



Municipal Water Wanted Critical Computer Connections Evaluated

EXECUTIVE BRIEF

- Goal:** For a small municipal water authority to evaluate the security of the computer portion of its operation with a limited budget.
- Solution:** Backbone Security puts vulnerability assessments within reach of organizations on a limited budget. A basic system scan and review can be performed to provide a solid foundation for secure operations. In this case special considerations were added to accommodate the SCADA components, but that didn't drive the final price beyond a few thousand dollars.
- Results:** They received a complete on-site and off-site evaluation by a team of Backbone Security engineers. At the completion of the project, an out brief was conducted a report delivered. Their cumulative net benefit amounted to \$4,815 based on an estimate of the costs to perform the same work using internal staff.

In a proactive action, a Municipal Water Authority decided to have its computer systems audited for possible security issues so they could be corrected before anyone compromised their systems. The Municipal Authority serves water to over 4,300 accounts representing a population of approximately 20,000 people in residential, commercial, public and industrial settings. The Authority operates on an annual budget of approximately \$2.3 million with an annual capital improvement program budget of \$400,000 to \$600,000. The Municipal Authority produces approximately 1.9 million gallons of water daily. In its efforts to ensure total compliance with all state (PADEP) and federal (USEPA) regulations the Municipal Authority spends over \$15,000 per year to have outside independent laboratories test its water, so it seemed prudent to spend a few thousand dollars to make sure the electronics, including web servers, SCADA devices and networked computers in this critical infrastructure were also top notch.

NOTE: This case study was authored by the Backbone Security.Com. Results shown are not a guarantee of equivalent performance

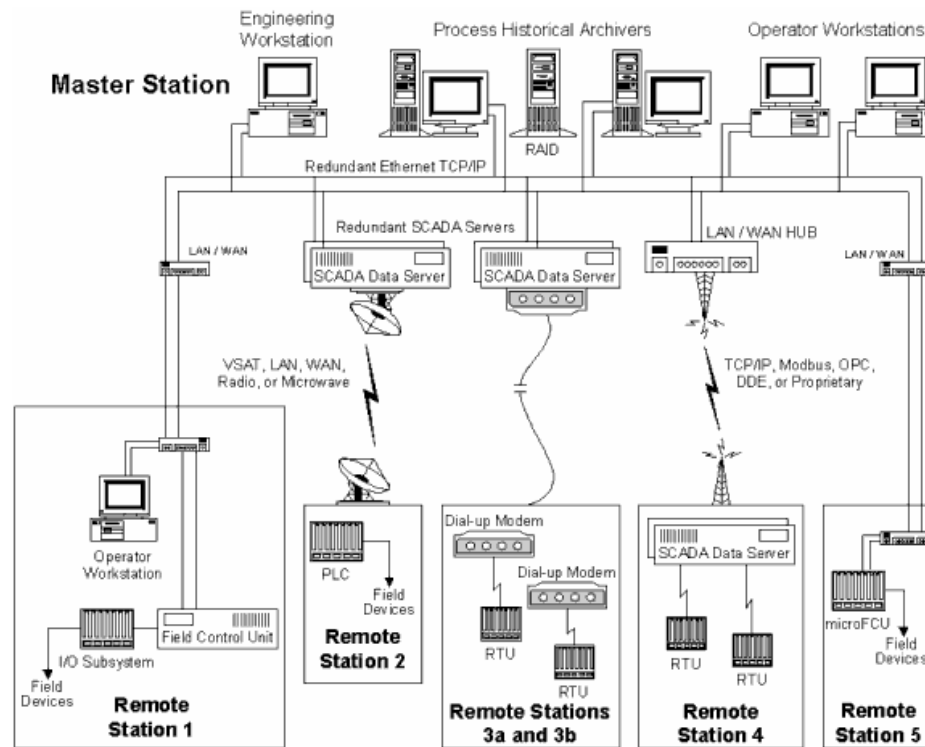
Benefits

Objective	Benefits Achieved
Verify computers used by the water authority were protected from outside manipulation	Backbone was able to verify that the critical systems used, included those on wireless networks, were being protected or were inaccessible to internet users
Verify that networked computers used for billing were being protected	Backbone probed the billing computers that were the most publicly accessible in the system. Several changes to the web based system were suggested to lock this system down from malicious attack. The changes were made by the authority's staff.



The Challenge: Security Audit that includes SCADA and Web Servers within a tight budget

This case is a good illustration that security can be audited, and improved on a tight budget. For this customer, Backbone Security developed a working schematic like the one below, to establish situational awareness. We then set about isolating and testing each component for basic security weaknesses that could be exploited. Finally a report was generated on the issues discovered along with several alternative fixes presented in a low, medium and high cost format.



Remote Station 1 required significant monitoring and control. A local operator monitored and controlled the process. The FCU gathered data from PLC I/O, executed sequential and regulatory control logic, and sent operator-initiated commands to that I/O. Exception-based technology was used to transfer data to be archived or shared with the master station or other remote sites, thus minimizing communications traffic. Local monitoring and control helped insulate this site from other failures in the system. Redundancy made local shutdowns rare.

Remote Stations 2 and 3 were a more traditional configuration. The redundant SCADA Data Servers (SDS) at the master station gathered data from remote RTUs, PLCs, flow computers, intelligent valve controllers, meters, and so forth via serial polling. It also transferred operator-initiated commands to those devices. This configuration can also be used as a backup. If the primary connection fails, the master station's SDS can dial-up Remote Station 4 to establish communication with the field devices until primary communications can be re-established.

Remote Station 4 serves as a true data concentrator. The process at this site does not require a local operator, but does benefit from local control. Just like Remote Station 1, the configuration at Remote Station 4 minimizes communication traffic, isolates the site from failures elsewhere, and is a redundant configuration.

Remote Station 5 requires local control but does not necessarily need an on site operator. The UCOS microFCU is a small PLC that executes sequential and regulatory control logic, and sends logic- and operator-initiated commands to the I/O and field devices.

The Bottom Line for the Water Authority

An analysis of the implementation shows that the medical center will gain a cumulative one-year net benefit of \$4,815, and an annual ROI of 72%. The entire project has a payback period of 7 months.

The following chart provides a detailed analysis of this low cost audit.

BUSINESS ANALYSIS OF THE SOLUTION

Project Summary

Annual ROI with Backbone Security Project	72%
Payback Period with Backbone Security (months)	7
Cumulative one year benefit	\$4,815
Cumulative one year net cost of Backbone Security's Component	\$2,800

Project Costs	Startup	Year 1	Year 2
Hardware & Maintenance	\$0	\$0	\$0
Software & Services	\$0	\$2,800	\$0
Staff Costs for Implementation & Support	\$0	\$0	\$0
TOTAL COST	\$0	\$2,800	\$0

Benefits	Year 1	Year 2
Saving in staff costs @ 12.02 / hr	\$5,769	\$0
Saving in staff costs @ 23.08 / hr	\$1,846	\$0
		\$0
TOTAL BENEFITS	\$7,615	\$0

Financial Analysis

Net Benefit	\$0	\$4,815	\$0
Cumulative Net Benefit	\$0	\$4,815	\$4,815
Net Present Value	\$2,540		
Average Annual ROI	72%		
IRR	N/A		
Payback Period (months)	7		