Radiflow

Use Case

Cybersecurity for Water and Wastewater Facilities

Oldsmar, Florida is a small town of 15,000 on the shores of Tampa Bay -- a dot on the map not far from Clearwater. Even longtime residents of central Florida haven't heard of it.

On February 2021, Oldsmar became the most visible known victim of a cyberattack on a municipal water treatment plant. An unknown perpetrator gained remote access to the plant's industrial control system (ICS), briefly raising the amount of highly caustic sodium hydroxide being injected into the water treatment process.

As modern cyberattacks go, this one showed a remarkable lack of sophistication. The intrusion was observed in real-time by a human operator at the plant. The sodium hydroxide level was corrected right away, and the public was never in danger.

However, the results could have been far worse. The Oldsmar attack should serve as a wake-up call highlighting the fragility of water systems and their susceptibility to cyberattacks.

The Importance of Securing Water Facilities

A disruption can cause extreme and lasting damage:

A determined and sophisticated attacker with some knowledge of water or wastewater plant operations could cause significant disruptions to different operational facets:

- Disrupt treatment and conveyance processes by turning off pumps, disabling equipment, closing/opening valves, etc, which poses a threat to customers' health (no water; over- or under-chlorination/fluorination), to the environment (release of toxic substances), and to municipalities' revenues.
- Install ransomware and other malware, which can disable business or process control operations
- Disable remote monitoring & control of distributed unmanned facilities

In the worst case, a cyberattack can disable the entire system for days or weeks, leaving residents and businesses without a safe and reliable water supply.

The Challenge of Securing Water Facilities

Fresh water systems are highly distributed, from intake and pumping to reservoirs/water towers, chlorination and transportation to users. Each stage requires power for pumping, to maintain water pressure and/or elevation, making it a point of vulnerability. Remote facilities are often unmanned, and rely on limited-bandwidth communication networks to send data to a central monitoring location (which opens new attack surfaces), as well as on physical barriers to prevent unauthorized entry.

Wastewater systems share the same challenges, with the additional complexity of treatment centers located inside or in close proximity to cities and small towns, compounding the health and ecological hazards.

Complex, Often-Antiquated ICS

Most traditional ICSs were designed with the assumption that they would be isolated from other systems, particularly the facility's data communication network. This left ICS systems exposed to cyber threats. As the Oldsmar case shows, exploiting ICSs' remote access capability can be trivially easy, even for an unsophisticated hacker.

Over the years many municipal and regional water facilities have been modernized with ICSs and other data network-connected systems. However, chronic underfunding has left these critical systems vulnerable to cyberattacks. Most municipal water departments have little or no IT support personnel to perform cybersecurity tasks.

Also, as in any complex ICS, both types of water systems typically host an array of devices by multiple vendors, thus introducing a host of device- and vendor-specific vulnerabilities. Understanding the interplay between devices and business processes is a key factor in calculating risk.

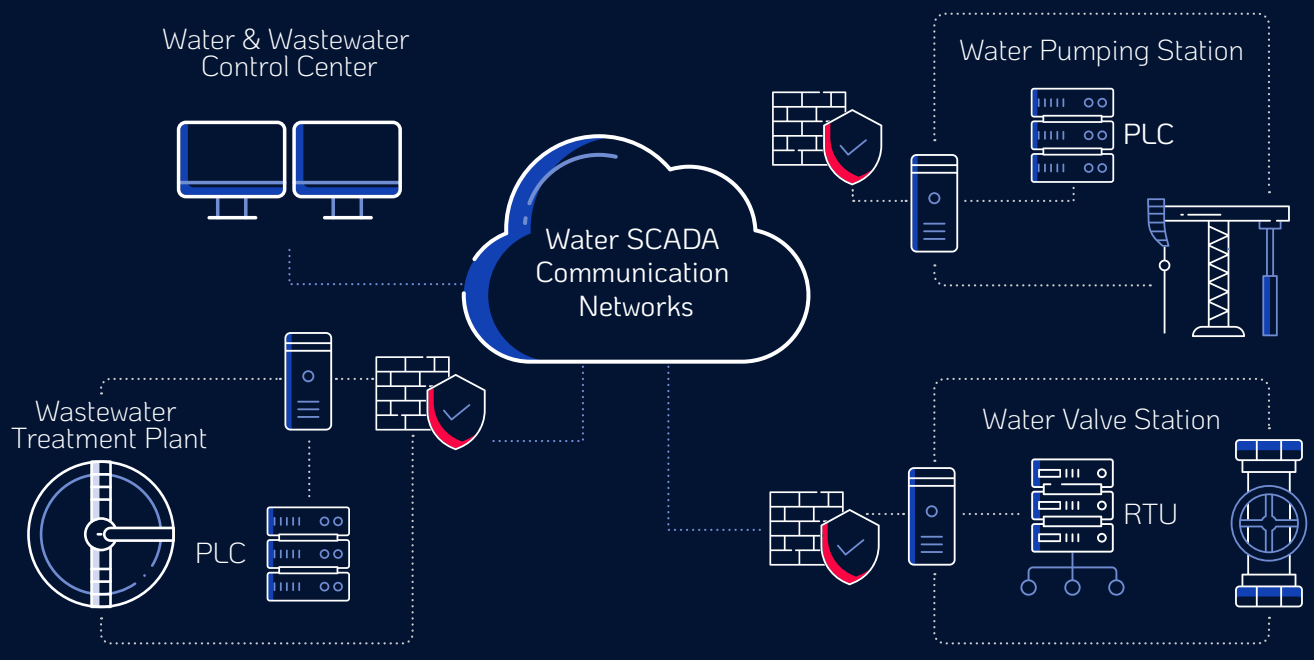
To make it worse, many facilities use devices that were never designed for networked operation, and so don't have adequate cyber-protection. As a whole, and by nature of government-controlled systems, water systems are typically slow to adapt to new technologies.

The Solution - Transitioning to a Secure Public Water System

Securing a public water system doesn't happen overnight. It is a phased transition:

1. Network visibility gain access to detailed network visualization maps that provide easy access to each device's properties, state, vulnerabilities and potential inter-zone attack vectors.
2. ICS security assessment: includes an inventory of ICS hardware and software components and an ICS risk assessment to determine the most critical and vulnerable components.
3. **Implementation**: Based on the results of the ICS security risk assessment, a hardening plan is drafted - taking into consideration the customer's security preferences and budget constraints, with a prioritized list of mitigation measures toward strengthening and optimizing OT security. These actions are in accordance with IEC62443 compliance and may address physical facility access security as well as the security of the data network, databases, applications and the remote access control system.
4. **Long-term security management**: Fixing existing vulnerabilities is just the first step, as systems grow and evolve, new components get integrated, and hackers become more sophisticated and determined. The key to long-term system security is ICS network monitoring, which provides constant identification and mitigation of intrusions as well as changes in the risk posture due to new threats.

Water System Networks



Radiflow Solutions for Water Facilities

Radiflow has deployed its solutions to dozens of water and wastewater facilities worldwide. We offer a variety of products and services, as well as industry-specific expertise, for protecting water and wastewater treatment facilities to support the customer on the journey to achieve cyber resiliency:

Map the network assets, the connectivity between the assets and group the assets into zones and business processes using our threat detection tool.

Know the risk posture of each site by simulating the relevant attack techniques on the digital image of the site using our 1st of its kind OT BAS (Breach Attack Simulation) tool. The tool can map your risk posture according to business impact as well according to the IEC62443 standard. Furthermore, the tool supports multi-site analysis so you can see in one glance the risk-status in your overall domain.

Generate an **actionable plan** for implementing security controls to improve the cyber resiliency of the sites using the mitigation optimization engine that compares hundreds of WHAT-IF scenarios to prioritize your security road-map.

Continuously **monitor** the site network for anomalies as well as for changes in the risk posture due to the changes in the threats landscape and in the site.

Secure your Water Facility

At Radiflow, we believe the most important steps toward securing your systems are taken before a threat is identified. There should be no compromise on ICS or OT security, but you can't protect what you can't see, and you can't manage what you don't know.

Our cybersecurity experts perform all phases of the security process. We leverage our best-in-class products and services to optimize the security of your facility and its OT.

The task of securing water and wastewater treatment facilities from cyberattacks is best left to outside security professionals, especially when in-house staff lack the knowledge and skills to carry it out.

Radiflow's renowned team of cybersecurity experts take the guesswork out of OT security by empowering our customers with actionable data. We can assess your cybersecurity readiness and offer the solutions necessary to protect your operations. If you're ready for industrial threat detection and risk management decisions backed by research and led by innovation, **contact us today**.

Radiflow | For more info: **radiflow.com**