PLC or HMI (CISA, 2021, 2024).

Incident readiness and public communication: Adopt the WWS IR Guide playbooks and at least once a year, rehearse manual fallback and communications plans. Also, define thresholds for public notification and regulatory involvement (CISA *et al.*, 2024)

These domains accord with broader federal critical-infrastructure messaging and are supported by threat reports tracking the persistence of exposures and weaknesses (Dragos, 2025, 2021). According to trade and policy publications, legislators and agencies continue to debate OT-specific gaps as well as funding and the conversation has shifted from awareness to implementation (Ribeiro, 2025; Perez, 2025).

Now federal advisories, sector playbooks, and strategic warnings (CISA, 2024a; CTIIC, 2024) together give an integrated policy scaffold. Boards and city managers may operate it with four mandates: zero external exposure of control assets; remove default credentials, everyone uses MFA; enforced IT/OT segmentation and configuration-change governance; rehearsed incident response and public-communication plans. The larger policy reflected in national media and industry commentary has moved from "if" to "how fast" small utilities are adopting these basics (CISA, 2021, 2022; CISA *et al.*, 2024).

LIMITATIONS & THREATS TO VALIDITY

Evidence availability and reporting bias

There are an uneven public record of incidents and their outcomes in small communities. Many water and sewer operations do not have the resources to post detailed after-operations critiques of their own functioning, at times agencies simply withhold information when an investigation is still going on. In addition, part of the debate behind all this is how trustworthy these open sources are, and while there has been an emphasis on other aspects of continuing disruption to water system in federal briefings due further attention needs to go into the technical explanation of this disturbance, as well (Satter, 2024 CBS, 2024). Assessing sources strategically further indicate state sponsored pre-positioning in U.S. critical infrastructure, implying that some compromises may remain undisclosed (CISA, 2024b; CTIIC, 2024). The WWS Sector Incident-Response Guide also highlights the communications pressures that can limit the granularity of public narratives during response (CISA *et al.*, 2024).

Attribution and TTP granularity

Most official documents usually confirm unauthorized access but do not give technical details-even when constraints on the use of intelligence data have not been observed. In high-profile cases regulated by statute (e.g., Bowman Dam), where remote SCADA access was proven, the actual mechanism was not disclosed (U.S. Attorney's Office, 2016). Targeted advisories also emphasize conditions like "default or no passwords" and general mitigations rather than a detailed statement of the steps that the attackers followed from original intrusion through to takeover (CISA, 2023, 2024). This precludes fine-grain mapping for ICS and requires taking a conservative view of things.

Verifying OT impact vs. IT-side disturbance

Open sources can sometimes mix enterprise (IT) disruption with Process level (OT) manipulation. Our cases include both near-miss OT (a rise of Oldsmar 's sodium hydroxide setting which was brought back down by operator) and confirmed physical effects (Texas overflow) with little technical detail (The Consortium of Cybersecurity Clinics, 2025; Greenberg, 2021; Miller, 2024). Thus “HMI cursor/control observed” and “PLC interface defacement” go down as SCADA- touch points, but not necessarily into sustained logic alteration unless the record says so (SecurityScorecard, 2023).

Media and practitioner-source bias

The media can help pin down when events occur, but they tend to simplify things from the technical point of view. Blogs put out by vendors and pieces in trade press can emphasize standards aligned with product or policy agenda (Forescout Research, 2023; Ribeiro, 2025; Perez, 2025). We therefore put vendor/press as secondary sources in our synthesis and are looking for corroboration from tier-1 sources.

Selection, timeframe, and generalizability

The review window (2013–2025) combines both recent strides and historical precedent, but it lacks the ability to cover every post-incident event for vulnerable US utilities. Concentrating solely on four triangulable cases risks neglecting the interests of electric/gas utility firms, and large multi-sited operations. We partially address this by referencing cross-sector studies that report analogous exposures in the electric sector (Glenn *et al.*, 2016). The discoveries of this investigation are most useful for small to medium-sized American utilities that rely on remote transability and have legacy equipment.

Temporal instability and trend interpretation

Knowledge, adversary tradecraft and exposure patterns evolve. OT/ICS Cybersecurity yearly reviews detail shifting event mixes and new exposed assets as pages of advice are also revised over time (Dragos, 2025, 2021; CISA, 2025). Our interpretation is based precisely on the reported date of each document and should be re-visited as advice is re-evaluated.

Safeguards applied in this study

We limited over-reach by (i) at least two sources for every case; (ii) a conservative approach to coding when OT interaction was only implied but not proven with evidence; (iii) distinguishing IT outages from SCADA/HMI/PLC impacts; and (iv) a hierarchical system that is, the evidential weight of government or official documents. In cases of doubt, we explicitly marked the relative strength of evidence in each case.

Ethical and legal restraints

Some details are restricted due to law-enforcement sensitivity or due to obligations of privacy concerning affected communities. The Bowman Dam case demonstrates how legal filings show physical access yet refrain from specifying technical details (U.S. Attorney's Office, 2016.) Our approach therefore respects these considerations and eschews any hypothetical re-building. Public sources provide a strong, practice-oriented synthesis, however incomplete TTP detail, inconsistent reporting and evolving advisories need to be treated with care and kept current. By following official advisories, comparing these with peer-reviewed material from reputable writers, and coding OT damage conservatively, we reduce but do not eliminate this set of threats.

CONCLUSION

The utility accidents in the United States are proof that adversaries can and do sometimes reach SCADA/HMI/PLC layers. When things go right, that usually result in near misses (Oldsmar); when they do not, there is a localized process effect (Texas overflow). In all these cases, three pathways are alike. They all occur through unfettered access to the internet, weak or default credentials, and abused remote-access. Even under these contingency conditions, operators and manual fallback remain the detective apparatus, demonstrating further the still the detective apparatus, demonstrating further an ongoing requirement for tailored alarms and trained responders. Federal advisories and sector playbooks now add support; what is needed is to convert these into rules and standards. Presently, pragmatic basic ideas for small utilities are clear,

Publisher: SARC Publisher

eliminate external exposure on all remote paths, strictly enforce credentials and MFA. Segment IT/OT, harden PLCs/HMIs (including vendor access), and measure readiness with simple KPIs. Future progress must join these essentials to a device which is aware of process and can thus be used for detection, along with more standardized incident reporting.

REFERENCES

1. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues." *Computers & security* 125 (2023): 103028.
2. Caws, J "11 recent cyber-attacks on the water and wastewater sector." *Wisdiam.* (2024).
3. CBS. **"**Cyberattacks on water systems are increasing*," EPA warns, urging utilities to take immediate action***.** (2024).
4. Cervini, J., Rubin, A., & Watkins, L. "Don't drink the cyber: Extrapolating the possibilities of Oldsmar's water treatment cyberattack." *International conference on cyber warfare and security*. Vol. 17. No. 1. Academic Conferences International Limited, (2022).
5. Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., & Debbabi, M. "Cybersecurity of distributed energy resource systems in the smart grid: A survey." *Applied Energy* 383 (2025): 125364.
6. Christello, G. (2024). The Rise of Iran's Cyber Capabilities and the Threat to US Critical Infrastructure.
7. CISA, P. "State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure." (2024).
8. CISA. "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." (2021).
9. CISA. "Water and Wastewater Systems." (2025).
10. CISA. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities". (2024).
11. CISA. "Exploitation of Unitronics PLCs used in Water and Wastewater Systems" (2023).
12. CTIIC. "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024." (2024).
13. Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), & Environmental Protection Agency (EPA). "Federal Roles and Resources for Cyber Incident Response." *Water and Wastewater Systems Sector* (2024).
14. Department of Financial Services (DFS), NY. "Statement from Governor Andrew M. Cuomo on Cyber Attack Charges Announced by U.S. Attorney General Loretta Lynch and FBI Director James Comey Involving the Bowman Avenue Dam in Westchester County*"* (2016).
15. Drados. "OT/ICS CYBERSECURITY REPORT." *8th Annual Year In Review 2025.* (2025).
16. Dragos. "Executive Summary. ICS/OT Cybersecurity." *Year In Review 2021* (2021).
17. Forescout Research., Vedere Labs. "Hacktivists attack U.S. water treatment plant – analysis and implications." (2023).
18. Garden State Cyber Threat Highlight. "Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategie." *Cybersecurity & Communication integration Cell. NJ.* (2021).
19. Glenn, C., Sterbentz, D., & Wright, A. "Cyber threat and vulnerability analysis of the US electric sector" *(No. INL/EXT-16-40692). Idaho National Lab.(INL), Idaho Falls, ID (United States).* (2016).
20. Goldstein, P. "Cybersecurity Lessons Utilities Can Learn from the Oldsmar Water Plant Hack." *Utilities can take steps to shore up their defenses and protect operational technology from cyberattacks*. BizTech. (April 2021).
21. Greenberg, A. "A hacker tried to poison a Florida city's water supply, officials say." *Wired. com* 2 (2021).
22. Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. "A review of cybersecurity incidents in the water sector." *Journal of Environmental Engineering* 146.5 (2020): 03120003.
23. Kaufman, E. K., Adeoye, S., & Batarseh, F. A. "Leadership for cyberbiosecurity: The case of Oldsmar water." (2023).
24. Lach, E. "Cyber War Comes to the Suburbs*." The NEW YORKER.* (2016).
25. Miller, K. "Rural texas towns report cyberattacks that caused one water system to overflow." *AP News* (2024).
26. Olorunlana, T., & Mohammed, H. "Analysis of the Colonial Pipeline Cybersecurity Incident." (2025),
27. OT Security News. "Analysis of a Water Treatment Plant Attack." *Lessons Learned for*

Publisher: SARC Publisher

Mitigating Threats to Industrial Control Systems. Cloud Range. (2024).

28. Perez, J. “Cybersecurity Snapshot: *Expert Advice for Securing Critical Infrastructure’s OT and Industrial Control Systems, IoT Devices and Network Infrastructure.* Tenable. (September 2025).
29. Ranathunga, D., Roughan, M., Nguyen, H., Kernick, P., & Falkner, N. "Case studies of scada firewall configurations and the implications for best practices." *IEEE Transactions on Network and Service Management* 13.4 (2016): 871-884.
30. Ribeiro, A. “US critical infrastructure remains exposed as Congress confronts OT cybersecurity gaps, fifteen years after Stuxnet.” *Industry Cyber.* (2025).
31. Satter, R. “US warns hackers are carrying out attacks on water systems.” *Reuters*(2024).
32. SecurityScorecard. “Cyber Risk Intelligence: Iran-Linked Attack on U.S. Water Treatment Facility. (2023).
33. Sikder, M. N. K., Nguyen, M. B., Elliott, E. D., & Batarseh, F. A. "Deep H2O: Cyber attacks detection in water distribution systems using deep learning." *Journal of Water Process Engineering* 52 (2023): 103568.
34. Steinbrecher, D. “Cyber incident against a water authority in Pennsylvania (2023).” *Scenario 29: Cyber operations against water and water infrastructure*. (2024)
35. Stone, A. “SCADA Critical Infrastructure Works to Block Cyberattacks.” *Federally operated power facilities work to block the possibility of cyber attacks.* FedTech. (June 2022).
36. Ta, Q. V. "Study on cybersecurity solutions for water supply infrastructure." (2025).
37. The Consortium of Cybersecurity Clinics. “Case Study: The Oldsmar Attack.” (2025).
38. U.S. Attorney's Office, Southern District of New York. “Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities.” (2016).
39. Yadron, D. “Iranian hackers infiltrated new york dam in 2013.” *Wall Street Journal, 20.* (2015).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Panful, B., Apaflo, B. and Hutchful, N. " Cyber-Physical Systems Under Threat: A Case-Study Review of Recent SCADA Attacks in the U.S. Utility Sector." *Sarcouncil Journal of Engineering and Computer Sciences* 4.12 (2025): pp 104-117.

Publisher: SARC Publisher