SIGA
Level Zero OT Resilience

Cybersecurity for the Water industry

White Paper

April 2023

Cybersecurity is a top priority for the water sector

A safe water supply and effective wastewater management are crucial elements of modern economies. To better manage growing demand, water authorities worldwide invest heavily in automation and computerization for water purification, wastewater management, desalination, storage and delivery. Water infrastructure ecosystems have zero tolerance for downtime, human risk and failure. Yet despite ever-tighter regulations and increasing public scrutiny, reliance on sensor data for decision-making leaves critical water infrastructure dangerously exposed to attack or failure.

The Critical Infrastructure and Security Agency (CISA) issued a special advisory on cyber threats to U.S. water and wastewater systems in October 2021. The advisory was released in conjunction with partnering agencies the FBI, the EPA and the NSA. It described ongoing malicious cyber activity targeting the information technology (IT) and operational technology (OT) networks, systems and devices of U.S. Water and Wastewater Systems Sector facilities.

A recent survey by CISA found that out of the small number of water supply facilities across the country that choose to receive cybersecurity assistance, one out of 10 had a critical vulnerability. And more than 80% of the vulnerabilities were related to previous software flaws that emerged before 2017. This meant that too many water system operators had not taken the critical steps to keep remote access software patched and updated.

Regulators have a good reason to send out an urgent call for water organizations worldwide, cyberattacks on water infrastructure can have a devastating potential – not only to the organizations but to entire nations.

A History of Water Security Challenges

Although when we think of cyberattacks the principal concern is the severe disruption to business operations, in the case of water facilities, the most alarming preoccupation actually relates to public health, and the disastrous consequences they may bear. In the US alone, there have been some serious cyberattacks that threatened the supply of potable water, management of sewage water and affected water diversion. A disturbing example dates back to the year 2016, where hackers breached a regional US water utility, taking control of hundreds of programmable logic controllers (PLC's) that governed the flow of water treatment chemicals and endangering thousands of lives. This incident, which in part led to the US Water Infrastructure Act of 2018, highlighted the inherent vulnerability of critical water infrastructure worldwide.

Most global water OT (Operations Technology) infrastructure, despite being automated and computerized, are still not resilient in the face of cyberthreats, natural disasters, and equipment malfunctions. Malicious manipulation of data or malfunction can leave operators blind to the actual state of critical assets and result in costly or even catastrophic downtime.

There are many types of threats which challenge the water sector. Hackers can gain access to these critical systems and execute a series of harmful actions without ever being accounted for them. For every example we know of, there are probably plenty more that we are unaware of. Nevertheless, the examples we have at hand clearly demonstrate the extent of control these hackers gain over mission-critical systems and the horrifying things they can do.

A History of Water Security Challenges

While you might think that the menaces on water treatment facilities relate only to manipulating the critical systems, you will be surprised to be informed that the water sector is also susceptible to ransomware attacks. *Thames Water* a UK based company providing water to 15 million people across London and the Thames valley has experienced a ransomware attack in what seems to be the worst timing possible, amidst Europe's 2022 dire draught. Although the attack itself did not directly harm the systems on the facility, the sole fact that the entire operations and information of this organization was held by malicious actors, raises the atrocious implication this attack can have - denying water supply to millions of people, knowing that there is no other provider that can back-up their services, leading to a calamitous humanitarian crisis.

Up until this point we have seen the tremendous deal of threats the water sector is dealing with, from Ransomware attacks to Insider threats, as well as "classic" cyberattacks. As we have seen above there's in no country that is exempted from such threats: Australia, USA, Israel, UK, and still counting. Water facilities across-the-board are attempting to take measures to protect themselves from such assaults.

The OT Environment in a Water Facility

The OT environment in the water sector can be divided into 3 major sections:

- **Drinking Water preparation, treatment, and distribution:**

  including Desalination plants, water Treatment plants, holding and distribution facilities.

- **The Water Consumers**: mainly residential, agricultural, and industrial users.

- **Wastewater treatment and Water recycling plants**

The main assets and control measures in these assets include various physical and cyber-physical machinery and sensors. These may include - feed pumps, filtration units, chemical dosing, membranes, high pressure vessels, water quality assurance and metering, water level control, water disinfection, steam generators, demineralized process water, separation and oxidation methods and many more.

Addressing OT Cyber Security attacks on a water facility with SigaGuard

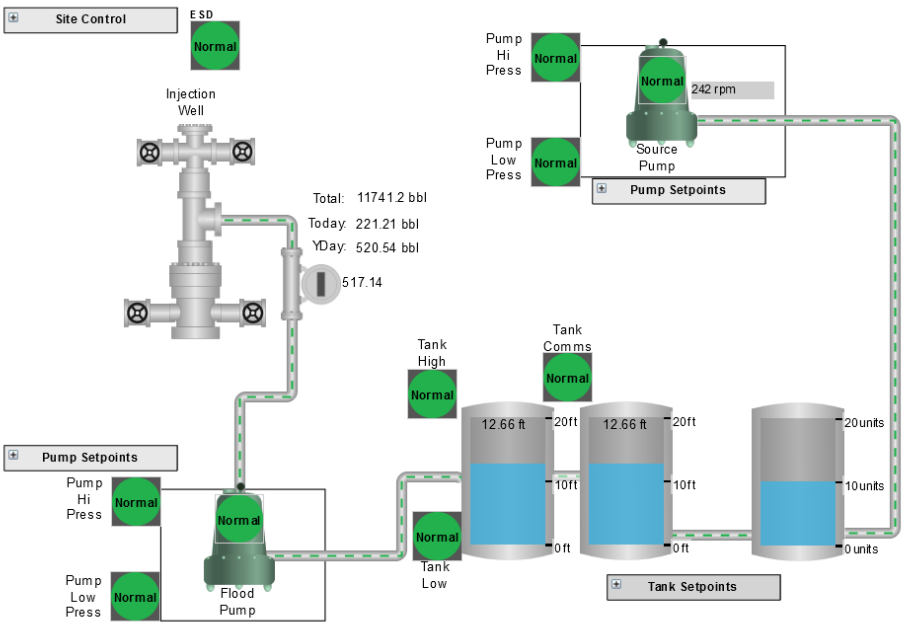
There are several attack vectors that can compromise a water facility which could lead to dangerous results. Below are three different attack scenarios on a water facility's control systems which could be thoroughly examined:

Scenario no. 1 – Increasing chemical dosage volumes in drinking water

In this scenario the attacker may attack the chemical dosing pumps in a drinking water treatment plant, in order to deliberately change the amount of chemicals and contaminate the water. The attack could cause the water facility's control systems to malfunction, leading to the release of harmful chemicals in an unsupervised quantity into the water supply. This could cause illness, injury, or even death to people and animals that consume the contaminated water.

Scenario no. 2 – Disruption of water supply

Cybercriminals can introduce malware into the water facility's computer systems through phishing emails, malicious websites, or other means. The malware could then target the industrial control systems in order to disrupt critical systems or shutdown the water supply.



Addressing OT Cyber Security attacks on a water facility with SigaGuard

Scenario no. 3 – Exploiting remote connectivity

The water infrastructure is characterized by widespread geographically dispersed facilities, many in remote locations. In many cases these facilities have remote connectivity to their systems to ease the maintenance and supervision to these site. Contractors in many cases are involved in opening remote access in order to avoid the need for physical access to the remote site. The remote access may be set up negligently, with minimum security or with none at all.

There have been many cases where threat actors exploited these remote connections in order to gain access into the control systems. Even employees or contractors with access to the water facility's computer systems may intentionally or accidentally cause damage to the water facility.

Implementing SigaGuard in the water sector

It's important for water facilities to implement robust cybersecurity measures, including firewalls, intrusion detection systems, and employee training programs, to mitigate the risk of these and other types of cyber attacks. As governments and organizations plan to increase their expenditure to secure the water infrastructure, we are still left with a vital question to answer – How can we ensure cybersecurity resilience of water infrastructure, bearing in mind that hackers outnumber organizations' budget and workforce? What can water companies and governments do to 'out-smart' the hackers?

There are several cyber protection tools in use in the OT environment of water facilities today, all of them are focusing on Level 1 or the above levels of the Purdue Model, aiming at the protection of the OT network and its components.

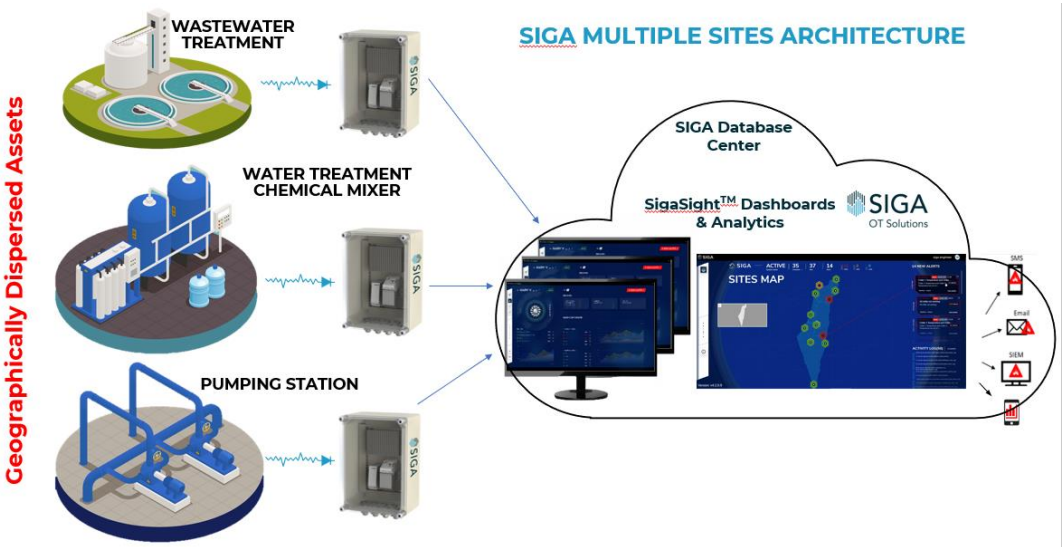
The cyber monitoring and protection system monitors the OT network and computer servers, but they do not , however, monitor the control systems and process operation. Hence, the most critical layer of the OT environment, Level 0 (the physical layer), is exposed to numerous kinds of cyber-attacks. Additionally, most of the water facilities get remote support, normally used to install software or firmware updates to the control systems, leaving Level 0 unattended as the perfect breach for perpetrators, facilitating their access to the most critical assets, and thus increasing the probability of it being attacked.

Despite the air gap between the protection systems and other OT networks, this barrier can be easily overcome by today's highly sophisticated attackers.

This challenge can be addressed by monitoring the most reliable source of data for OT environments, namely the non-penetrable physical source – the raw electrical signals of Level 0 coming from the sensors and actuators. This source of data is rich & unfiltered, un-hackable, and often unavailable to operators.

By activating Machine Learning on the electrical signals at Level 0, SigaGuard delivers an autonomous cyber inspection & analytics solution, offering bullet-proof detection of any cyber-attack on the physical layer, inaccessible insights, and operational resilience of industrial processes and automated machinery. SIGA's cutting-edge technology capitalizes on this unique level to deliver operators with inaccessible insights to combat cyber-attacks in real-time. SIGA forefront platform tracks the electrical signals coming directly from the machines, by connecting to the sensors and actuators on the critical assets. This rich data is transferred in a unidirectional manner to SIGA's innovative ML/AI engine to process the information and deliver operators with unparalleled situational awareness.

SIGA is a completely out-of-band solution, fully dedicated to Level 0, to ensure that while SIGA lights the darkest corners of your operational processes, your processes can proceed without any disruptions. This valuable information is always presented through SIGA's interactive dashboard that sends out real-time alerts to ensure operators are aware of their critical assets' state. SIGA's solution is a highly dynamic one, it is compatible with other solutions in higher levels of the Purdue Model (Level 1,2, etc) and can also adapt to the organization's preferred environment.



Summary

Managing cybersecurity is a complex challenge that requires an interdisciplinary, risk-based approach, involving an organization's business leaders, as well as their technical and legal advisors. A robust and tested cybersecurity method is critical to protect water infrastructure, and by doing so protect public health and safety, prevent service disruptions. The diverse nature of the water and wastewater sector, with organizations of varying size and ownership, calls for the implementations of innovative solutions to protect this vital services and minimize the potential terrifying consequences of cyberattacks on these organizations.

Level 0 is the ideal way to address the issues faced by the water sector, ensuring visibility like no other solution does, for the sake of detecting attacks as soon as they initiate, to provide operators with unparalleled insights to mitigate the industry's threats.

About SIGA OT Solutions

SIGA OT Solutions (https://sigasec.com/) is securing the integrity of critical OT processes by delivering AI enhanced monitoring and in-depth operational perception. SIGA's Solution, SigaGuard, is a unique comprehensive OT cyber security solution for critical infrastructure and industrial assets using ICS/SCADA electrical signal-based advanced analytics, Artificial Intelligence and Machine Learning. SIGA is providing out-of-band real-time OT sensors and processes monitoring and analytics for safeguarding the critical industrial assets.

SIGA OT Solutions, has implemented SigaGuard in the United States, Canada, Europe, Singapore, Japan, Dubai and Israel. SIGA holds approved US & European patents with additional patents pending and is also certified with the ISO/IEC 27001 information security standard. SIGA was named a "Cool Vendor" in Gartner's "Cool Vendors in Industrial IoT and OT Security" for 2018, awarded the European Union's "Seal of Excellence" in 2019. SIGA is a partner in two different development project consortiums: as a part of the EU's H2020 program and as a part of the BIRD Foundation Energy Center program – both for developing cyber protection toolkits for the energy sector.