CYBER SECURITY SOLUTIONS TO MEET WATER SECTOR REQUIREMENTS

EXECUTIVE SUMMARY

Industrial Control Systems (ICS) and related Supervisory Control and Data Acquisition (SCADA) systems have improved water and wastewater operations by providing increased reliability and service for their customers. As costs have declined, ICS have been used more and more for process monitoring and control, which has made the water sector, and other critical infrastructures like energy, transportation and agriculture, more vulnerable to accidental cyber events or targeted cyber attacks.

The U.S. Water Sector Cyber Security Working Group (AWWA and DHS) and the European Network and Information Security Agency (ENISA) have both reported that cyber threats to ICS are growing in number and sophistication. This means that ICS security now requires more than simply blocking hackers or occasionally updating anti-virus software.

With the rapidly changing digital environment, water sector infrastructure ICS are being used in ways that were never anticipated. Many systems were designed decades ago with little consideration for cyber security. Increased connectivity and use of common operating systems and platforms have also contributed to increased security risks.

Water sector utilities understand that interruption of a clean and safe water supply would erode public confidence or, worse, generate significant public health and economic consequences; however, the path to secure SCADA systems is not always clear.

VISION AND ROADMAP

Government and industry leaders have collaborated to develop a unified security strategy. Their efforts produced the "Roadmap to Secure Control Systems in the Water Sector", a long-term framework of goals and milestones to reduce the risk to ICS. The framework integrates the experience of a cross-section of operators, asset owners, ICS and government experts.

By following this roadmap, water industry leaders expect that ICS throughout the water sector could operate with no loss of critical function during and after a cyber event. The roadmap covers the formidable technical, business, and operational challenges that lie ahead in strengthening the critical systems against increasingly sophisticated cyber attacks.

A critical component of this program involves the manufacturers of ICS, particularly those utilized for SCADA applications. While some vendors have made improvements in their recent products, all face challenges in upgrading equipment installed 10 or more years ago. In many cases, the only solution may be a complete and expensive replacement. As water sector cyber requirements evolve, it is important the security functionality be core to a vendor's current product and not merely a collection of hastily added features.

WATER INDUSTRY RESPONSE

Although frequently thought of as lagging other utilities in implementing security measures, the water sector is the only one of 18 critical infrastructure and key resource (CIKR) sectors, defined by the U.S. Department of Homeland Security that has completed two rounds of required metric reporting on its sector specific plan.

Two additional standards, ANSI/ AWWA G430 and ANSI/ASME-ITI/ AWWA J-100, were developed to help utilities become more secure. These standards provide methodology for water utilities to identify, analyze, quantify and communicate the risks of specific malevolent attacks against water and wastewater systems. Currently voluntary, these standards will likely become mandatory in the near future.

The U.S. Federal "Cybersecurity Act of 2012" was tabled pre-election, but is expected to pass in 2013. Water sector utilities must take steps now to prepare their SCADA systems for cyber security requirements that are almost certain to come in the future. Near-term expenditures in ICS should at a minimum include basic cyber security functions like encryption and user authentication. The solution should also have a published plan with easy upgrades to meet future mandatory requirements.

MOTOROLA'S FOCUS ON SECURITY

Motorola understands high-security system trends, through its many critical military and government customers, and recognized that increased security measures would be required in all utility SCADA areas as well. In 2010, we initiated collaboration among our own experts and those of DHS, TSWG (Technical Support Working group, the antiterrorist arm of the U.S. Department of State) and a third governmental security agency to develop a secure Motorola ICS/SCADA product. We integrated comprehensive security and information assurance functions into the ACE3600 SCADA systems with minimal performance degradation. ACE3600 protects all points of entry to the network, limits points of vulnerability and prevents attempts to compromise the network and the data it transmits and uses.

Regarded as a pioneer project in the ICS security area, our leading edge product was successfully tested by Idaho National Labs and released in July, 2012.

KEY ELEMENTS OF ACE3600 SECURITY

Effective security methods used in other critical enterprise networks are now applied to secure Motorola SCADA. The most important features in the ACE3600 enhanced security option include:

SECURITY POLICY ENFORCEMENT

System-wide set of security settings defined and installed in all equipment.

BUILT-IN FIREWALL

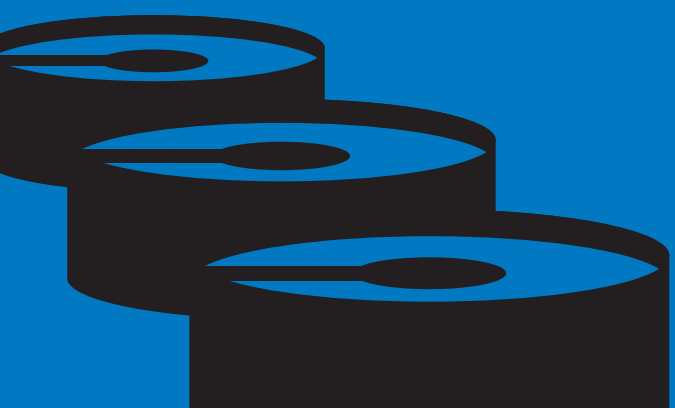
Filters IP communications by port, direction, protocl and IP address.

ACCESS CONTROL

User authentication tools verify specific user access and if use is legitimate and allowed; it is executed at the RTUs (M2M) or system servers.

ROLE-BASED ACCESS CONTROL

Restricts types of access to authorized users only. System administrator can define job roles and assign different combination of permissions to each role.



"THE COUNT OF INCIDENT TICKETS RELATED TO REPORTED INCIDENTS AT WATER AND POWER GENERATING UTILITIES IS GOING UP. WHILE ONLY NINE INCIDENTS WERE REPORTED IN 2009, THE NUMBER GREW TO 198 IN 2011. JUST OVER 40% CAME FROM WATER-SECTOR UTILITIES ... THERE'S A LOT OF EXPOSED WATER SYSTEMS."

KEVIN HELMSLEY, A LEADER IN THE CONTROL SYSTEMS SECURITY PROGRAM AT ICS-CERT

INTRUSION DETECTION SYSTEM
Legitimate traffic is allowed but unauthorized access activities, such as an attempt to alter an RTU program or drop unauthorized data packets, are identified; ACE3600 blocks these activities, logs the events and if enabled sends a report to the system administrator.

APPLICATION CONTROL SOFTWARE
Also known as "white listing", this software blocks unauthorized applications and code on PCs and RTUs. ACE3600 firmware protects user programs with this technique, and ACE3600 configuration management tools on PCs are protected with McAfee™ Solidifier.

ENCRYPTION
An algorithm makes data readable only by a device with a specific key to decrypt the message. ACE3600 communication data encryption prevents listening in or spoofing a message. Data stored in the ACE3600 is also encrypted using an AES (Advanced Encryption Standard) with a 256-bit, FIPS-140-2 approved key.

UNUSED PORT DEACTIVATION
Mechanism disables communication in any ports that are unused.

TIME-WINDOW COMMANDS
Adds an additional layer of defense via the application that designates a "time window" of action in response to a command message.

"UTILITY CYBER SECURITY IS IN A STATE OF NEAR CHAOS. AFTER YEARS OF VENDORS SELLING POINT SOLUTIONS, UTILITIES INVESTING IN COMPLIANCE MINIMUMS RATHER THAN FULL SECURITY, AND HACKERS HAVING NEARLY FREE REIGN, THE ATTACKERS CLEARLY HAVE THE UPPER HAND."

PIKE RESEARCH REPORT Q4, 2011

MOTOROLA SOLUTIONS UTILITY HERITAGE
Motorola brings over thirty years of experience in SCADA and other critical data communications. We offer unparalleled solutions to a wide range of utility challenges. Our RTUs connect with a wide range of utility equipment, support popular protocols and interface to many control center software packages. We have deployed over 150,000 RTUs worldwide, serving water and wastewater utilities, along with oil, gas and electric providers and public safety agencies.

We are a leading provider of wireless communications products, using licensed or unlicensed spectrum and making available leading edge security features. Utility SCADA systems by their nature preferentially use wireless media to link their remote locations and Motorola has an integrated solution for virtually all use cases.

ORDER ACE3600 ENHANCED SECURITY
Enhanced Security is available July, 2012, with new, optional secured versions of RTU firmware and STS software including:

FW 16.00
Requires VA00360AA security enable option per RTU/IP Gateway.

SECURED STS16.50 OR HIGHER – F7560
Supports 64 bit WIN XP Pro, SP3 and WIN 7 Pro

COMPATIBILITY
Requires CPU 3680 with security enable option FW 16.00 or higher, and secure STS 16.50 or higher. Existing CPUs must be upgraded to the security firmware.

An end user declaration or encryption export license is required for the secured STS.

For additional information, contact your Motorola SCADA representative or visit **motorolasolutions.com/SCADA**.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com**

MOTOROLA