INS Industrial Networking Solutions

BELDEN

Modernizing Legacy Networks

Upgrading Water Treatment Facilities for Modern IT Technologies and Secured Critical Infrastructure

BY EXPERIENCED CONSULTANTS

Value-added reseller Industrial Networking Solutions (INS) and Belden, digitization solution provider, demonstrated the need for skilled auditing, product selection, and implementation to upgrade and secure a process control network at a water utility.

Contact Us

800-889-1461
Sales@industrialnetworking.com
3321 Essex Dr, Richardson, TX 75082
www.industrialnetworking.com
services.industrialnetworking.com

Industrial Networking Upgrades are Streamlined

Overview

Water/wastewater facilities and other utility-grade operations are intended to operate for decades, and this concept works well for physical and mechanical components. However, this is a bit at odds with the more rapid evolution of digital technologies, which require comparatively frequent upgrades to improve performance, enhance end-user experience, modernize capabilities, and address emerging threats like cyber-attacks. Cybersecurity is a topic of great concern for critical infrastructure operators.

Utilities with large and geographically dispersed assets face the additional challenge of handling upgrades which are typically localized to one or few remote locations, or only a portion of a site. This results in an overall industrial control system (ICS) comprised of mixed-vintage technologies, which can complicate ongoing operational performance and support efforts (Figure 1).

Implementing a process control network (PCN) solution for the ICS, along with ensuring proper cybersecurity measures are in place, is a multi-disciplinary task that most utility operators are not staffed for. Supplying the right solution requires a PCN and cybersecurity design team that is thoroughly familiar with networking best practices, the products and installation methods suitable for the harshest environments, typical ICS devices and instruments used in the field, and even the utility operation and functionality itself. This case study examines why INS, a value-added reseller, partnered with Belden, a digitization solution provider, are well-positioned to support utility operators with their crucial networking needs.

Industry Challenge

Two of the main challenges facing water/wastewater facilities are network visibility and vulnerability. Water/wastewater facilities and other utility operations implemented over the last few decades were built with digital control and monitoring technologies. These implementations may include devices for basic control, such as industrial programmable logic controllers (PLCs) or remote terminal units (RTUs), in addition to local operator interface terminals and more advanced PC-based human-machine interfaces (HMIs). Even operations that have been in service for many years will likely use supervisory control and data acquisition (SCADA) systems, which interact with digitally operated assets over great distances.

All these devices communicate with each other via network connections. Early iterations frequently relied on simple, hardwired serial or proprietary interfaces, but advancements over the years have introduced fiber-optic media, wireless radio, cellular connections, and satellite systems. Ethernet has risen in prominence as the networking standard of choice, even though there are a variety of industrial communication protocols still available.

To add to this complexity, a great deal of existing technology installed is now obsolete, and in many scenarios, documentation was poorly updated or even lost. Best practices may not have been applied to older designs, or localized projects may have lacked continuity from an overall system perspective. And networks might have been designed as fragmented and flat local area network (LAN) segments, instead of as an integrated hierarchical whole.

End users at these industrial sites urgently need a way to take stock of their systems and determine a best path forward for addressing these concerns and mitigating risk. Even beyond basic performance and compatibility, modern industrial networks are called upon to do more than ever before. They now must be able to handle the rapid growth of device integration, serve as the bridge between operational technologies (OT) and business information technologies (IT), and accommodate the increasingly commonplace requirement of internet-based connectivity. All these factors lead to a great emphasis on cybersecurity.

The following example shows how one large water treatment facility engaged Industrial Networking Solutions (INS) and Belden to upgrade its networking and cybersecurity.

Discovery

INS administered a network assessment that began with a comprehensive understanding of the client's operation workflow and processes to identify challenges and uncover opportunities. The next step was an in-depth network audit to determine current state and benchmark to measure results. In rare cases, this audit can reveal a well-documented and up-to-date network deployment, but it is much more common to discover informational gaps and installation vulnerabilities.

(Figure 2) Industrial process control network installations and traffic can differ quite a bit from common IT installations, so a VAR must be familiar with the unique aspects of both to provide a complete result.

After the audit, INS was ready to provide recommended architecture changes to support upgrading to a completely monitored network. INS collaborated with Hirschmann, a Belden brand, to identify the hardware and software up for the task.

Since this large water treatment facility was experiencing many of the PCN problems identified earlier in this case study, the project team determined a network upgrade was vital to address the issues. Due to the always-on nature of the facility, the network was upgraded and secured in stages to minimize any outages through:

1. **Progressively upgrading network hardware** – INS assessed the water utility's existing infrastructure and determined new networking hardware was required to meet their goals. INS selected products from Hirschmann, a Belden brand, to provide state-of-the-art hardware.

2. **Implementing an in-depth cybersecurity solution** – Once new infrastructure was in place, cybersecurity software was needed. INS and Hirschmann teams determined this was crucial to continuously monitor the network for unapproved devices and applications, block external attack vectors, and protect OT assets and human safety in the event of a breach.

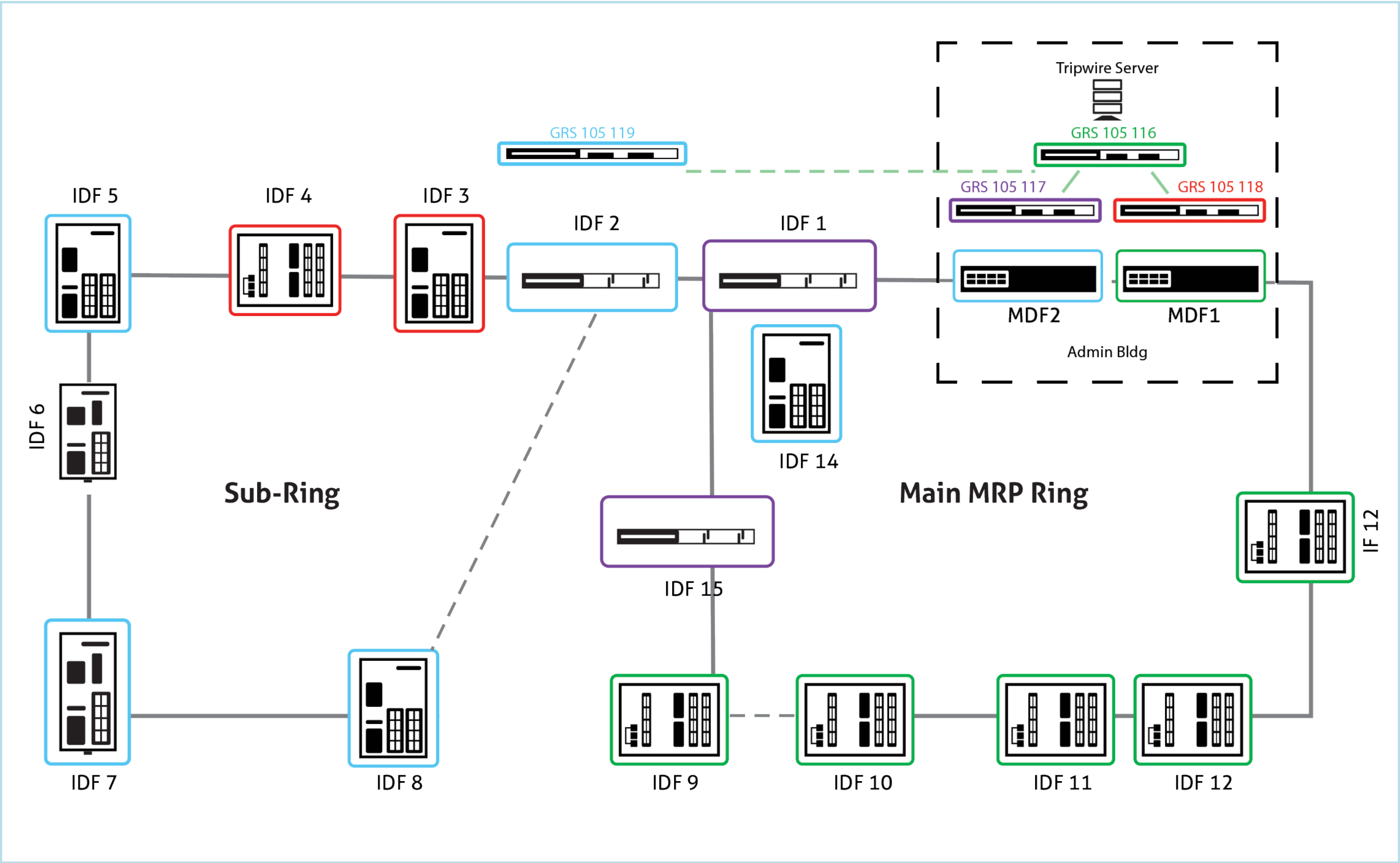
Holistic Network Monitoring

At the water facility, the extended site generally had spare fiber available, so INS recommended deploying a mirrored network. A mirrored network is often preferred because it can be added to existing installations with minimal disruption, translating to low risk and minimal downtime.

A mirrored network was deployed to connect Hirschmann switches to the monitoring solution. A sample network diagram is depicted in Figure 3. Switches with respected boxes have their mirror ports aggregated to:

🟩 GRS 105 116 🟪 GRS 105 117 🟥 GRS 105 118 🟦 GRS 105 119

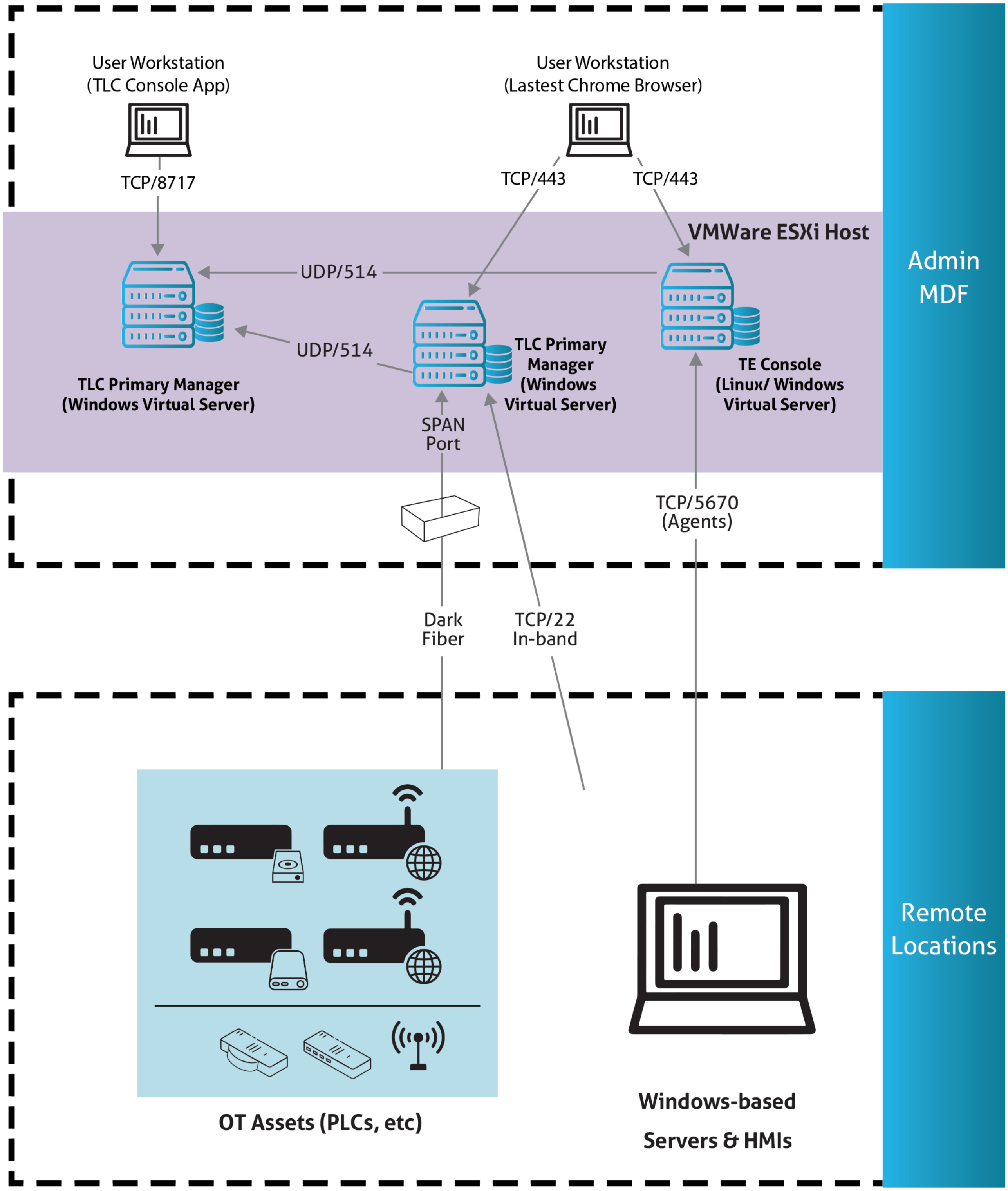
Note: All GRS 105s have HiOS 9.02, All GRS 1040's and RSPE35s have HiOS 7



(Figure 3) A PCN monitoring solution requires mirrored networks and/or sensor networks to transmit all traffic up to a supervisory server.

Comprehensive Cybersecurity Software

With the audit complete and the mirror network in place, INS then integrated the network monitoring application. This software provides comprehensive visibility, continuous threat monitoring, vulnerability detection, and deep insights into ICS installations and PCN networks in a single comprehensive solution (Figure 4).



(Figure 4) Network monitoring applications can collect data over dark fiber mirror networks and/or VLAN sensor networks, to identify vulnerabilities and attack vectors, detect threats, provide deep ICS and PCN visibility, perform real-time change management, and more.

By continuously monitoring all network communications, network monitoring applications can identify policy violations that threaten system reliability, and provide the information and alerts necessary for system administrators to respond quickly. In the water facility, this software employed several discovery techniques, combined with five distinct behavioral-based anomaly detection engines, to deliver comprehensive ICS and cybersecurity intelligence to users. Data can be gathered from multiple sources by leveraging both passive monitoring and active querying, and then aggregated into a database.

Results

This water utility partnered with INS and leveraged solutions from Hirschmann, a Belden brand, to establish an industrial-grade networking infrastructure, with comprehensive management and cybersecurity monitoring software. These network enhancements allowed for better protection from cyber threats, improved operational efficiency, increased intellectual property protection and greater visibility into the status of the network. As a result, the water utility experienced reduced downtime and improved diagnostics from network-related issues. In addition, the facility was able to upgrade their network without having to rip out the existing network and replace it, resulting in significant cost-savings. By upgrading their technology, the water utility's network is future-proofed, reliable, ruggedized and secure.

As a VAR specifically experienced in the industrial sector, and with access to a wide variety of hardware and software products, INS has developed core capabilities in defining and deploying these types of network solutions. This example demonstrates how a VAR partnered with a digitization solution provider is best positioned to understand the unique needs of industrial and utility clients, and how a complete networking and cybersecurity solution can be designed and delivered efficiently.

www.belden.com

www.industrialnetworking.com