Practical Cyber Resilience for Water/Wastewater Environments

1/07/2022

Introduction

Cyber risk is the top threat facing critical infrastructure in the United States. The federal government's various intelligence agencies and authorities have universally confirmed consistent global threats from individual cyber criminals or groups backed by foreign governments. These threat actors are specifically targeting the nation's water and wastewater facilities, operations, and systems.

The Water and Wastewater critical infrastructure sector is *one of*…if not *the*…most vital interdependent sector providing resource to Energy, Transportation, Nuclear, Manufacturing, Agriculture, Medical, and Emergency Services. Water utilities need to address many challenges, including increased operations and facility maintenance costs, educating personnel on cyber issues, outdated systems and infrastructure. Adversaries know this as well, which is why Water and Wastewater is a high-value target. The innovation and sophistication of threats and attacks are becoming more advanced every day.

Acknowledged by the White House by way of executive order, supported by the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of National Intelligence (DNI), it has become imperative that water and wastewater entities have the necessary cyber security, risk management, and incident response programs in place to protect public health and safety, prevent service disruptions, and safeguard customer and employee personal and financial information. Inadequate cyber defense measures and lack of cyber incident response or risk mitigation strategies will result in significant impact, outages, direct and cascading effects that can ultimately lead to potential loss of life in critical scenarios.

In January 2018 the BRIDGE Energy Group conducted a survey (*BRIDGE Index Utility Industry Grid Operations Survey*) of more than 20,000 utility employees, revealing that cyber threats are what they fear could have the biggest impact on operations, with a lack of resources and conflicting priorities as the greatest challenges. Fast forward to 2021, and the situation has worsened considerably. Water and Wastewater sector organizations and entities have been impacted by a broad range of attacks, most notably ransomware attacks, manipulation of Industrial Control Systems, valve and flow operations, and chemical treatment formulations, and efforts to disrupt and potentially destroy production environments.

In decades past, the threats experienced today could have been averted with traditional methods such as "Air Gap" deployments, keeping the vital water and wastewater supervisory, control, and process networks isolated from the information technology (IT) networks. However, the rise in data analytics, distributed management, remote access, as well as the Industry 4.0 Revolution driving digital transformation, implementing new capabilities and increased business value and insight. This is an important step forward, but these changes are introducing new, inherent security vulnerabilities.

Water and wastewater facilities and operations entering this new IoT-powered future are managing old systems alongside the new ones, while integrating OT and IoT/modern technologies. Unfortunately, the application of air gaps and simple perimeter defenses are not sufficient to address today's cyber threats. Water utilities must factor the myriad of cyber threat vectors with the broader understanding of the edge and perimeter applications. They must provide tools to address segmentation, access, anomalous behavior, application performance, identity, and trust. The constant evolution of markets, operations, and requirements, coupled with the relentless and ever-increasingly sophisticated and diverse global cyber threats make cyber resilience and security solutions a daunting task.

Federal Response and Initiatives

U.S. Homeland Security Presidential Directive 7 was superseded in 2013 by Presidential Policy Directive 21, which expanded the list of critical infrastructures from 7 to 21 and renamed the Water Sector to the Water and Wastewater Systems Sector. The U.S. Environmental Protection Agency (EPA) is the agency for the Water and Wastewater Systems Sector and works with the Department of Homeland Security (DHS), other agencies, and industry groups to improve security for water and wastewater systems. In response to Presidential Policy Directive 21, DHS issued the National Infrastructure Protection Plan, which provides an updated approach to critical infrastructure security.

Also in 2013, Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, established that, "It is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

EO 13636 also called for development of a voluntary risk-based cybersecurity framework, as set forth in industry standards and best practices, to help organizations manage cybersecurity risk. As a result of EO 13636, the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity, and the American Water Works Association (AWWA) published the Process Control System Security Guidance for the Water Sector. Additionally, NIST has revised several its SP 800 series standards in the years since EO 13636 was issued.

Presidential Policy Directive 21 and EO 13636 have led to an increased focus on national policy regarding ICS security in critical infrastructure. Industry associations and government agencies are

making concerted efforts to quickly educate utilities. The guidelines and standards from these groups and agencies are designed to affect the way critical infrastructure projects are engineered and implemented. These guidelines apply to any entity, public or private, that runs critical infrastructure facilities.

The EPA's response to EO 13636 recommends using a voluntary approach to foster compliance with the cybersecurity framework developed by NIST. However, the EPA closed its response with the following statement: "If the voluntary partnership model is not successful in achieving widespread implementation of the Cybersecurity Framework or if warranted by a changing cybersecurity risk profile, the EPA can revisit the option of using general statutory authority to regulate cybersecurity in the Water and Wastewater Systems sector."

Addressing the Challenges

Cyber threats and risk to critical infrastructure and the current regulatory requirements, water utilities are faced with the prospect of adoption, implementation, integration, and investment of robust and reliable cybersecurity platforms and solutions. In the past, the water industry was less vulnerable to cyber threats, as utilities had the ability to switch to manual plant operation while the industrial control and automation cybersecurity concerns were addressed. Recently a lessoned learned with the COVID-19 outbreak has shown that extreme circumstances can create unanticipated labor resource constraints. Decisions by local authorities and the concerns of individual citizens may affect utilities' ability to manually control facilities for prolonged periods of time, resulting in a swing toward plants and processes being operated remotely. This, in turn, increases the risk to water utilities, as it has been shown that threat actors intensify their activities during crises and specifically target critical infrastructure.

Sweeping trends, new technologies, and now the global pandemic are reshaping how water and wastewater treatment plants are operated, now and into the future. Utilities will require a more mature formulation of objectives for water security. Executives and boards charged with sponsoring adoption and investment in cybersecurity, and ultimately with endorsing management's proposed cybersecurity programs, rely on mature methods for cyber risk evaluation and cybersecurity program strategies designed to promote cyber resiliency within the industrial network. Key elements of a successful cybersecurity approach include effective next-generation endpoint protection, an effective demilitarized zone (DMZ), and the ability to monitor and control assets over a protected network.

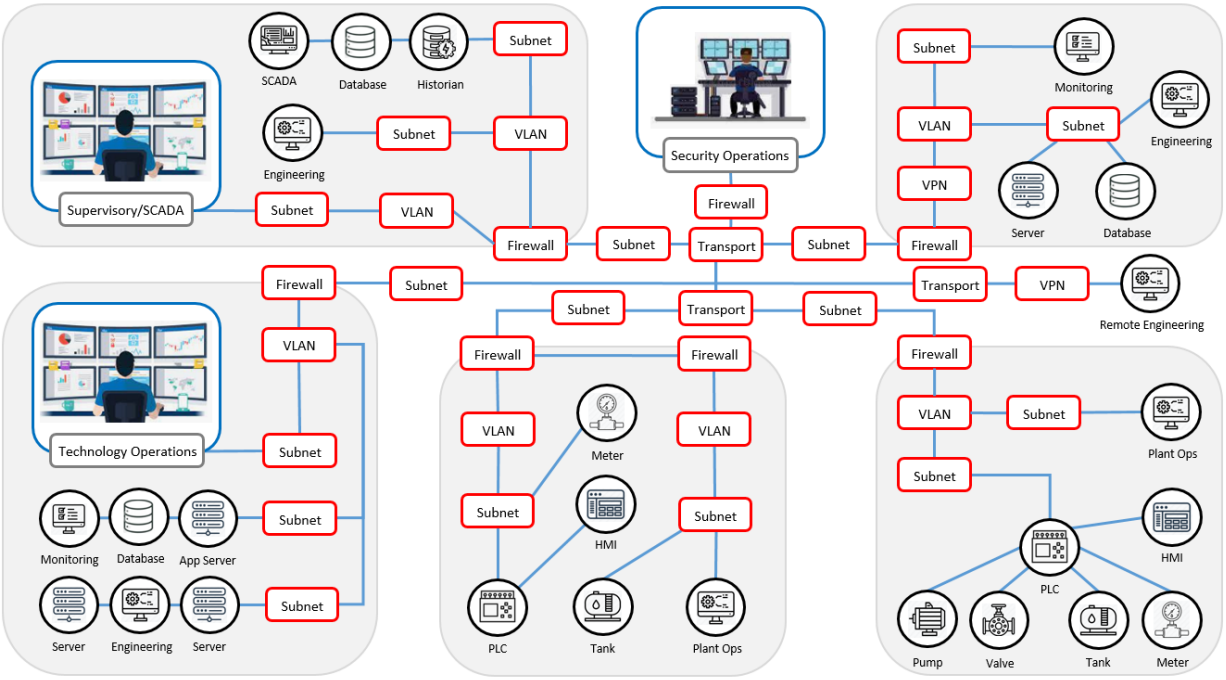
The relationship between operational risk and operational continuity to produce, store, and deliver water is as important and sensitive as ever. Utility managers are faced with a balancing act between the seemingly endless number of malevolent threats targeting their networks, people, and processes and defining their security posture, while trying to address physical and cybersecurity concerns to secure control systems and maintain critical operations across the business.

Public and private enterprise networks alike, from the plant level down to the field level, are experiencing deficiencies in plant security, physical access control, network security, and system integrity leading to many of the infiltrations and outages experienced over the past decade, including most recently Oldsmar, FL, Colonial Pipeline, and JBS Meats.

#	Location	Year	Target System	Investigator	Primary Impact
1	Australia	2000	Wastewater	HWT & Queensland EPA	Environmental pollution
2	PA, U.S.	2006	Water treatment	FBI	Data breach
3	CA, U.S.	2007	Irrigation	System personnel	Water theft
4	IL, U.S.	2011	Water plant	DHS	Cry-wolf effects
5	FL, U.S.	2012	Wastewater	System personnel	Data breach
6	NY, U.S.	2013	Dam	Justice Department	Data breach
7	U.S.	2013	Water utility	Third-party provider	Data manipulation
8	U.S.	2016	Water utility	Verizon Security	Control manipulation
9	U.S.	2016	Water utility	DHS	Data breach
10	U.S.	2016	Water utility	DHS	Bandwidth theft
11	U.K.	2017	Water supplier	Verizon Security	Financial impact
12	Europe	2018	Water utility	Radiflow	Resource theft
13	NC, U.S.	2018	Water utility	State and Federal	Data loss
14	CO, U.S.	2019	Water district	System personnel	Denial of access
15	FL, U.S.	2019	Water utility	FBI, DHS and Secret Services	Data loss

The challenges are significantly increased for Water and Wastewater critical infrastructure due to the nature and essential characteristics of water supply and wastewater disposal transport over long distances as well as decentralized and widely branched water and wastewater network infrastructures, including the Water Supply, Wastewater Disposal, Water Treatment Facilities, Control Centers, Plants, and External or Remote Stations.

Depending on the plant types and sizes as well as other influencing factors,
there are typical approaches for the industrial automation and control systems
(IACS) of water supply or wastewater disposal, from small plants with local operations only, through larger water and wastewater treatment plants to widely distributed networks as well as main control centers for monitoring and control of several plants of large operating associations. This can lead to large distributed systems, complex infrastructure and connectivity, communications, and the associated threat vectors, vulnerabilities, and exposures as represented by the graphic below.



Water utilities will face increasing pressures from these current challenges and from a rapidly evolving world. Digital transformation of water utilities provides the opportunity to combat many of these challenges by delivering innovative solutions to protecting and securing vital assets and operations of critical facilities, capability for remote operations, and increased efficiency.

A Practical Approach and Comprehensive Solution

Blue Ridge Networks was founded 24 years ago on the principle of making this uphill climb practical and effective, with the mission of protecting the nation's vital systems, intelligence communities and critical infrastructure from the sophisticated cyber-attacks witnessed today.

More than two decades of product development, innovation and technological advancement have produced the Blue Ridge Zero-Breach products and solutions that protect the operations, control systems, networks, and applications within water and wastewater facilities and organizations.

Blue Ridge Networks has delivered successful deployments of the LinkGuard network security and AppGuard workstation and server endpoint Zero-Breach security solutions, allowing organizations within the nation's critical infrastructure to seamlessly and strategically meet the new demands of Zero-Trust, Cyber Resilience and Incident Response identified within the most recent May 2021 executive orders that set the stage for immediate initiatives in 2022 and ongoing objectives for the years to follow.

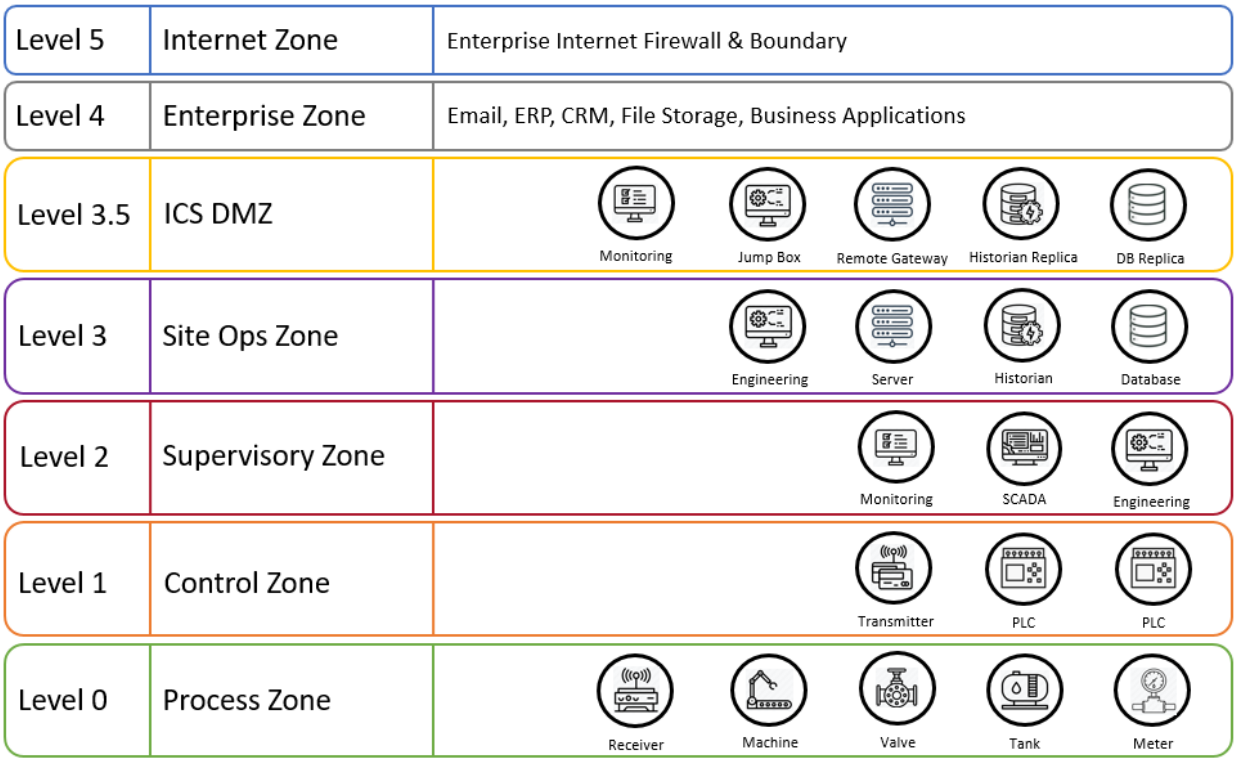
In addition to the Zero-Trust principles, the Zero-Breach solutions, specifically for IACS and OT

environments, provide operations and automation managers, engineers, and practitioners the capability to align industrial control systems and supporting technologies to the proven ISA/IEC 62443 standards and the Purdue Enterprise Reference Architecture, creating the necessary defense-in-depth logical "zones" and "conduits" within the policy-driven Zero-Breach configuration and management console.

Regardless of the current state of local, remote, centralized, or distributed network infrastructures, connectivity, and communications, the Zero-Breach "cyber-cloaking" or security overlay, delivers a purpose-built and practical strategy for ICAS/OT-centric security management, policies, procedures, and best practices for a secure-by-design architecture ensuring the IACS and OT components to be secure-by-design and to be governed by an OT/IACS-centric security management system that has policies, procedures, periodic review, specific requirements and instill best practices.

Traditionally, "air-gapping" limited interconnections between OT and IT environments and provided security to track north-south traffic communications at the network level. Where it was needed, Next Generation Firewalls were added to control and filter traffic between each of the layers. As next generation converged designs have rolled out, building leaders have realized conventional IT processes, including segmentation via complex VLAN and firewall configurations offers more problems than solutions. Furthermore, the complexity of these designs has often created misconfiguration issues resulting in prolonged downtimes that cannot be tolerated in the OT environments.

The safety of these critical infrastructure systems are weakened with a lack of defined boundaries and broadening of services and vendors that must be trusted. These security considerations must be understood and bounded for efficiency and profitability. Models like the Purdue Enterprise Reference Architecture (PERA) depict clean delineation and separation of functions and protections between those systems. The truth in most deployments is much different.



The problem of creating and maintaining clean functional grouping is even tougher for geographically dispersed systems such as pipelines or water/wastewater systems. In those architectures, the issue of secure communications and trust, or more specifically – risk, becomes exponentially complex. This is due to limited funding and a dependence on public communications mediums in order to connect those systems.

The ISA/IEC 62443 standards do not directly supersede nor replace the ISA95 and Purdue models. Instead, they leverage previous concepts, and divide security and management of cyber risk into several areas. These cover not only cyber security reference architectures, but also guidance for security processes, requirements, technology, controls, security acceptance/factory testing, product development, security lifecycles, and a cybersecurity management system (CSMS). The 62443 standards reach beyond ISA95 in terms of coverage, cybersecurity and modern concepts, but ISA95 and the Purdue models may still have value for organizations that have specific security requirements, for example when Industrial Internet of Things (IIoT) devices are connected directly to the Internet or the cloud.

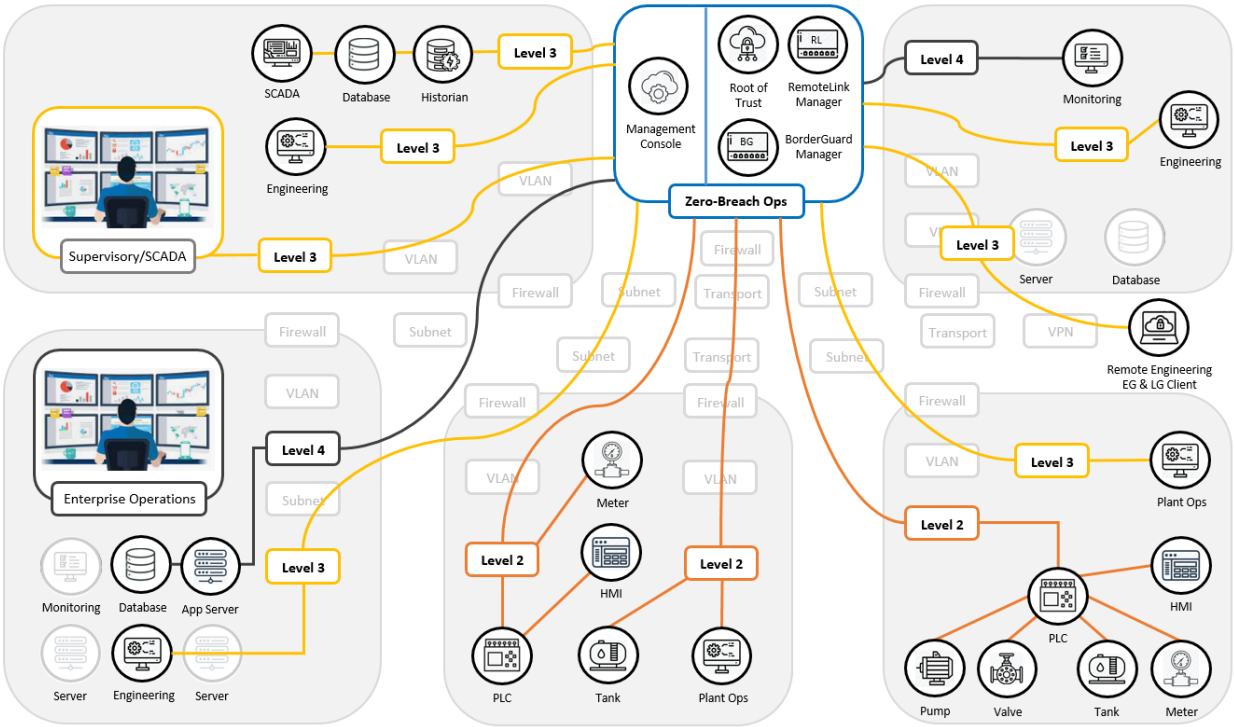
When considering distributed architectures or technology-related trends such as the Industrial Internet of Things (IIoT), where physical hierarchy and communications mechanisms are much harder to define, the model is viewed as an abstraction and solutions are needed to provide the structure. Zero-Breach LinkGuard solutions provide the required security, with ease of deployment, and the capability to mirror or create the hierarchal structure based on the Purdue Model with the logically

configured enclaves that serve as the “zones”, and policy-driven trusted pathways that provide the “conduits” of communication.

The Zero-Breach Solution

Blue Ridge Networks Zero-Breach solutions and deployments have delivered advanced threat protection without the lag of detect and respond approaches. This approach has been proven in the most hostile of environments over Blue Ridge Networks’ 24-year history supporting governments and military organizations. Blue Ridge Networks’ software, systems, and services solutions employ advanced cybersecurity technologies that “cyber-cloak” network assets and data-in-transit to eliminate risk of breach and protection lag from unknown vulnerabilities. These cyber-protected enclaves prevent external discovery and data exfiltration of protected operations.

The virtual and cyber-physical solutions deploy easily and are compatible with existing and future IT and OT infrastructure reducing integration complexity and costs. They can be easily tailored to resiliently protect a wide-range of use cases without disruption to critical operations. solutions work autonomously with no dependency on management system connectivity to maintain protection with minimal overhead or latency on network operations. Our software, systems, and managed security services enable optimization of cybersecurity capabilities to increase enterprise productivity.



Zero-Breach "cyber-cloaking" with the policy-driven LinkGuard security overlay allows the organization to obfuscate, as depicted below, the critical water and wastewater assets and operations from the rest of the threat vectors and vulnerabilities within the infrastructure identified on the previous graphic, while adhering to ISA/IEC 62443 zones and levels.

Nearly all IIOT systems are extranets. By this, we mean they cross organizational lines, perhaps even spanning multiple companies, including vendors who provide OT systems support. Strong authentication systems are considered a bedrock requirement for good cybersecurity. For lack of cost-effective and supportable strong authentication systems, most extranets employ week, shared-secret authentication. This is an invitation to credential theft and subsequent unauthorized access by attackers.

From its first generation, LinkGuard has incorporated its own public-key trust system, still considered the gold standard for network authentication. For robustness, it was essential from the start that it incorporated its own infrastructure with no external dependencies. Other products may use public-key technology, but invariably require expensive and complex infrastructure.

LinkGuard uses a technique called pre-placed public keys, managed by the LinkGuard Management System. By pre-exchanging the public keys, the management system establishes mutual bilateral trust among each pair of appliances that constitute a LinkGuard enclave. Once established, any two of these devices in trust may establish a strongly authenticated connection without dependence upon a third element, including the management system itself. This is a strong distinction from many other authentication systems that are transitive in nature and require active reference to a third-party component. Examples include X.509, Microsoft Active Directory, Radius servers, and Kerberos with its many variants. The mandatory mutual public-key authentication of LinkGuard enables two other features: stealth operation and quantum computer resistant public-key operations.
Well-known communications encryption systems like IPsec or TLS have explicit or implicit dependencies on communications media and protocols. For instance, the effective security policy in IPsec is a function of configuration as well as the address content of the packet presented to the device. This effectively allows a potential attacker the ability to vary inputs and observe the results to discern the preconfigured policy. This is a simplistic example of fuzzing, a well-known cyber reconnaissance technique. LinkGuard's security policy is mandatory and invariant.

Conclusion

It is imperative for water utilities to perform a thorough assessment of IACS and OT systems and assets and understand vulnerabilities, followed by devising a robust plan for ensuring cybersecurity throughout their digital implementation efforts. Planning today for the secure infrastructure of tomorrow should be a top priority in this transformative time. The water industry's technical

innovations, the benefits to the organizations, the consumers, and the environment will require the secure, reliable, and practical approach that assures access to this valuable resource well into the future.

Even though most of the current standards enforce only large facilities to act now and be audited on a regular basis, the relevance to small and medium sized water and wastewater plants and networks is of similar relevance and should be implemented based on the same comprehensive methodology. Isolation and segmentation of water and wastewater plant networks and distributed infrastructure with Zero-Breach solutions can help ensure protection and prevention from cyber threats and attacks.

Considering water supply and wastewater disposal as critical infrastructure implies the need to develop a security strategy and take countermeasures to continuously protect and secure the operation of water and wastewater plants and networks. Blue Ridge Networks, and the Zero-Breach LinkGuard and AppGuard product solutions provide the components necessary to implement the desired security level with a policy based defensive solution that reduces your attack surfaces and works against zero-day attacks. Take control and defense your systems verses hoping other systems work in time. Real-time, policy based, breach prevention.