INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

WATER AND WASTEWATER SYSTEMS:

AN APPRAISAL OF THE CYBER RISKS AND THREATS FACING THIS CRITICAL INFRASTRUCTURE

Institute for Homeland Security

Sam Houston State University

Narasima Shashidhar

Cihan Varol

Water and Wastewater Systems: An Appraisal of the Cyber Risks and Threats Facing this Critical Infrastructure

Narasimha Karpoor Shashidhar[1*], and Cihan Varol[2]
Digital Forensics and Information Assurance Lab
Department of Computer Science
Sam Houston State University, Huntsville, TX
{karpoor, cvarol}@shsu.edu

*Corresponding author

Technical Research Paper

I. Abstract and Motivation

The stability and national security of our country is very strongly correlated with the robustness of our water and wastewater systems. The health, well-being, technological advances, and prosperity of our nation is intricately tied to our country's ability to prevent water-borne, communicable pathogens, and associated diseases, protecting our precious natural resources, and in general to maintaining and protecting our flourishing natural environment. It is self-evident, therefore, that we pay utmost attention to the threats and risks that the systems encapsulating the water and wastewater treatment facilities face on a regular basis. The economic disasters that befall our country as a result of an ill-secured water infrastructure are catastrophic and the costs dire. Given the myriad avenues of attack on this critical infrastructure such as denial of service, injection of noxious chemicals, subverting SCADA systems, our broad goal in this project is to conduct an appraisal of the cyber risks and threats facing this critical national infrastructure.

Keywords: water systems, wastewater systems, PLCs, SCADA, security threats, vulnerabilities, risks.

II. Critical components of a waste management and water treatment facility

The economic development of a region depends on reliable, high-quality water. Job creation, tax revenues, visitor spending, real estate values, growth and investment

[1] www.linkedin.com/in/karpoor
[2] https://www.linkedin.com/in/cihan-varol-53105012/

are all tied to water quality. The U.S. Environmental Protection Agency (U.S. EPA[3]) notes that the critical components of a waste management and water treatment facility are the chemical addition system, coagulation and flocculation system, sedimentation, filtration, and disinfection systems. These components of course correspond to the distinct stages involved in the treatment process. Computing technology is integral in each of these above-noted systems. From CAD software for design, to flow management, most units of the system are dependent on the smooth, secure operation of the cyber physical systems that are integral to the system. While this is not an exhaustive list, the most commonly found cyber physical components of a water and waste-water SCADA systems are common sensing solutions such as water tower level monitors, remote pump monitoring systems, wastewater pump station monitoring, chlorine analyzers, ambient air monitoring, remote pressure monitoring, water well monitoring, and desktop software (and more likely related mobile applications).

Broadly speaking, the critical components of a waste management facility include sorting and processing stations, treatment technologies, storage and eventually disposal (landfill or further processing at recycling centers). Along the same lines, a water treatment facility is composed of intake systems where water enters the system from the source (lake, river, reservoir, etc.). The water then goes through a pretreatment phase to remove large matter through processes such as screening, grit removal, and coagulation and flocculation. Both coagulation and flocculation aim to neutralize the charges of the particles in the water while amalgamating these smaller particles into larger clumps so as to encourage sedimentation. This step is typically tackled in the clarification stage of the process followed by filtration using sand, or carbon-membrane based filters. Disinfection using chlorine agents to kill pathogens typically occurs just before storage and distribution to homes and industries. The tables below aim to illustrate a simplified model of these components with a flow-and-process oriented approach.

Table 1: Critical Components of Both Systems

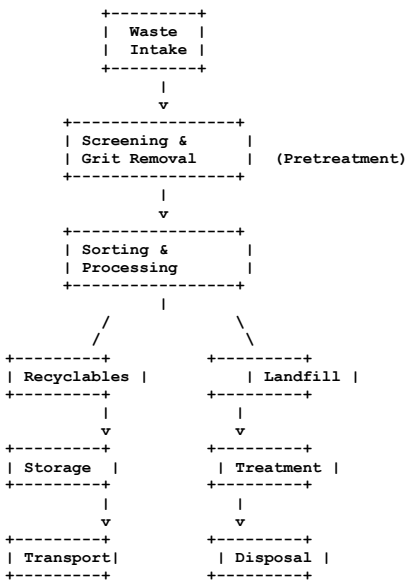
Waste System:	**Water System:**
• Waste collection arrives at the facility. • Sorting and processing separate recyclables from landfill waste.	• Water is drawn from the source (river, lake, etc.) through an intake.

[3] https://www.epa.gov/

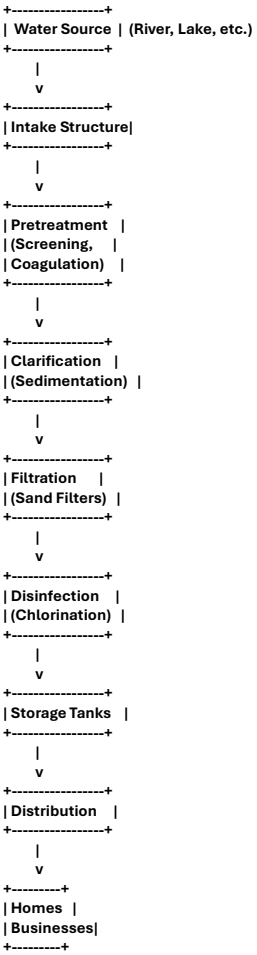
• Recyclable materials are stored and then transported for recycling. • Landfill waste undergoes treatment before storage and disposal.	• Pretreatment removes large objects and suspended particles. • Clarification removes large particles from the water. • Filtration removes any remaining particles from the water. • Disinfection kills bacteria and other harmful microorganisms. • Treated water is stored in a reservoir before being distributed.

Table 2: Flow and Process in Both Systems

Waste Management Facility



Water Treatment Facility



III. Exposure to Risks and Potential Threats

While the water and wastewater systems are prone to a diverse set of risks such as natural disasters, physical attacks, aging infrastructure, and contamination, in this report, we are interested in highlighting the cyber-attacks that can be launched against these systems. The cybersecurity and infrastructure security agency (CISA), America's Cyber Defense Agency[4], has identified ransomware and data theft to be the most critical risks faced by these systems[5].

The most prevalent and pernicious threats and vulnerabilities are:

1. **Data theft and Ransomware:** Data theft/breach is a very common occurrence and captures the situation where an unauthorized party gains access to data. Ransomware, on the other hand, takes it a step further. Ransomware (also called crypto virus) encrypts the victim's data and attempts to extort the victim to decrypt their data. The authors have a published report funded by the Institute for Homeland Security on Ransomware and Cryptovirus [3].
2. **Improper network segmentation:** Segmenting and partitioning a network is done in an effort to contain the spread of network threats. Done correctly, an infection or attack can be isolated and thereby unable to wreak havoc on the entire infrastructure. This is particularly true in water and wastewater systems which employ SCADA architecture. Typically, these SCADA systems are prohibited direct access to the Internet (air gapped) thereby preventing a direct attack on these control systems from the outside world. At the very least, the control system computing devices, programmable logic controllers, and field sensors, and devices are each consigned to their own network segments.
3. **Lack of firewall hardening:** SCADA systems were not designed to be exposed to the Internet. The sensors, actuators, valves, and other components are not equipped with the computing capability to be imbued with security mechanisms and protocols (these SCADA components cannot run anti-virus software for instance, use legacy communication protocols, and almost always have limited memory, and storage components on board). To this end, the design philosophy behind their architecture calls for network segmentation, and to be placed behind a perimeter security system such as an adequately hardened firewall, behind the

[4] https://www.cisa.gov/

[5] https://www.cisa.gov/resources-tools/resources/cyber-risks-and-resources-management-water-and-wastewater-systems-sector

DMZ, so that they cannot be accessed directly from an untrusted network such as the Internet.

4. **Escalated privilege user settings:** As we've noted earlier, SCADA systems were designed at a time when security concerns were not paramount. It is not uncommon for systems to be used with default, weak, or no passwords. Most users on the control systems of a water system use 'administrator' privileges. The issue is that a vulnerability that is exploited by a malicious actor will also find himself/herself with an elevated privilege as well and consequently be capable of generating greater damage that if the *principle of least privilege* were to have been adopted. NIST SP 800 defines the principle as follows: a security architecture designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function [2].
5. **Unpatched software/SCADA firmware:** There are components found in both the IT (information technology) and OT (Operational technology) systems that need to be patched, maintained, and kept up to date. Failure to do so will leave these systems vulnerable and afford a malicious actor access to data and the ability to infiltrate more sensitive systems within the network.
6. **Weak authentication mechanisms:** Authentication mechanisms used in most SCADA systems are weak and ineffective. Weak, shared passwords, devices and servers with unnecessary services, and ports open, all lead to a weakened system. A water treatment facility is only as strong as its least protected component.
7. **Ineffective disaster recovery and contingency plans:** While natural disasters can indeed grind operations to a halt and necessitate contingency plans, in this report, we are more interested in documenting the consequences of cyber disasters and their implications on continued operations of water treatment facilities. As outlined earlier, a ransomware attack, where all the data is encrypted, and a ransom demand is placed to recover lost/encrypted data, effective disaster recovery plans and contingency operations including backups, and cold storage, can assist in bringing the systems back online and operational without much delay.

In fact, these threats affect all the sixteen critical infrastructure vectors[6] outlined by CISA that are deemed vital to the health and security of our country. In the spirit of advancing the security efforts by the Departments of Homeland Security, Defense, Energy, Treasury, Health and Human Services, Agriculture, and the Environmental

[6] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Protection Agency, The White House released the Presidential Policy Directive 21 in February 2013 [1]. This directive aims to improve collaboration among these agencies towards the common goal of reducing risk to critical infrastructure.

Some Prior Attacks

As a means of drawing the readers' attention to the fact that attacks on water and waste management facilities are on the rise, we'd like to outline a few articles from the mainstream media to underscore this issue. On May 20, 2024, CBS[7] news published an article impressing the urgency of water utilities across the country to stay vigilant and bolster security of their systems. The EPA (Environmental Protection Agency) has put out bulletins stating that cyberattacks are becoming more frequent and severe. Surprisingly, many water utilities in the U.S. are falling short in very trivial ways, such as using systems with default authentication data, i.e., usernames and passwords. This leaves them vulnerable to simple, but damaging attacks such as a denial-of-service attack leading to interruptions to water, treatment, damage to critical infrastructure components, and hazardous chemicals in the water. FBI director Christopher Wray warned, on April 18, 2024[8], that Chinese hackers are targeting U.S. infrastructure, including water treatment plants. One such example is the Chinese sponsored cyber group called '*Volt Typhoon*' that uses botnets to launch their attacks. Another example involves an attack in late 2023 by Iranian cyber criminals on a Pennsylvania water system. Earlier this year (April 2024), the Texas Tribune[9] reported an attack on a rural town's water system causing it to overflow. This attack has been attributed to a Russian hacker group. On the domestic front, in 2021, a disgruntled employee of the water treatment plant in Oldsmar, Florida attempted to increase sodium hydroxide levels to dangerous levels[10]. A cursory search on the Internet reveals several such attacks linked to many cyber attackers in the past few years. The common denominator in all these cases is the fact that the vulnerabilities that plagued the systems were left unprotected. One goal of this white paper is to shed light on the fact that these systems are very vulnerable and deserve our time and attention for their adequate defense. In the next section, we will delve into some of the reasons behind these increased attacks and perhaps the ease of launching

[7] https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/
[8] https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says
[9] https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/
[10] https://www.wired.com/story/oldsmar-florida-water-utility-hack/

such attacks. This coincides with the development and rapid deployment of SCADA and IoT systems.

IV. Evolution of IoT and SCADA systems

SCADA[11], System Control and Acquisition Technology, has been used in industrial settings for a long time now. As the capabilities of this technology increased, and the advent of IoT at the turn of the century, utilities, and in particular water, sewer, and treatment facilities started embracing the innovations in this sector. The field of water quality monitoring has seen the most advances and adoptions of internet of things (IoT) technology. The myriad sensors used to measure water safety parameters such as acidity, alkalinity, temperature, pressure, oxygen, particulate matter, pollutants, toxins, microorganisms, etc. are all possible thanks to the advances in IoT and sensing systems. Some of the notable benefits of implementing these systems are that reaction times are reduced upon receiving an alarm, continuous monitoring, and observation of the vitality of the system, respond algorithmically to specific threats and alerts, and the ability to operate the entire system remotely.

a. Increased Attack Surface Area

Given that these above noted capabilities conferred by IoT and SCADA are highly attractive, water treatment facilities across the country are rushing to deploy them in their treatment centers and plants. To enable these features, SCADA, and IoT systems have necessarily had to embrace cloud-based storage and command modules. The future digital innovations in this sector may well be propelled by artificial intelligence, machine learning, nanotechnology, virtual/augmented reality, and robotics. While these tools and technologies are a boon to humanity, these advances also increase the surface area and the available attack territory that these technologies inhabit. Even a rather innocuous attack, such as a Denial-of-Service, in the case of a water treatment facility would have devastating consequences. Incidentally, these types of attacks can be launched against any industrial system with these SCADA components and is not only isolated to water and waste management facilities.

[11] https://scada-international.com/

We present below a brief synopsis of the distinct functions of a SCADA system as it relates to our context of water and waste management facilities.

1. **Monitoring**: gathering real-time data from sensors and monitoring various aspects of the treatment process including flow rates, pressure levels, chemical concentrations in water, motor operation at pump stations, and equipment status.
2. **Control**: Based on pre-programmed parameters and operator input, SCADA systems are programmed to automatically control and adjust valves, control regulators to manipulate water flow, turn pumps on or off on demand, and tweak chemical levels and doses as indicated by sensors.
3. **Data Acquisition/Analysis**: SCADA continuously collects and stores data, collating this data at the centralized repository, allowing operators to monitor trends, identify potential issues, and optimize treatment processes.
4. **Alarms:** SCADA systems are typically programmed to set off alarms in the event of deviant or anomalous sensor readings. This way operators can identify anything out of the normal operating ranges, alerting them to prompt action.

   Ironically, hijacking the SCADA system will permit an attacker to report 'normal' readings to the operators while the system is running aground. This did happen in the case of the cyber weapon (malware) Stuxnet targeted to attack the industrial control platform Siemens model S7 PLCs (programmable logic controllers). This cyber weapon is commonly believed to have been authored by the U.S. and Israel to slow and hamper the Iranian efforts to enrich weapons grade uranium at their Natanz facility. We point the interested reader to the excellent white paper by Symantec researchers called the 'W32. Stuxnet Dossier'[12] for more details on these classes of attacks on industrial control systems and Stuxnet in particular.

Benefits of deploying SCADA systems in Water and Wastewater Facilities

1. **Efficiency**: It's much faster and more efficient to automate data collection and analysis using real-time components. Not only is this eminently desirable, but it's also a necessity in today's complex water and waste

[12] https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

management facilities to minimize wasted time, effort, cost, and resources.

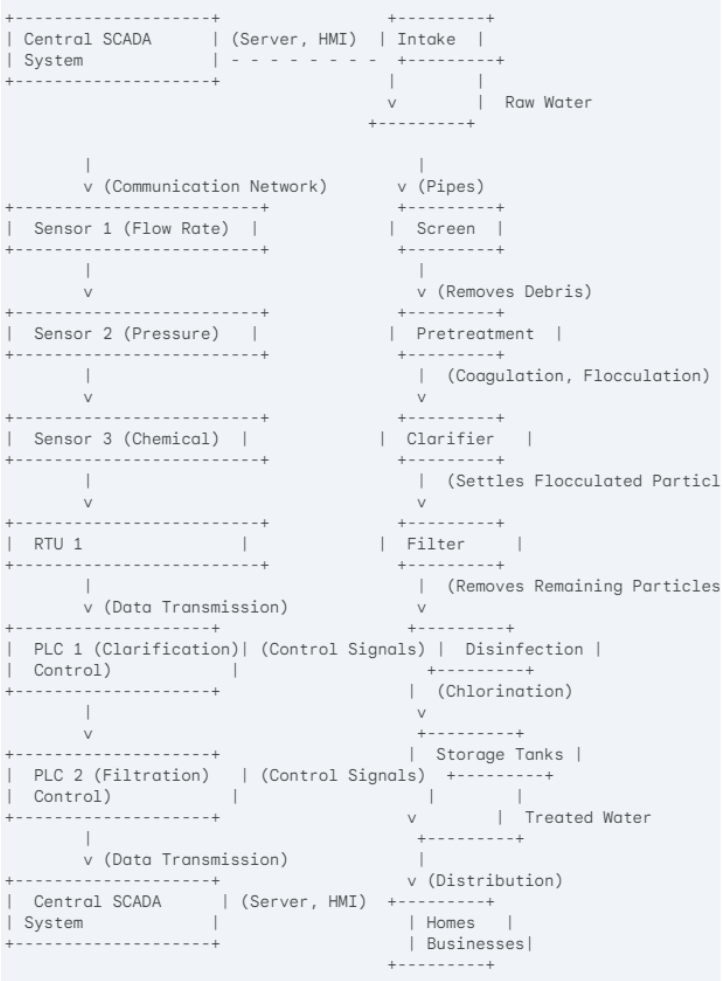
2. **Safety:** Timely detection of malfunctioning equipment can prevent hazardous conditions should the abnormal condition persist for a longer duration.
3. **Energy Savings:** SCADA systems can be finely tuned to optimize any parameter the operators of a plant desire, including energy, chemical usage, heat, etc.
4. **Enhanced decision-making ability:** With greater access to timely, real-time data, trends can be generated and with the assistance of artificial intelligence, preemptive maintenance and upkeep can be performed.
5. **Remote capabilities:** SCADA systems, by virtue of their ability to be accessed remotely, permit operators to monitor and run entire facilities from afar, away from potentially dangerous working conditions.

Typical SCADA components in water and waste management facilities:

- **Human-Machine Interface (HMI):** This is the interface afforded to the operator. Put simply, the operators interact with the entire system via the software interface on a computing terminal. This is often the only primary 'control panel' that comes to mind when one thinks of an industrial control system.
- **Programmable Logic Controllers (PLCs):** These are rugged, industrial computers, often highly specialized for the environment and function they are tasked with, used in industrial automation. They are different from the general-purpose computers (desktops, PCs, laptops) used by consumers in the civilian world. They are designed to execute targeted control logic based on pre-programmed instructions and sensor readings received from the SCADA system.
- **Remote Terminal Units (RTUs):** RTUs and PLCs are very similar in nature and function. The primary difference stems from the fact that RTUs are parameter-based devices. They collect data from sensors in the field and transmit it to the central SCADA system like their PLC counterparts but are more suited in instances where complex, continuous processes like pipelines, and water treatment systems are to be monitored and are more cost-effective when compared to PLCs.
- **Communication Network:** A secure network infrastructure is the backbone for the entire system. This network connects all the SCADA

components, enabling data flow and remote access in a secure manner.

Fig 1. Conceptual diagram of a SCADA system overlayed on the water treatment facility



In Figure 1 the components of the SCADA system are laid out in parallel with the physical elements of the water treatment facility to illustrate their functional roles. The central SCADA server and HMI are used by operators for data visualization and control. The communication network is pervasive and ensures a safe and secure backbone network for messages and relays throughout the system permitting data exchange. The sensors that are placed strategically throughout the facility aid in monitoring the parameters they've been tasked with such as flow, pressure, temperature, chemical levels, etc. The RTUs and PLCs collect and transmit sensor data to the central repository of the SCADA system for further processing and analysis/visualization in addition to executing logic to operate pumps, valves, and other devices.

In the next section, we discuss security hardening measures in an effort to defend the SCADA system, and the underlying water and waste management plant from threats and attacks. To this end, a working knowledge of the flow of data (which interestingly enough corresponds to the flow of water) through the system would be of immeasurable value to us. To begin with, life in the system begins with collection of data. We know that the sensors of the system continuously gather real-time data on various aspects of the treatment process. The data travels through the secure communication network to the RTUs. RTUs transmit the collected data to the central SCADA system for analysis. The SCADA system displays the data on the HMI for operator monitoring and analysis. Based on the settings and operator input, the SCADA system sends control signals to PLCs. PLCs execute control logic, adjusting valves, pumps, and chemical dosing systems to optimize treatment processes. This simplified view will suffice for us to explore how we might defend the system against attacks.

V. Risk Assessment: Imminent Public Harm and Loss When Threats Meet Risks

While the purpose of our white paper is primarily technical and cyber security oriented, we would be remiss if we did not identify a couple of instruments that would aid water utilities with assessing risk and mitigating them in an objective manner. This is also done in the service of meeting our practical applicability commitment of our project. We hope that utilities are able to use the resources listed in this section to this end, both in TX and around the country.

a. **Popular Risk Assessment Metrics and Tools: Practical Applicability**:

In this section, we discuss some metrics and tools for risk assessment when it comes to waste management and water treatment facilities. One authoritative resource when it comes to risk management framework for the water and wastewater systems is the U.S. EPA (Environmental Protection Agency). America's cyber defense agency, CISA, has published sector resources and working groups tasked with protecting water and wastewater systems of our nation. The Environmental Protection Agency is designated as the *Sector Risk Management Agency* for the Water and Wastewater Systems

Sector[13]. Presidential Policy Directive 21 changed the name of the Water Sector to the Water and Wastewater Systems Sector in 2013. The National infrastructure protection plan (NIPP 2013) [5], Partnering for Critical Infrastructure Security Resilience, published by the Department of Homeland Security outlines the core tenets and establishes the vision, mission, and goals that are supported by these core tenets focused on risk management and partnership to influence future critical infrastructure security and resilience planning at the international, national, regional, and owner and operator levels. The details of this plan as it relates to water, and wastewater systems, can be found in a report published by the U.S. EPA and The Department of Homeland Security [4].

The EPA also maintains a water resilience webpage[14] aimed at assisting utilities conduct a risk assessment, adapt to climate change impacts, develop water surveillance and response capabilities, and adopt cybersecurity best practices. In addition to these tools, there are training modules available on a number of topics including multi-year exercise plans to increase emergency preparedness, tabletop exercises for all-hazards scenarios, in addition to workshops and webinars. This enforcement alert[15] provides community water systems with information on immediate steps they can take to ensure compliance with the Safe Drinking Water Act (SDWA) Section 1433 and to reduce cybersecurity vulnerabilities. This webpage by the EPA is dedicated to risk assessment and reduction for drinking water and wastewater utilities[16].

VI. Security Hardening Measures

As we begin to conclude our report, let us look at some tips and techniques to mitigate the cyber risks faced by our water and waste management systems. These defense mechanisms are not exclusive or unique to water and waste management systems, but are applicable to all typical, modern industrial systems that employ SCADA and similar subsystems. As we've seen, SCADA systems are critical infrastructure in these installations, and are unfortunately vulnerable to cyberattacks

[13] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector
[14] https://www.epa.gov/waterresilience
[15] https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities#:~:text=Recently%2C%20disruptive%20cyberattacks%20from%20adversarial,protect%20our%20nation's%20drinking%20water.
[16] https://www.epa.gov/waterriskassessment

by virtue of their architecture. Here are some key measures to protect systems in water and wastewater facilities:

1. **Network Segmentation**:
    a. This is a standard security measure in network design. The premise behind this approach is to segment distinct units of the network in such a manner that a vulnerability exploited in one section of the network does not manifest itself in another section of the network.
    b. To this end, the advice is to isolate the SCADA network from the business network and the internet. Air-gapped systems are less prone to attacks from the outside world.
    c. The goal is to minimize the attack surface and prevent attackers on the business network from reaching critical control systems.
2. **Secure Network Configuration**:
    a. Firewalls, intrusion detection, intrusion prevention systems, and a DMZ (demilitarized zone) perimeter network are commonly employed as a standard approach to secure network configuration. These screened subnetworks separate a local area network (LAN) from other untrusted networks, such as the Internet.
    b. Implement firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor network traffic for suspicious activity, both ingress and egress.
    c. Use strong encryption for all communication within the network.
    d. Disable unused network ports and services on all hosts on the network to reduce potential vulnerabilities.
3. **Access Control**:
    a. Implement strong authentication protocols (multi-factor authentication) for all access to the SCADA system. Eliminate the usage of default authentication mechanisms (passwords, usernames, etc.)
    b. Enforce the principle of least privilege, granting users only the access level required for their specific tasks. Most MS-Windows users, unfortunately, operate their devices as administrators, which must be strongly discouraged.
    c. Regularly review and update user access permissions. A periodic purge of users and permissions is also a responsible task to maintain the health and vitality of the system.
4. **System Hardening**:

    a. Keep all SCADA system software and firmware up to date with the latest security patches. This is also true for all hosts, and operating systems for any other computing devices on the network.
    b. Disable unnecessary services and functionalities on SCADA devices.
    c. Regularly scan SCADA systems for vulnerabilities and take steps to remediate them.
5. **Physical Security**:
    a. While not a cyber security measure, secure physical access to SCADA control rooms, HMI, and equipment to prevent unauthorized tampering.
    b. Implement security measures like cameras, and motion detectors to monitor for physical intrusions.
6. **Cybersecurity Awareness and Training**:
    a. Regularly train personnel on cybersecurity best practices, including phishing awareness and secure password management. There are several resources by the U.S. EPA for training and emergency preparedness as outlined in the previous section.
    b. Encourage employees to report any suspicious activity so as to deter social engineering activities.
7. **Backup and Disaster Recovery**:
    a. Regularly back up critical SCADA system data to ensure a quick recovery in case of a cyberattack. This mitigates in the event of a ransomware attack as well, which SCADA systems are particularly prone to.
    b. Develop and test a disaster recovery plan to ensure operational continuity in the event of a cyberattack as outlined by CISA.
8. **Additional Considerations**:
    a. Conduct regular penetration testing to identify and address vulnerabilities in the SCADA system.
    b. Consider employing security solutions specifically designed for SCADA systems.
    c. Stay informed about the latest cyber threats and vulnerabilities targeting SCADA systems.
    d. Implement phishing-resistant multi-factor authentication and ensure logging is turned on for application, access, and security logs and store logs in a central system.
    e. Plan “end-of-life” for technology beyond manufacturer’s lifecycle.

By implementing these measures, water and wastewater facilities can significantly improve the security of their SCADA systems and reduce the risk of cyberattacks.

Furthermore, since defense is an ongoing process, continually assessing the utility's security posture and adapting these strategies as needed is paramount for a smooth and safe operation.

VII. Putting it all together and Lessons Learned

In summary, thus far, in this white paper, we have seen how vulnerable our current water and waste systems are. The vast majority of vulnerabilities in these systems have been introduced primarily due to the rapid adoption of new and bleeding-edge technologies, such as SCADA and IoT. But this is inevitable, especially in the current era, given the inexorable march of technology. The simplest advice comes from the EPA[17] which have been listed below.

Some actions EPA, CISA, and the FBI strongly recommend in Top Actions for Securing Water Systems:

- Reduce exposure to public-facing internet
- Conduct regular cybersecurity assessments
- Change default passwords immediately
- Conduct an inventory of OT/IT assets
- Develop and exercise cybersecurity incident response and recovery plans
- Backup OT/IT systems
- Reduce exposure to vulnerabilities
- Conduct cybersecurity awareness training

In addition to this advice, they also offer free help to implement such changes to utilities that need it.

Free help to implement changes:

- Contact EPA through its Cybersecurity Technical Assistance Form: https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector

[17] https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities#:~:text=Recently%2C%20disruptive%20cyberattacks%20from%20adversarial,protect%20our%20nation's%20drinking%20water.

- Email CISA Cyber Hygiene Services: *vulnerability@cisa.dhs.gov* with subject line: Requesting Cyber Hygiene Services.

These resources and the urgent call for action have been spurred by the recent, disruptive cyberattacks from adversarial nation states that have impacted water systems of all sizes, including many small systems. As a result of these increased threats, the U.S. Environmental Protection Agency (EPA), CISA, and the FBI has increased its enforcement activity to protect our nation's critical systems.

VIII. Future Work

An interesting avenue of research and development, spawned by the rapid advance of Artificial Intelligence (AI) and Machine Learning (ML), is the applications of AI and ML in predictive analytics. Specifically, in the field of SCADA and IoT, how might AI and ML be employed in the field of maintenance, anomaly detection, and optimization. On the other hand, these new and bleeding-edge technologies open the door to more insidious threats and persistent dangers that our systems need to be able to thwart. Another avenue of improvement is in the area of standardization. Currently, SCADA vendors use proprietary protocols and communication mechanisms. This makes it challenging to devise universally secure defense mechanisms and a free exchange of ideas among utility providers and security professionals. Better interoperability, that overcomes incompatibility, can facilitate a tighter integration of new technologies with sound defense techniques thereby equipping us to combat these developing threats and dangers.

IX. Practical Applicability

On a practical note, we have identified the distinct components of these systems including the flow and offered a process-oriented approach to defense. We've outlined the potential threats and highlighted the vulnerabilities that these threats could be attributed to. We showed some prior attacks, the motivations and modus operandi behind these attacks, both in the state of Texas, and across the nation. We asserted that these vulnerabilities and weaknesses stem from a rapid adoption of ever evolving technologies including IoT, and SCADA. While we do not deny the benefits conferred by these technologies on the operation of modern water and waste systems, our argument was merely that care should be taken prior to the rapid adoption and deployment of these tools. We looked at some risk assessment metrics, and outlined some of the several wonderful tools offered by the EPA, CISA,

and the FBI. Next, we turned our attention to security hardening measures, and the tools offered and advice by these agencies to achieve this goal.

X. Conclusions

The key conclusions we can draw from our discussion in our report about waste and water utilities and related systems is that efficient and safe operations of this infrastructure stems from a foundational understanding of the technologies employed. Next is the realization of the critical role played by SCADA and IoT. Lastly, the importance of cybersecurity and the vulnerability to cyberattacks cannot be understated. We've also seen the different stages involved in waste management and water treatment, the benefits, and specific components of the SCADA systems strategies for defense.

XI. Acknowledgement

The authors would like to thank the Institute for Homeland Security, and the Department of Computer Science at Sam Houston State University for the funding and support.

XII. Biographical Sketches of the Authors

Dr. Narasimha Shashidhar is a Professor of Computer Science and Digital Forensics and serves as the Director for the Doctor of Philosophy Program in Digital and Cyber Forensic Science. He received his Bachelor of Engineering in Electronics and Communication Engineering from The University of Madras in 2001, and his M.S. and Ph.D. degrees in Computer Science and Engineering from The University of Connecticut in 2004 and 2010, respectively. His research interests include Digital Forensics, Information Security, Cyber Forensics, and Computing Education. He was a part of the Voting Technology and Research Center (VoTeR) at the University of Connecticut where he advised the State of CT on the security and deployment of electronic voting machines. He has over 100 conference/journal publications and serves on the editorial advisory/review board and the Technical Program Committee (TPC) of a number of books, journals, and conferences.

Dr. Cihan Varol, is a Professor of Computer Science at Sam Houston State University. He received his Bachelor of Science degree in Computer Science from Firat University, Elazig, Turkey in 2002, Master of Science degree from Lane Department of Computer Science and Electrical Engineering from West Virginia University, Morgantown, WV, USA in 2005, and Doctor of Philosophy in Applied Computing from University of Arkansas at Little Rock in 2009. His research interests are in the general area of information (data) quality and its applications on Digital Forensics and Cyber Security areas, with specific emphasis on personal identity recognition, privacy preserving record linkage, entity resolution, secured IoT systems, social media forensics, 3D printer forensics, and web forensics. These studies have led to more than 130 peer-reviewed journal and conference publications and three book chapters. He is an executive board member of IEEE Education Society Standards Committee and the chair of IEEE P2834.1 Standards on Digital Forensics on Trusted Learning Systems.

XIII. References

1. Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Accessed April 13, 2024.
2. NIST Special Publication 800-53, Rev 5. Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce. Wilbur L. Ross, Jr., Secretary. National Institute of Standards and Technology. September 2020.
3. Shashidhar, N. & Varol, C. (2023) Forensic Digital Data Sanitization A Guide for Small and Medium-Sized Businesses A Primer on Data Erasure: An Integral Component of Data Lifecycle Management. (Report No. IHS/CR-2023-1028). The Sam Houston State University Institute for Homeland Security.
4. Water and Wastewater Systems Sector-Specific Plan2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. Accessed June 11, 2024.
5. National infrastructure protection plan. NIPP 2013. Partnering for Critical Infrastructure Security Resilience. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. Accessed June 11, 2024.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Varol, Cihan & Shashidhar, Narasimha (2024) Water and Wastewater Systems: An Appraisal of the Cyber Risks and Threats Facing this Critical Infrastructure (Report No. IHS/CR-2024-1010). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/3WF8B