Whitepaper

Secure Connectivity for Utilities

Protecting Water and Wastewater Facilities against Cybersecurity Threats with Zone Segmentation and Conduits

In water and wastewater processing facilities, nothing is more important than security. Communities need to have pure drinking water and wastewater needs to be as clean as possible before being returned to the local environment.

While modern water utilities are working hard to prioritize security alongside performance, the game has recently grown tougher. Water treatment equipment and Programmable Logic Controllers (PLCs) are now more frequent targets of cyberattacks, bringing new urgency to the task. In December 2023, the FBI reported a series of breaches at water treatment centers that all targeted the same industrial equipment. In a high-profile incident in 2021, an unauthorized individual gained remote access to a PLC in a Florida water treatment facility and raised the levels of sodium peroxide to unsafe levels. (Thankfully, an employee monitoring the values caught the change before it could have any impact).

As cyber threats rise, water processing facilities may soon face more stringent regulatory pressure to shore up their defenses. In the United States, legislators have introduced a bill intended to address cybersecurity weaknesses in the water and wastewater sector in an effort to protect the nation's critical infrastructure.

For water treatment facilities, addressing these new security requirements in the Operational Technology (OT) environment can be a tall order. Many operate multiple remote facilities beyond the main control room, such as tanks, pumphouses and lift stations. Those remote stations often run legacy components and equipment that have worked reliably for years or decades. The challenge for controls engineers now is to bring those systems up to date in line with today's cybersecurity standards.

The good news is that as industrial automation control systems become smarter and digitized, they benefit from years of Information Technology (IT) experience in cybersecurity best practices.

BEST PRACTICES FOR WATER FACILITIES: THE ISA/IEC 62443 STANDARD

The ISA/IEC 62443 standard is a consensus-based cybersecurity standard for industrial automation and control system (IACS) applications, which includes water and wastewater processing plants. It consolidates global IT cybersecurity best practices and translates them into security standards for utilities and other industrial applications. The result is a solid roadmap for water treatment facilities that need to shield their data and systems from breach or damage and to strengthen their overall security posture.

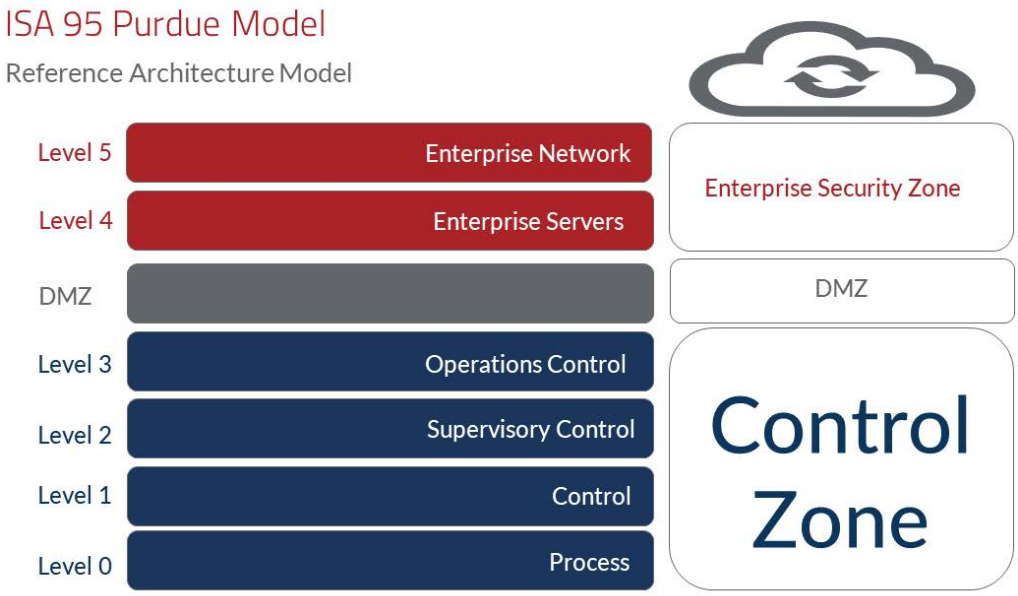
The standard defines how networks and connections should be configured and secured for the entire lifecycle of utilities applications – from design through to decommissioning. It drives a crucial point home, one learned and borrowed from IT: Security is not just implemented but needs to be continuously improved.

STRENGTH THROUGH SEGMENTATION: ZONES AND CONDUITS

For water utilities, that means adopting a layered security approach. At the level of network connectivity, the ISA/IEC 62443 standard establishes requirements for dividing systems into segments as a key security measure to fortify industrial systems.

To illustrate, consider the six-layer Purdue Model (referenced by ISA/IEC 62443), an established blueprint for building secure control systems.

The architecture is divided into six layers: a lower “Control Zone” which comprises the most critical OT functions, and an upper “Enterprise Security Zone, which consists of two layers for IT functions. The two areas are separated by a protective barrier, called the Demilitarized Zone (DMZ).



Consider a wastewater processing facility with separate stations for pumping, coagulation, sedimentation, filtration, etc. (Processes A, B, C, D), each with their own input/output (I/O) devices, PLCs, and Variable Frequency Drives (VFDs). Those process systems and their control devices – VFDs, PLCs, SCADA systems, etc. – sit at Levels 0-3. However, many water and wastewater providers maintain flat networks with no divisions between the different processes in the Control Zone. The problem is that a device plugged in at any of the remote stations can access every other part of the facility.

This ease of connectivity is a major security risk and can lead to intentional or unintentional compromise. An employee laptop infected with malware connected to the filtration PLC, for example, could damage the rest of the system. A hacker with malicious intent could infiltrate one network and gain easy access to the others.

A safer approach is to segment the Control Zone into multiple smaller containers, called zones. Since each zone has its own network, any device plugged into that zone can only access the processes and devices in that area. Devices and processing data at a lift station, for instance, can be kept separate from equipment and data in a sedimentation tank. Zones create a layered security boundary with process control and help maintain the same security level for all equipment, systems, and devices within that zone.

Zones aren't isolated from one another, however. Communication between different zones can be enabled through conduits that control and monitor traffic in and out of individual segments.

For example, if our imaginary water facility's Process A had a PLC that needed to communicate to a PLC in Process C, a conduit would be set up to connect Process A to Process B, and a second conduit would connect Process B to Process C. Those conduits would block or allow traffic. Done right, they would also provide visibility into what's happening at each boundary.

THE RISKS OF TRADITIONAL VLAN

A conventional approach to zone segmentation in water and wastewater processing relies on VLAN technology. However, for facilities with remote stations comprising various devices and systems, VLAN can be technically challenging and resource heavy. Each zone needs its own VLAN subnet, with its own unique IP address, subnet mask, and default gateway. For devices to communicate properly within and between zones, every single device in those VLAN subnets – PLCs, VFDs, and I/O devices – would need to be updated with new parameters reflecting those new IP addresses. You'd also have to set up routers for those subnets.

A VLAN solution would still require firewalls to block traffic ingress and egress at transport and network layers and effectively allow or disallow communication through segment boundaries.

Getting VLAN, router, and firewall technology to work effectively together can be a challenging process. Every piece adds a layer of complexity, and a single change introduced to one part of the solution requires adjustments to every other device.

When a water treatment process has been running smoothly and reliably for 10 to 20 years or more, any change to that process is daunting. The local community relies on facility for drinking water and safe wastewater treatment. The concern with VLAN technology is that what begins with a little downtime could impact water or wastewater services or jeopardize the whole process.

Solving network segmentation using VLANs requires a significant time and labor investment, which many municipal utilities do not have or cannot access. On top of the work involved, the number of configuration changes required introduces significant risk. IP addresses of hundreds or even thousands of devices may need updating. A simple typing error could bring operations to a halt and necessitate a lengthy troubleshooting process to identify the error and restore the system. Key Performance Indicators (KPIs) including Overall Equipment Effectiveness (OEE), productivity, and quality could decline during the ensuing shutdown.

MEETING CYBERSECURITY STANDARDS OUT-OF-THE-BOX

A better and easier method is possible with Red Lion's RA10C compact industrial firewall. You simply install the RA10C in your panel as the conduit between two zones (e.g. Process A and Process B). Rather than having a cable that runs between Processes A and B, cables from Process A and Process B both plug into the RA10C, acting as the conduit and providing the necessary segmentation between zones.

The unit provides firewall protection, along with traffic control and monitoring, and eliminates the need for VLANs and routers. In contrast to the VLAN approach, the Red Lion unit supports zone and conduits capability and preserves network communication without requiring any time-consuming and risky changes to network devices.

With the RA10C operating in Bridge Mode, users can control, visualize, and monitor network traffic with a single piece of software. No special expertise is expected in either networking or firewall functionality. A setup wizard launches during setup, asks users a few questions, and guides them through the installation process.

The RA10C comes installed with configuration software that enables the automatic creation of a host list of devices trying to communicate with the RA10C. The user only needs to know which hosts should be connected to each other and which connections should be blocked. Those decisions are easily and securely managed through a graphical user interface. Arrows indicate which communication pathways are open and closed, and users can direct, redirect, and block traffic with a few simple clicks.

Among the system controls is a Syslog that logs and stores network events on the RA10C unit. In the case of a cyber incident or other breach, those network events can be collected and used to alert the IT department that something has occurred.

BRIDGING OT AND IT FOR CYBERSECURITY RESILIENCE

Given the mounting threat of cyberattack on critical infrastructure, including water and wastewater processing facilities, utilities providers around the world are seeking new ways to increase the resiliency and security of their OT.

When safer, stricter access control is a priority for water treatment, large, flat networks are no longer viable options. A zones and conduits approach to network communication meets modern standards and provides more robust security and the necessary data traffic control.

Experienced controls engineers sometimes feel wet behind the ears when it comes to cybersecurity. Fortunately, cybersecurity standards for utilities applications have their best interests in mind: High uptime and regulatory compliance. The tools that deliver those priorities best are those that support IT cybersecurity principles by design.

Adopting a layered security approach doesn't just make engineers look good. It strengthens the security posture of the organization, protects upstream and downstream partners, and enhances the security of the water and wastewater sector overall.

About Red Lion

Red Lion is focused on being THE Industrial Data Company™. We empower industrial organizations around the world to unlock the value of data by developing and manufacturing innovative products and solutions to access, connect and visualize their information. Red Lion's global manufacturing and support facilities serve customers in factory automation,alternative energy, oil and gas, power and utilities, transportation, water and wastewater industry segments. We provide scalable solutions for cloud connectivity, edge intelligence and asset management, industrial Ethernet switches and industry leading panel meters and operator panels, to make it easy for companies to gain real-time data visibility that drives productivity.

www.redlion.net

RED LION®