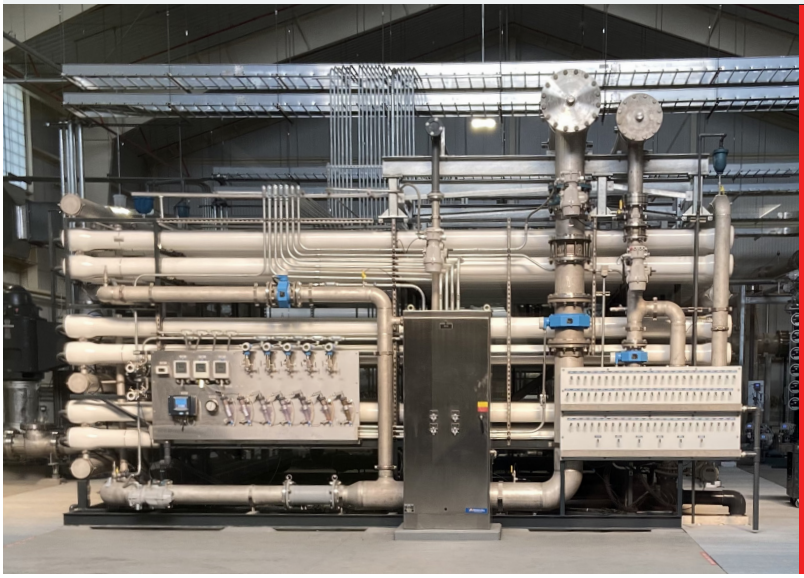
BEDROCK®
OPEN SECURE AUTOMATION

Case Study

Migrating to the Open Secure Water Plant – A Bedrock Automation Case History

The PLCs that the East Cherry Creek Valley (ECCV) Water & Sanitation District had been using to control the potable water treatment facilities and pump stations that supplied water to 60,000 people in the Denver suburbs were becoming obsolete. It was time for an automation upgrade and the utility's operations managers saw this as an opportunity to deepen cyber security protection as well.



SUMMARY

Customer requirement: Modernize controls to avoid vulnerabilities of legacy operating systems, software and tools, without ripping and replacing entire system.

Bedrock Automation solution: A phased-in proxy approach using Bedrock OSA Remote control nodes to concentrate radio data received from field devices via radio and transmit it to the SCADA system securely.

Result: ECCV now has a secure communications channel between its SCADA and control networks and a process for migrating all of its controls to that channel with minimal service disruption.

"Like most other public utilities, we must adapt to an ever-changing world and that includes cyber security. We've always had robust physical security and required usernames and passwords for access to critical systems and controls, but we saw the world around us changing quickly. Many of today's automation technologies are not as secure as they could be because they were developed long before security was a major issue in the industry. Most of the security added to them was an afterthought," said Shay Geisler, I&C Administrator, ECCV Water & Sanitation District.

A look at the legacy system

ECCV's existing plant control architecture was comparable to what many municipal water systems use. A dedicated Windows Desktop or Windows Server OS. The top end SCADA software system is housed on a dedicated Windows desktop or server along with a communications driver, in this case an OPC Server that speaks to the PLCs via legacy Bristol Standard Asynchronous/ Synchronous Protocol (BSAP) and

to some Ethernet IP devices. Data concentrators sat above the PLC network to help manage data communications and aggregation across a serial radio network involving about 80 sites running a mixture of RTU and PLC types and generations. These radios functioned like firewalls separating the SCADA Network and the PLCs in the field, but signals were not encrypted.

"We knew security could not be limited to the SCADA software only. There were too many downstream systems and assets that, if left untouched, would present a huge vulnerability. We determined that the vast majority of these potential vulnerabilities could be solved by addressing the PLC and SCADA communications system," said Geisler.

Geisler and his team decided they had to focus on securing the following three communications paths:

- SCADA software to PLC
- PLC to PLC
- Radio network

They explored several strategies to secure those communications, including adding firewalls and network cloaking, but ultimately determined that getting the depth of security they needed required upgrading the PLCs, RTUs and network radio. Working with automation solutions supplier Process Control Dynamics (https://pcdsales.com) and system consultant RSI Company (https://rsicompany.com), they chose Bedrock Automation's Open Secure Automation, OSA® platform to provide PLC/RTU functionality because of its intrinsic security along with a new ethernet radio solution to provide high data encryption capabilities.

Software upgrade

Supporting the new capabilities required upgrading the current 32-Bit SCADA Software to a 64-Bit solution, which enabled them to leverage the latest Windows

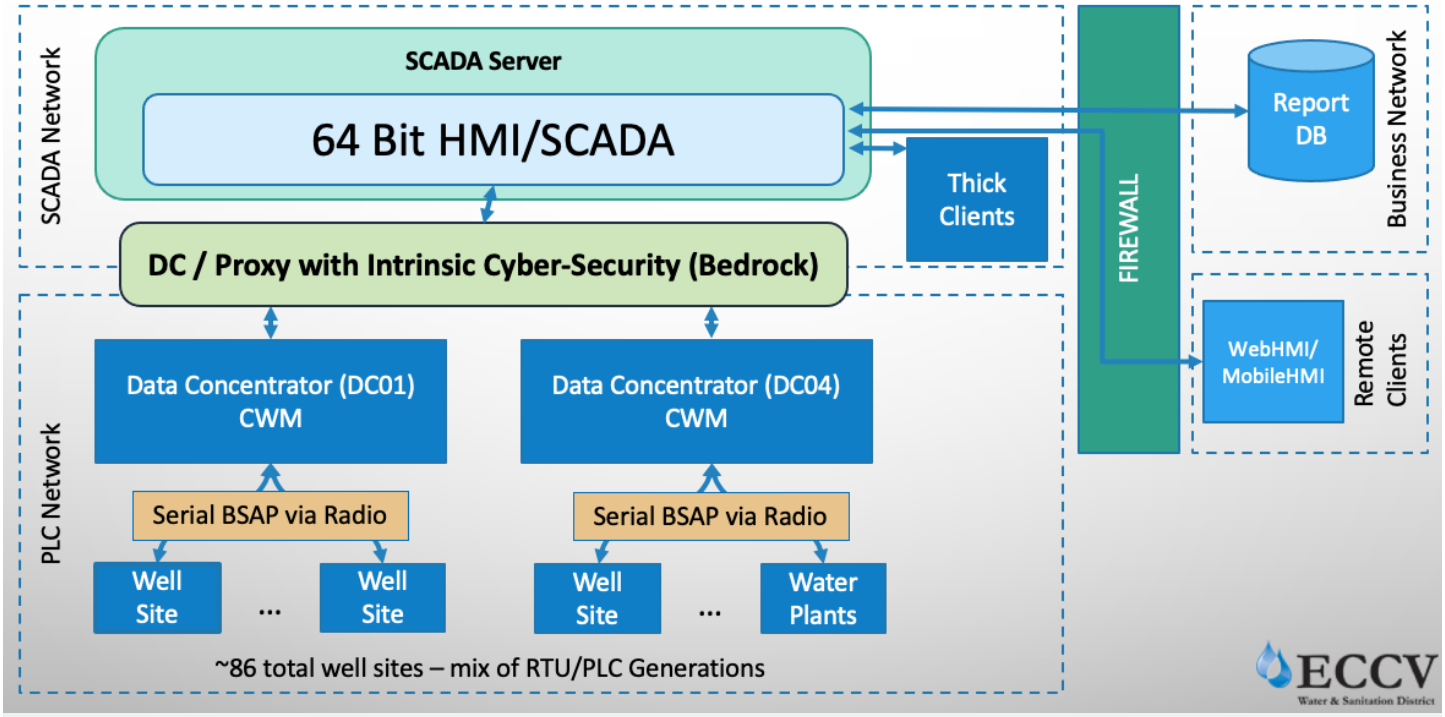


Figure 1: Bedrock OSA Remote control units provide a secure proxy server between the data concentrators and the SCADA server.

Server and Windows-10 based OS capabilities.

"Just upgrading the software provided a much higher level of confidence within both our IT and OT Departments. We also gained valuable operational features and functions, along with many new and powerful security features in the SCADA software itself. This addressed some of the security issues we had with our legacy systems, but it was not enough. We still saw those possible security holes downstream of the SCADA System, and we wanted to address those," said Geisler.

Geisler and his team concluded that the most secure and cost-effective approach would be to connect the SCADA network and control networks with a secure

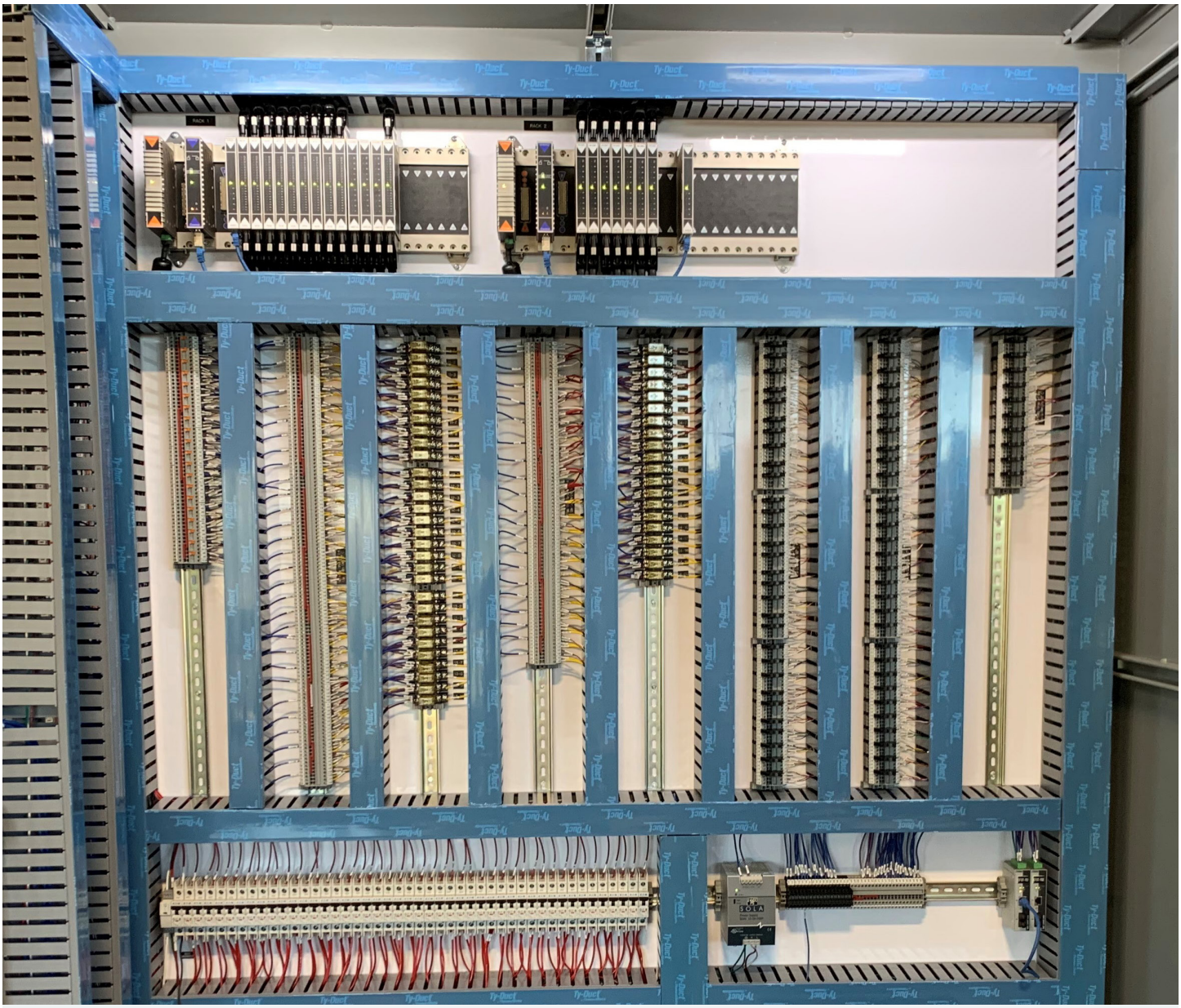


Figure 2: Bedrock OSA control systems in ECCV enclosure.

communications channel. Fully implementing this, however, would have required ripping and replacing their entire system, which would have been costly and would require significant disruption of operations. Instead, they adopted a phased-in approach which began by deploying Bedrock OSA® Remote control units as a secure proxy server between the data concentrators and the SCADA server.

"A cyber-secure data concentrator functions as a proxy server that secures communications from the SCADA Software and the PLC Network. Downstream the data concentrator speaks BSAP or Modbus directly to the existing unit in the field as well as some Ethernet/IP for smart devices," said Geisler. Because the OSA Remotes support BSAP, the utility could continue communicating with its remaining legacy devices while transitioning to new controls, avoiding any significant interruption of service.

Moving downstream

The next phase was to secure a direct connection between the SCADA software and the well sites, pump stations and water treatment facilities with PLCs and controllers with intrinsic cyber security, along with new Ethernet Radios. Covering so many I/O points (roughly 9000) required scaling to a Bedrock OSA platform that scales infinitely through the addition of 5, 10 and 20 I/O control module racks, depending on the number of I/O at each site.

With these Bedrock units installed (Figure 3), they can leverage new SCADA features that extended a root of trust from the PLC controllers to the HMI/SCADA System, thereby limiting all communications with the PLC/Controllers to securely certificated programs and users only. This enabled them to execute standard IT certificate practices such as time limitation,

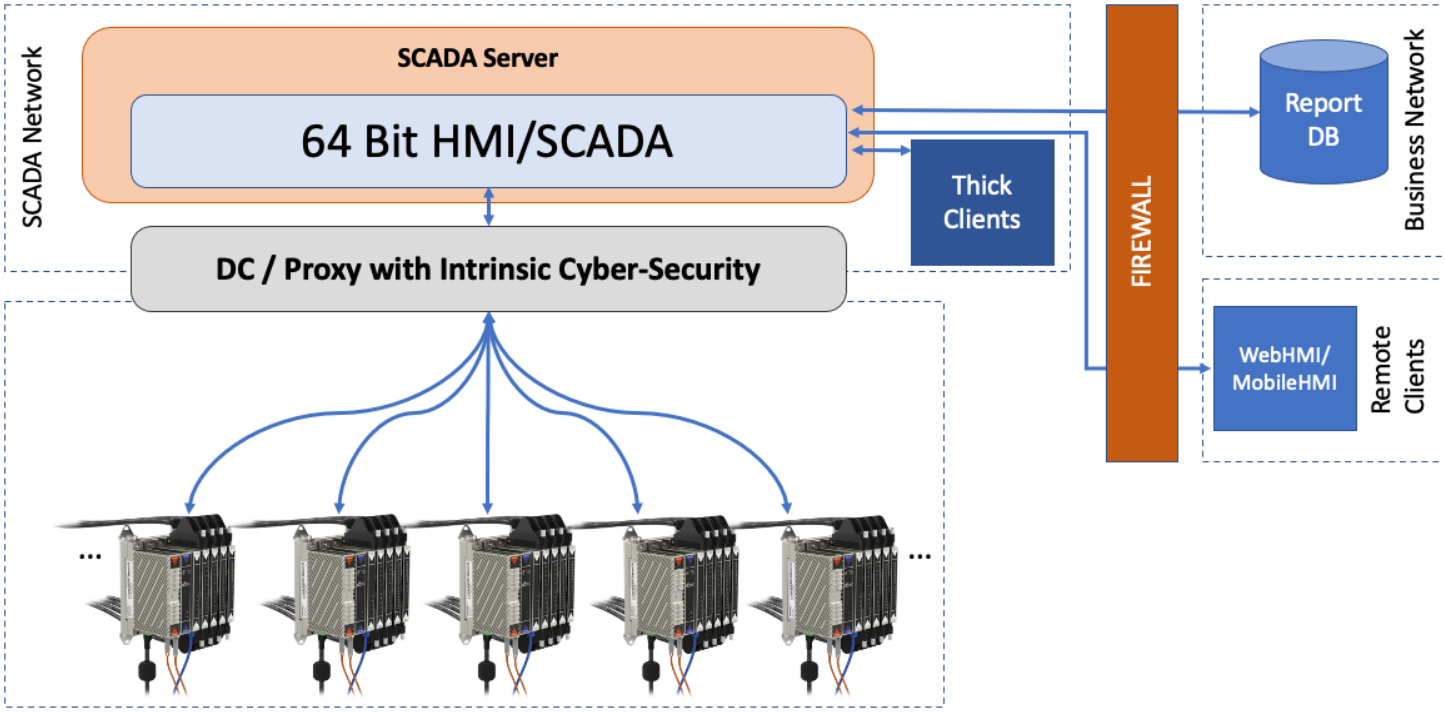


Figure 3: Secure peer-to-peer communications with encrypted Ethernet radio network.

revocation, etc. to individual users or groups with ease. The result is secure, certificated communications from the SCADA Software all the way down to the Remote PLCs/RTU.

Figure 3 shows the target completed architecture. The 64-bit SCADA software connects directly and securely to a peer-to-peer network of scalable Bedrock OSA control systems connected with an encrypted radio network.

The intention was to complete the final architecture within five years, but Covid-related delays may extend this. As they build the system out, ECCV has the option to keep the OSA Remote concentrator/proxy nodes in place or remove them because the system will be secure all the way to the field level PLC/RTU devices due to the secure Bedrock controllers. This is one of the many advantages to transitioning with Bedrock. Another is Bedrock's free software. They are now evaluating the operational pros and cons of the data concentrator model and will decide later on, but either way, it will not break the security model. Geisler feels that the plant is well-equipped to weather the next round of changes.

"We expect the technology for industrial systems to be ever evolving and improving. With this open architecture and technology, we will be able to continually improve and upgrade as we need to, so we don't have to face this type of wholesale transition again," Geisler said, adding that they expect to get more than 30 years of useful life from their new PLC/RTU systems and because Bedrock manufacturers most of its own chips and controls their secure supply chain, they offer a non-obsolescence policy that is unique in the industry.

About Bedrock Automation

Bedrock Automation, based in San Jose, California, has developed the world's most powerful and cyber secure automation platform. This Silicon Valley company has assembled the latest technologies and talents from the automation, cyber security and semiconductor industries to build unprecedented automation solutions for industrial control and power based on three prime directives: simplicity, scalability and security.

The result is an award-winning automation platform called Open Secure Automation (OSA®), with a revolutionary architecture and deeply embedded ICS cyber security that delivers the highest levels of system performance, cyber security and reliability at the lowest lifecycle cost.

Build on Bedrock®

Just some of the recent Bedrock Automation product awards

BEDROCK®

OPEN SECURE AUTOMATION

www.bedrockautomation.com