BAYSHORE
Industrial Network Security

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

# TABLE OF CONTENTS



# 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.

# Three Categories of Unexpected Risk

This white paper reviews the water industry in general, and how it supplies and delivers a critical resource to essentially the entire globally developed population. Despite this, it has been almost entirely overlooked in terms of adopting security protections to account for the three categories of information security risk:

- *Availability:* *the #1 concern for all operators, and potentially a critical health and safety issue;*
- *Integrity:* *how to protect the target system from unauthorized changes; and*
- *Confidentiality:* *how to protect the details of the system from unauthorized access and misuse*

# History of Public Infrastructure Security

It wasn't until 1998 that the United States created the formal notion of Critical Infrastructure Protection (CIP). These standards covered several sectors, but in practice, most of the identified sectors did not receive attention from the information security product vendors and thought leaders. The most notable exception was the North American Electric Reliability Corporation (NERC), which took the Presidential directive and ran with it.

The private sector didn't sit idle and wasn't constrained solely to the interests of the United States. From the late 1990s onwards, tremendous efforts on enterprise IT security were made as technology was created and evolved rapidly, standards for governance and best practices were modeled and refined, and wily attackers continued to stay, in general, one step ahead.

This dynamic remained unchanged throughout because of information asymmetry. An attacker, once in possession of the knowledge to perform an attack, doesn't have to act immediately. The owner of the intended target has no way to know the potential for specific compromise exists, even if they use vulnerability management tools. These tools assign degrees of risk that are blind to the probability of actual compromise within a stated period. It is a problematic situation because network owners are left with either disregarding the practical risk or defending against an infinite set of unknowns.  Consider the ability to compromise a water supply at will, with its operator being none the wiser.

Information asymmetry enables attackers to stay one step ahead.  Consider the ability of an attacker to compromise a water supply at will, with its operator being none the wiser.

***Information asymmetry enables attackers to stay one step ahead.  Consider the ability of an attacker to compromise a water supply at will, with its operator being none the wiser.***

# Example: The Three Types of Risk Within Airline Security

In the period following the 9/11 terrorist attacks, there was an intense focus on airline security. Investments were made in background checks, increasingly intrusive airport screenings, and rules governing what could be carried onboard a plane. Many of these changes – implemented uniformly across the entire US traveling public – were in response to isolated incidents. It is naive to believe that these changes will protect against all possible future incidents, but everyone, nevertheless, accepts the restrictions and inconveniences because there is no alternative if we want to board a commercial flight.

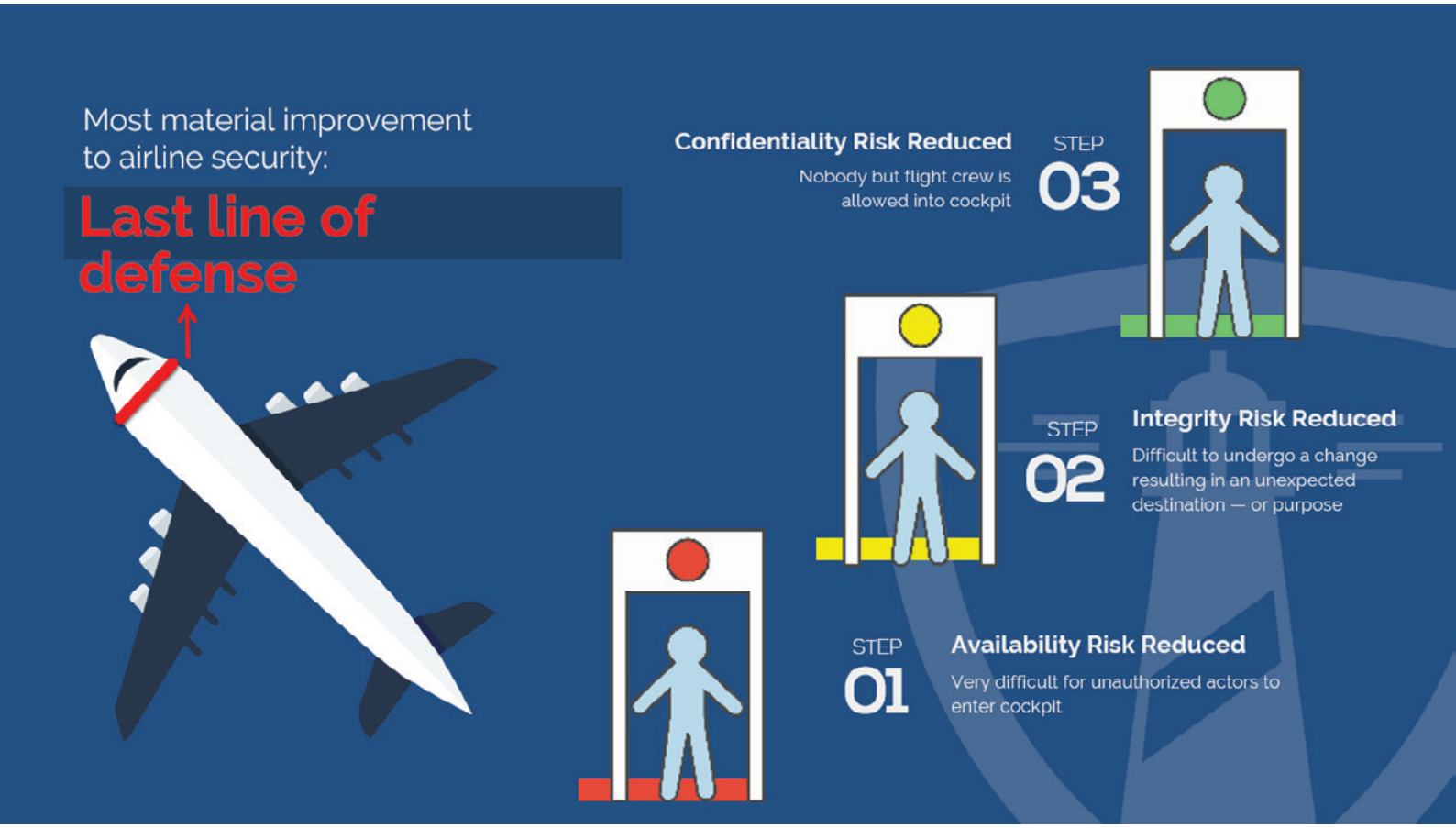
## Most material improvement to airline security: Last line of defense

In practice, the most material improvement to airline security didn't take place in the airport terminal, or in databases operated by DHS to track passenger data. It took place at the last critical boundary when a plane is in flight: the cockpit door. All US commercial passenger aircraft now use deadbolts in flight, along with special protocols when one pilot leaves the cockpit to ensure two people are present at the flight controls at all times.

This is what makes the difference when all other measures have been overcome by cunning attackers or simple accidents.  If you identify an aircraft as a potential weapon, the crown jewels of that aircraft are its flight controls.  If an attacker cannot get into the cockpit, he cannot take them over.  The effort now required to compromise a flight is significantly higher, and the risk to the population outside that aircraft is greatly reduced. This strategy is a combination of correctly identifying the last line of defense, and making the hard decision about what defines an acceptable risk.

In terms of the three risks introduced previously, the strategy directly addresses all of them, to a reasonable degree.

- *Availability risk is reduced because unauthorized users cannot gain access to the control center of the plane — the cockpit.*
- *Integrity risk is reduced because the aircraft is less likely to undergo a change resulting in an unexpected destination — or purpose.*
- *Confidentiality risk is reduced because there is a single, unambiguous condition which isn't permitted under any circumstances, and any attempt to review or modify that is immediately detectable. Nobody outside the flight crew is allowed in the cockpit while in flight.*




In the power industry, robust governance, coupled with a federal mandate to achieve compliance with the evolving CIP standards, has helped improve the overall standard of practice for bulk power transmission systems and related power generation sites. As a rising tide lifts all boats, we've seen trickle-down effects for better-funded (but not compliance-obligated) sites to pursue similar levels of cybersecurity proficiency. While most experts would agree we're not anywhere close to where we need to be as a nation, in general, it's not unreasonable to say that things are better than they were.

But what about areas of public infrastructure outside of power, or transportation? There are other types of systems that collectively impact almost everyone in the country, as well as neighboring countries.

# WATER SECURITY

## History of Water Security

Public water systems were anticipated in the original CIP directive, but water systems fall within EPA jurisdiction, an agency not oriented around threat modeling in the same manner as DHS or NERC. Indeed, the notion of attacking the public via the water supply isn't new. It's featured frequently in everything from Hollywood films to conference presentations.

Historically the risks to public water systems were illustrated during major storm conditions when storage tanks overflowed and the physical separation between circuits within the treatment systems were cross-contaminated. There is minimal separation between "safe to use" and "unacceptable risk" during those conditions, and there is no easy way to provide rapid response. Cleaning a contaminated water system starts with a Boil Order (for organic contaminants), but only if there aren't other dangerous materials in the system. As witnessed in Flint, Michigan, sometimes the system itself is the source of critical risk; there is no easy way to replace lead pipes with another delivery method.

Even with the original Presidential Directive, only three areas of designated critical infrastructure received attention: bulk power, transportation, and financial services. All three share a common attribute: they recognize that a malicious attack is likely, and identifying ways to mitigate it is imperative.

Bulk power transmission has an innate capability to create cascading failures across large swaths of the country, and even across borders, as we saw in 2003. Water systems, in contrast, are generally defined by more local geographic boundaries, and while contamination can certainly propagate to adjacent sites, it generally does so more slowly. In addition, the fail-safes built into water systems – in terms of foreign agent detection, filtering, and redundant capacity – also help insulate the public from these lower-level threats.

Bulk power, transportation, and financial services all enjoy significant budgets, enforcement options, and industry attention, while the other areas of critical infrastructure have largely been overlooked. This is slowly changing.

## 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.***

## Physical Access No Longer a Deterrent

In reality, physical access is no longer a prerequisite for unauthorized use, precisely because of the insecure robust-perimeter-oriented deployment models for typical networking overlays. These plants have mostly flat, unsegmented networks, with exposed network switch ports in locations with little or no practical supervision. More advanced sites have video surveillance systems and basic access control, but there is still a considerable gap between the typical water plant and the typical NERC CIP-governed bulk power facility in terms of security controls and governance.

***In reality, physical access is no longer a prerequisite for unauthorized use.***

## Protection and Monitoring

Where protection does happen, it is usually oriented around the physical process of water treatment and delivery. Protecting water systems from failure modes, aside from the regular monitoring and treatment process control, adds on a few core activities:

- *Monitoring inputs – the water source itself, any treatment media added, any runoff or treated wastewater which is fed back into the system*
- *Monitoring outputs – the product as fed into the various delivery circuits, staging tanks, pumps, and towers*
- *A signaling system and set of procedures to ensure that the majority of consumers can be alerted when needed to avoid casualties arising from a lack of awareness of dangerous conditions*

A combination of occasional and real-time measurement techniques monitor inputs. Samples are collected at different points in the system and analyzed for chemical concentrations, pH levels, organic material, dissolved mineral solids, and various other factors. System performance is monitored in terms of pressure, flow, and temperature. Individual machines supporting the system are monitored for their levels of performance and responsiveness to instructions from the control system.

These monitoring techniques lend themselves naturally to the three categories of risk: availability is, in the simplest sense, about ensuring safe product comes out of the tap; integrity is about ensuring the process control isn't manipulated without authorization; and confidentiality is about ensuring inputs are kept as required and expected.

What is important now is that the role of performing those risk management functions cannot be left exclusively to the human operators, watching reactive status monitors. Threats on the automation control system, within the OT, do not reveal themselves immediately in terms of the safety and quantity of water produced.


## *Security Solution Must Keep Up with the Pace of Activity*

Marty Edwards, a former ISA Fellow, recently wrote an article (starting on page 10) equating the role of automation technology for the core activity to the need for automation technology in security incident response. The argument, in essence, is that automation enables both real-time processes and the ability to adapt to reasonable variation without having to initiate a full system shutdown.

***A security solution that cannot keep up with the pace of activity is not only unlikely to be useful; it is a net loss because the operators are forced to contend with alert fatigue and exception loops before deciding how to proceed.***

Furthermore, plant operators may not have the skills or perspective to make decisions, let alone the bandwidth to do it in real-time. In many cases, ICS cybersecurity solutions create precisely that problem: they perform passive activities, generate lots of arcane alerts, and leave the customer to stare at a huge backlog. Even if the alerts were valid, the customer's first priority would be to restore the plant, rather than to perform a root cause analysis on the security incident.

## *Opportunity To Improve a Water System's Information Security*

The community water system space is an extensive physical infrastructure used by hundreds of millions of people in the United States alone. It is rarely rebuilt and, therefore, on average, at least decades old. It has had automation systems added to it for production and monitoring purposes, and varying degrees of governance around the operating parameters themselves; security has had little or no practical consideration. The network designs and core technologies were installed with the first network-capable automation control systems 10-20 years ago and have hardly changed since then; they are flat and essentially unprotected architectures in most cases.

Also, the typical water utility operates a large number of physical sites within their system, many of which are unstaffed and have limited physical security. They are connected to an industrial control network via wired or wireless links, and it is hoped that they are inaccessible from corporate or public points of origin. In practice, this is not universally true.

The mindset of plant operators is to maintain availability and continuity of operation. The professionals responsible for plant safety know in detail what the machinery is meant to be doing, what the chemical payloads are meant to be, and who is meant to be making adjustments. There is tremendous institutional knowledge invested in this core, and any installed security program must leverage that knowledge first, rather than try to up end it with the introduction of new policies and procedures.

The opportunity then is to make improvements to a water system's information security, without disrupting normal procedures, requiring all new equipment, or introducing an unsolvable skills gap for incident response.

***Opportunity to improve a water system's information security without disrupting normal procedures, or introducing an unsolvable skills gap.***

## 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*

The following chart outlines some examples of specific accidental or malicious risks which could occur in an OT network, organized by Purdue Levels. For a more complete list, the MITRE ICS ATT&CK Framework outlines 81 specific techniques which can impact assets at Purdue Levels 1, 2 and 3.

# *Accidental or Malicious Risks*

| | Availability | Integrity | Confidentiality |
|---|---|---|---|
| **IT Network: Purdue Level 4-5** | | | |
| Unexpected access from IT network | ✓ | ✓ | ✓ |
| Unexpected remote access | ✓ | ✓ | ✓ |
| Illicit and accidental communications | ✓ | ✓ | ✓ |
| **OT Network: Purdue Level 2-3** | | | |
| Unauthorized wireless access point | | | ✓ |
| Data ingress across air gap | ✓ | ✓ | |
| OPC connectivity across air gap | ✓ | ✓ | ✓ |
| File transfer | | ✓ | |
| Attempted access by unknown device | | ✓ | |
| Unexpected access to isolated asset | ✓ | ✓ | ✓ |
| Abnormal workstation access | ✓ | ✓ | ✓ |
| **OT Network: Purdue Level 0-1** | | | |
| Protocol abuse/Denial of Service | ✓ | | |
| Asset and state reconnaissance | ✓ | | ✓ |
| Unauthorized automation instructions | ✓ | ✓ | ✓ |
| Unscheduled control logic update | ✓ | ✓ | ✓ |
| Unauthorized PLC config changes | ✓ | ✓ | ✓ |
| Unauthorized PLC data read/write | ✓ | ✓ | ✓ |

Bayshore's three products, SCADAfuse, SCADAwall and OTaccess, provide a layered security approach to protect water systems from compromise.

## 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.

## SCADAwall
Industrial Airgap Bridge

SCADAwall provides unidirectional data diode functionality creating an airgap bridge that controls, limits and enables communications from sensitive, restricted portions of the OT network. It provides isolated, non-routable, unidirectional data transfer such that no network information is exposed.

SCADAwall creates a full protocol break between two network entities, and thus transfers data without exposing machines to an untrusted network, and provides protection from unauthorized communications.

SCADAwall is a physical device that sits in front of sensitive portions of the network that alleviates the cost and complexity of physical only access or data diodes with an alternative connectivity option.

## OTaccess
Real Time Secure Remote Access

OTaccess provides secure, highly granular, remote access. It is more precise than any VPN through its ability to control access on a combination of policies configured per protocol + per activity + per seat, unique to your environment.

OTaccess policies are continuously enforced during remote access sessions and ensures OT assets and the OT network cannot be remotely manipulated outside of line of sight.

OTaccess is available as an on-premises hardware solution or as a cloud service. It minimizes the attack surface and enables the most secure option for remote employees or 3rd party vendors to access endpoints within the OT network.

# 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.

## How SCADAwall Protects A Water Plant From Loss of Integrity

SCADAwall protects a water plant's most critical machinery from the risk of unauthorized or unexpected network connectivity. This ensures integrity because there can be no unauthorized changes to specific machinery from the network which, in turn, improves the overall security posture for that machinery.

For most critical machines, there are very specific relationships required between the machine and a small number of workstations. The operator can state with near 100% confidence that only the enumerated connections and relationships shall be permitted; any other general network connectivity is therefore unnecessary and unauthorized.

Historically data diodes were used in highly mission-critical installations where logs and other data needed to be extracted from sensitive locations without introducing general network connectivity. SCADAwall enables a similar deployment model but at a far more accessible price point, and with greater flexibility than is possible with pure hardware diodes.

SCADAwall addresses precisely the need to transfer files from the most sensitive locations of the network to the rest of the OT network. With SCADAwall operators can retrieve status and monitoring data from the machinery without exposing that machinery directly to workstations and tools which could manipulate it without authorization — all such connections must pass through SCADAwall.

SCADAwall also supports OPC DA connectivity for arbitrary numbers of points and refresh intervals, again insulating the target device from all the general risks of malware propagation and reconnaissance activities possible over an unprotected TCP/IP network.

In essence, SCADAwall allows a water plant operator to limit access such that every asset could be accessible, but with varying levels of control and security.

## How OTaccess Protects A Water Plant From Loss of Confidentiality

OTaccess protects confidentiality (theft of operational Information) through policies that limit unexpected access and communications from the perimeter of the OT network — i.e. either from the IT network or from remote access.

It prevents Illicit and accidental communications from reaching Purdue Level 1/0 assets by automatically blocking any unauthorized attempts to contact physical assets, and is the 1st line of defense against risks such as Protocol abuse/Denial of Service, asset and state reconnaissance, unauthorized automation instruction, unscheduled control logic updates, unauthorized PLC configuration changes and unauthorized PLC data read/write.

In a water environment there are typically a number of physical sites within a single operation. OTaccess enables those to be accessed safely from anywhere by plant employees, and with the assurance that every connection is continuously monitored for policy compliance regarding read, read/write, or full access to the designated endpoint.

In addition, for plants using third parties to perform regular maintenance on OT assets, OTaccess provides a safe and uniform standard for third party risk management while providing the smallest possible attack surface for the level of remote access required. If your OEM maintenance staff only have three assets on your network under contract, there is no benefit, and significantly increased risk using a traditional VPN to give them access to anything beyond the essential services running on those three assets.

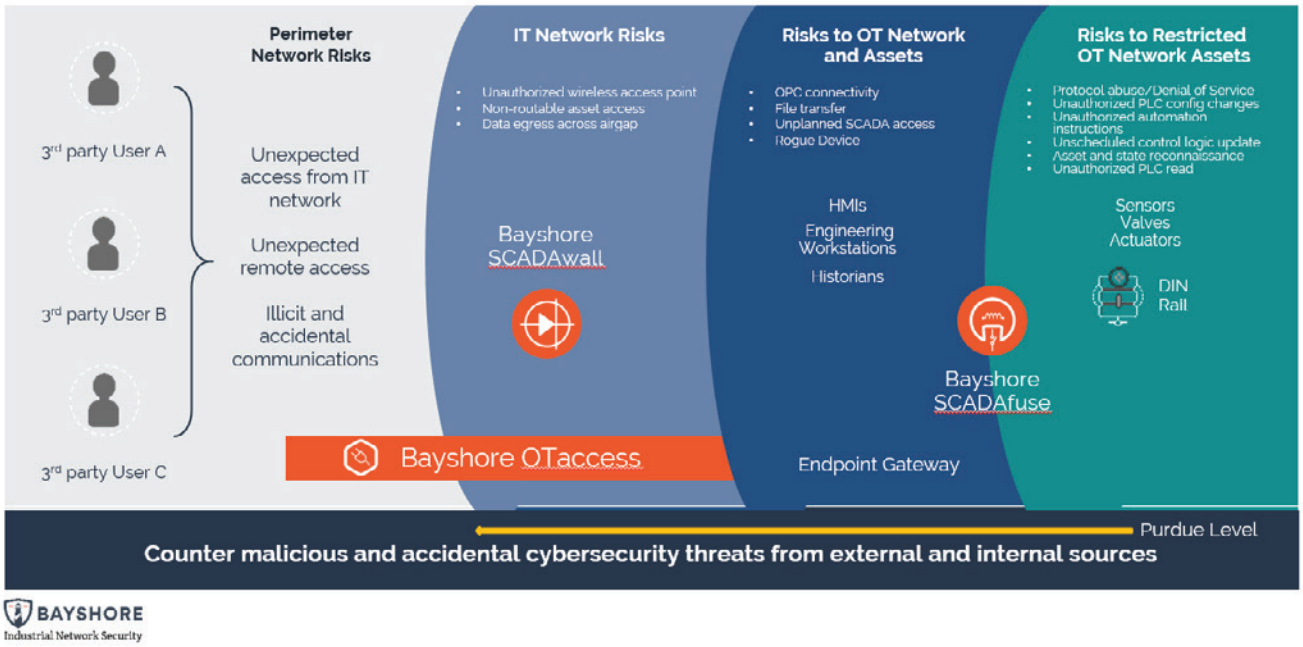
# Bayshore Products Address Risks to Availability, Integrity and Confidentiality of Water Systems

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*

| | Accidental or Malicious Risks | | | Mitigation | | |
|---|---|---|---|---|---|---|
| | Availability | Integrity | Confidentiality | OTaccess perimeter | SCADAwall airgap | SCADAfuse endpoint |
| **IT Network: Purdue Level 4-5** | | | | | | |
| Unexpected access from IT network | ✓ | ✓ | ✓ | ✓ | | |
| Unexpected remote access | ✓ | ✓ | ✓ | ✓ | | |
| Illicit and accidental communications | ✓ | ✓ | ✓ | ✓ | | |
| **OT Network: Purdue Level 2-3** | | | | | | |
| Unauthorized wireless access point | | | ✓ | | | ✓ |
| Data ingress across air gap | ✓ | ✓ | | | ✓ | |
| OPC connectivity across air gap | ✓ | ✓ | ✓ | | ✓ | |
| File transfer | | ✓ | | ✓ | ✓ | ✓ |
| Attempted access by unknown device | | ✓ | | | | ✓ |
| Unexpected access to isolated asset | ✓ | ✓ | ✓ | | | ✓ |
| Abnormal workstation access | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **OT Network: Purdue Level 0-1** | | | | | | |
| Protocol abuse/Denial of Service | ✓ | | ✓ | ✓ | | ✓ |
| Asset and state reconnaissance | ✓ | | ✓ | ✓ | | ✓ |
| Unauthorized automation instructions | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Unscheduled control logic update | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Unauthorized PLC config changes | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Unauthorized PLC data read/write | ✓ | ✓ | ✓ | ✓ | | ✓ |

## BAYSHORE ADDRESSES RISKS TO AVAILABILITY, INTEGRITY AND CONFIDENTIALITY




# 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.

## *Bayshore products all encompass the following capabilities:*

- *Native integration with procedures and tools already in use for daily operations.*
- *An operator-friendly deployment and usage model, defined and configured in terms of SCADA systems, Modbus registers, and vocabulary familiar to OT engineers.*
- *No specialized enterprise or IT security knowledge required to effectively deploy, integrate and manage.*
- *An affordable price point and budget-friendly purchasing options through existing suppliers to most water districts.*
- *World-class native OT security technology, protecting plant operators against a rising tide of native OT threats.*

Bayshore works with local integrators, engineering firms, and resellers, and would be glad to recruit any water plant's preferred partner to simplify the evaluation and procurement model. Please feel free to broker a mutual introduction based on your interest in the product, and we will arrange for onsite trials in your plant as soon as is convenient for you.