InstruLogic
CONTROLS. AUTOMATION. INSTRUMENTATION.

Is Remote Monitoring & Control too Risky?

I recently visited a treatment plant to talk about their new control system. Everything was new and the system was working flawlessly. The operators were happy with the greatly improved visibility into their process, automation of some procedures and enhanced ability to monitor and control the plant from multiple locations on site. The new system delivered results that far exceeded their expectations.

I also noticed the operator on duty scanning the main control console while happily surfing the internet, posting to facebook and checking email. So I was somewhat surprised when I asked about adding remote monitoring and control capabilities. The system we installed is based on Ignition from Inductive Automation. With Ignition, adding remote monitoring and control capability via smart phone, tablet or computer is simple and virtually cost-free. But the customer wasn't interested in extending the capabilities of the SCADA system beyond the plant grounds due to security concerns.

Security issues are a valid and serious concern when contemplating the addition of remote monitoring and control, but it is often also true that remote monitoring and control may not be your biggest security vulnerability or my not even increase your vulnerability to cyber threats. In fact, adding remote monitoring and control may provide the incentive to close existing gaps in your security profile thereby making your overall plant operations even more secure.

Benefits of Remote Monitoring & Control

Remote monitoring & control enhances operations by increasing process visibility, enhancing productivity, increasing efficiency and decreasing response time to critical events and process disruptions. Real-time access to a treatment plant control systems can improve operations by enabling on-call operators to respond to alarms immediately without the delays incurred by travel to remote sites. Interruptions to treatment operations, regulatory violations and threats to health and safety can be eliminated or reduced with more immediate action. At the same time overtime costs can be reduced and quality-of-life improved for plant operators who are on-call for weekends, holidays and nights.

Minimizing the risks

Nevertheless, it is unwise to add remote access to your SCADA system without addressing the security implications. Certainly adding remote access alone won't make make a system more secure. But addressing plant-wide security issues within a remote access upgrade may have the net result of making your operators more security-conscious, your infrastructure less vulnerable to intrusion and ultimately making your operations more secure. Here are some ways to minimize vulnerabilities and improve operational security.

Managed Access

The step that many operators overlook is managing access to system resources. Many operators have only one password for all of their users. Often it is the one taped to the control terminal. Some users also have a unique password for administrative users. It may not be taped to the console, but it is rarely a well-kept secret. Needless to say, this is not considered best practice for system security.

When remote monitoring & control is added to a treatment operation, managing access is often elevated in importance. Limiting each user's access to their roles and authority can often make the entire operation more secure. A user should only able to access those elements of the system that his or her job requires. Certain controls such as set-points and thresholds should be read-only for users lacking the appropriate authority to change them.

Security Zones

A Security Zone is a group of Gateways, Computers or IP addresses with defined policies and restrictions. These policies and restrictions limit access and functions to locations in addition to user-defined privileges. Therefore, unknown computers and devices will not easily gain system access. It also limits the type of data information that is passing over networks.

Tag-Level Security

Tag security is often the best way to configure security for data access. By defining security on a tag you affect the way it is accessible across all windows in your system. If a user opens a window that has components bound to a tag that the user does not have privileges to read or write to, the component will get a "forbidden" overlay. The intruder will neither see the data nor have the ability to change it.

Data encryption

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. This protects your installation from anyone "snooping" the data as it passes over the network. This also helps to thwart a security vulnerability known as "session hijacking."

Audit logging

Audit profiles record details about specific events that occur in your system. They record who initiated an action, what they did, and how they gained access- all with a precise time stamp. Although audit logs will not prevent unauthorized access, they will help identify the source and type of intrusion, provide an order of events, assess the damage, assist in recovery and provide information that can help prevent similar future intrusions.

The Instrulogic Advantage

If you want the the advantages of remote access and control while minimizing your vulnerability to cyber threats, Instrulogic can help. With over 25 years of measurement and control experience and as the industry leader in SCADA innovation, Instrulogic is committed to discovering and implementing the most cost-effective solutions for all of your measurement and control needs. Our security experts will design and implement a remote access solution that is effective and secure. And while we are at it, we just might improve your overall operational security.

Instrulogic LLC
Winchester, Va/ Raleigh, NC
540-338-2222
www.instrulogic.com
212 Fort Collier Road, Suite 1
Winchester, VA 22603