BAYSHORE
Industrial Network Security

INFORMATION SECURITY AND A PRACTICAL APPROACH TO THE DEFENSE OF WATER SYSTEMS

Is The Water Industry Prepared for An Attack?

For over 20 years now, the enterprise IT security industry has built solutions around three simple concepts: Confidentiality, Integrity, and Availability. Entire product categories and methodologies have consumed hundreds of billions of dollars of R&D investment, and the industry's best practices have matured into a robust set of frameworks and real solutions. The problem will never be "solved" but it's no longer an anomaly for a midsized company to have an information security officer and at least some amount of skills and ongoing budget to defend the information assets from malicious or accidental compromise. As Sun Tzu taught us in the 5th century.

Attackers seek to exploit our weaknesses with overwhelming force and where we are most unprepared.

Any casual reading of the news will reveal that products and procedures to protect from compromise is not yet universally deployed, but efforts are being made to mitigate risk, even if we may not always publicly hear about the impact of the efforts. What is clear is the scale of reconnaissance activity — building an inventory of known vulnerable targets — is running at a level many orders of magnitude higher than it was even five years ago.

Comparing enterprise information security to the security of physical plants, we've seen isolated investments as a result of certain federally-designated critical infrastructure categories. Bulk power, financial systems, and transportation have all enjoyed real investments in security and adapted when efforts were shown to be inadequate or ineffective. We'll discuss this in greater detail below, but for now, it's sufficient to accept that it is possible, despite all the bureaucracy, budgeting, and political challenges, to improve the security of physical infrastructure in a meaningful degree with practically applicable solutions.

Despite the evolution of stronger security options and with full knowledge of the potentially catastrophic effects of a disrupted water supply, power grid, or emergency response network, most physical infrastructure in the western world has little or no significant cybersecurity protection in place. We've learned how to do it on the enterprise side and in the designated critical infrastructure sectors where it "matters most", but what about everything else?

Twenty years after the advent of information security as an industry category, we face a major gap in degrees of preparedness and a critical mass of risk and attackers willing and able to exploit these connected networks which are relatively unprotected. Many of these networks are the economic lifeblood of regional employers, or the enablers of vital resources to communities: power, communications, and water. Large telecom companies at the national scale are more mature in their security practices, but many local or regional carriers, as well as municipalities, power cooperatives, and water plants, are all woefully behind.

Further compounding the problem is a budgeting process which isn't yet oriented around the ROI of risk management and security spending, and a workforce which does not lend itself to rapid recruitment of security professionals.

Contemporary Approach Based on AWIA 2018

It wasn't until the passing of America's Water Infrastructure Act (AWIA) in 2018 that the EPA received concrete guidance on protecting our nation's water. Section 2013(a), in particular, provides the first actionable goals via "Community Water System Risk and Resilience."

It requires that community water systems first undertake an assessment for the risk of malevolent acts and natural hazards, and, second, implement an Emergency Response Plan, which illustrates strategies and resources to improve the resilience of the system to include cybersecurity risks.

The 2019 National Defense Authorization Act created a new entity intended to drive the United States towards a comprehensive cybersecurity defense strategy, and critical infrastructure is one of its areas of focus. The entity, known as the Cyberspace Solarium Commission, will issue recommendations in the Spring of 2020. These are meant to be prescriptive and will be framed as a defense-oriented activity, rather than an academic or research objective.

One of the most pressing issues about water systems is their age, and that networking technologies have been retrofitted to existing water processing equipment. The transition to the Industrial Internet of Things (IIoT) has been pursued with varying enthusiasm across the country, but most plants have at least some networking infrastructure linking the machines to the control rooms. Such additions were done with little use of embedded security protections because it is believed that the difficulty of gaining physical access to a water plant is sufficient protection from most threats.

One of the most pressing issues about water systems is their age, and that networking technologies have been retrofitted to existing water processing equipment.

A Practical Approach to the Defense of Water Systems

If an automated environment is compromised, there are immediate real-world effects. Regardless if the original intention was malicious, accidental or simply unexpected, the product is lost, the lights go out, and people can't get water from the tap. Worse still, than no availability, is if the water is contaminated and users don't know how or why.

Large-scale water supply problems can impact millions of people, and even if the utility can notify 95% of customers within 6 hours (which is in and of itself highly unlikely), the consequences of the remaining 5% being ignorant to the risk are potentially catastrophic.

While understanding why network issues happen is an important question worthy of investigating, the #1 priority of Bayshore's technologies is to keep the plant online and safe. Bayshore Networks, founded in 2012, has developed security products specifically for OT environments. Its comprehensive technology inspects industrial network activity in real-time, to protect assets whenever anomalies appear. The company created SCADAfuse, SCADAwall and OTaccess to address the challenges of availability, integrity and confidentiality of OT environments.

The following table outlines the cybersecurity risks to OT networks, within the prioritized ICS framework of availability, integrity and confidentiality. The eleven impacts of ICS Attacks as defined by the MITRE ICS ATT&CK Framework can be categorized into this framework.

- *Availability impacts include actions which result in the following: Loss of Control, Loss of View, Damage to Property, Denial of Control, Denial of View, Loss of Availability, Loss of Productivity and Revenue, Loss of Safety*
- *Integrity impacts include actions which result in: Manipulation of Control and Manipulation of View*
- *Confidentiality encompasses actions that result in: Theft of Operational Information*

SCADAfuse
Automatic Industrial Firewall

SCADAfuse is an automatically configured industrial firewall and intelligent Intrusion Prevention System (IPS) designed for easy deployment and use by automation engineers.

It is a physical device that sits in front of critical utility endpoints protecting PLCs, VFDs and other network connected devices. It learns and enforces normal operations for your plant environment, and actively eliminates threats to OT assets in real-time.

SCADAfuse enables customized policies to ensure integrity of access and content of your unique environment and protect the ICS network from unauthorized config changes, device resets, device reads, logic updates and message values.

It is your last line of defense for protecting plant assets from unauthorized or unintended (mis)use.

How SCADAfuse Protects A Water Plant From Loss Of Availability

SCADAfuse protects the PLCs and other critical assets in a water plant from loss of availability. The assets will keep doing tomorrow what they were doing yesterday and today. No matter what happens, SCADAfuse ensures that those assets continue to take only known good instructions from known good sources and to block any deviations from that baseline.

SCADAfuse introduces strong security measures and operates via a transparent bridge mode at runtime. It seamlessly integrates into existing environments with no disruptions. SCADAfuse is effectively invisible to the protected assets and workstations. Due to these traits, the introduction of SCADAfuse to an environment seeking deep security requires no other networking changes, and a strong security posture is achieved with minimal effort.

SCADAfuse is an innovative approach to the generation of subjectively enforceable security policies. Its learning engine is designed to provide highly specific security rules based on an automated assessment of the network behavior patterns and resulting policies.

Rules are constructed based on learned traffic patterns encountered in the protected environment and surpasses what any generic set of rules could achieve given the number of unique possibilities within different ICS communication protocols and environments. The generic rules utilized by typical firewalls, are in fact, largely ineffective because in multiple environments running the same exact ICS communications protocol(s), there can be highly customized and modified variants.

To be truly useful, products operating in an OT environment need to understand the operational ranges of values such that threshold, or out of range violations are detected and handled accordingly based on the needs of each individual customer's environment.

SCADAfuse allows two responses in handling violations:

- *raise alerts or notifications, yet allow traffic to flow*
- *actively block traffic flows*

Beyond automated learning of appropriate policies for each unique environment, SCADAfuse allows experts to make modifications of these rules via a web-based graphical user interface (GUI). This is accessible from the control room but is protected from unauthorized use via the same protection policies SCADAfuse uses to protect PLCs from unauthorized access.

Bayshore Products Address Risks to Availability, Integrity and Confidentiality of Water Systems

Bayshore products protect water plants from accidental or malicious risks, at the perimeter, across the airgap and at the endpoint (PLCs and other Purdue level 0/1 assets).

- ***Bayshore's SCADAfuse*** *product is deployed as the last line of defense. It is a physical device that sits in front of critical utility endpoints and automatically prevents unauthorized actions and communications*

- ***Bayshore's SCADAwall*** *product creates a secure bridge across otherwise sensitive, air-gapped portions of the OT network while eliminating the risk of unauthorized changes*

- ***Bayshore's OTaccess*** *product limits unexpected access and communications from the perimeter of the OT network — either from the IT network or from remote access*

About Bayshore

Bayshore Networks was founded in 2012 and has developed security products specifically for OT environments for use by automation engineers and plant operators.

Its comprehensive technology inspects industrial network activity in real-time, and actively protects assets whenever anomalies appear. The company created SCADAfuse, SCADAwall and OTaccess to address the digital security risks which can compromise the availability, integrity and confidentiality of OT environments.

All Bayshore products are designed with five OT network centric principles to provide effective, practical deployment and use in OT environments. These capabilities are integral to every Bayshore product and are the differentiating factor between Bayshore and competitive solutions which are typically enterprise IT security products adapted for industrial environments.