

Protecting Critical Infrastructure and Cyber Assets in Municipal Water Systems



LISTEN.
THINK.
SOLVE.

Introduction

The United States' water supply and distribution network faces increasing threats from forces both inside and outside their distribution systems. Some enemies have already struck. In 2006, a foreign hacker used the Internet to plant malicious software in a water-filtering plant in Pennsylvania. The next year, a former employee of a canal authority in Northern California was charged with damaging the computer used to divert river water to farmers' fields.

Not all security breaches are malicious. When a large Southern California water system recently hired a professional hacker to probe the vulnerabilities of its computer networks, he needed just one day to seize control of the equipment used to chemically treat drinking water for millions of people. The hacker got in through a gaping security hole: County employees had been logging into the network through their home computers.

Fortunately, none of these cyber incidents caused cascading problems. But experts ranging from the U.S. Department of Homeland Security to the American Water Works Association (AWWA) are warning that security surrounding the nation's vital water systems must be substantially tightened to help prevent bioterrorism and other potential disasters.

The experts agree that the industrial control systems (ICS) currently used by most municipal and private systems have left the water sector vulnerable to cyber criminals and accidental threats.

"Today's industrial control systems are incredibly complex assemblages of technology, processes and people," the AWWA noted in a 2008 report on water-system weaknesses. "Increasing connectivity, the proliferation of access points, escalating system complexity, and wider use of common operating systems and platforms have all contributed to heightened security risks."

This white paper examines the nature and extent of those risks, and provides an overview of industrial security and regulatory trends affecting the water industry. This document also explains how systematic implementation of control and information-system technology can enhance security of critical water-system infrastructure. Specifically, this document describes the best-in-class solutions offered by Rockwell Automation to help municipalities and others in the water sector protect their operations – and their customers – from the dangers posed by ever-expanding security threats.

The Evolution of Risk

To take advantage of digital advances, water-process control systems – like those in other major industries – have changed dramatically in the last two decades. Once isolated and proprietary, most water-control systems today are part of a converged network that connects plant operations to the administrative environment. The migration from single-purpose supervisory control and data acquisition (SCADA) systems to industry standard, network-based systems provided numerous benefits. Among them: Increased information-sharing across the operation, and remote (Internet and wireless) access to control systems.

But those advances also created security gaps. By connecting to the larger web of networks, water-control systems are exposed to the myriad threats that lurk in cyber space, including viruses, worms and trojans. Poor control-system architecture, unfettered user access, and lax oversight of security policies and procedures have all combined to heighten the risk.

Meanwhile, manuals and training videos on ICS are publicly available, and many hacker tools can be downloaded or purchased on the Internet. Cyber criminals need little systems knowledge to infiltrate ICS operations.

For all these reasons, the number of control-system cyber-security incidents in the water/wastewater industry has escalated sharply, according to the Repository of Industrial Security Incidents (RISI), which reported a 300 percent increase in reported events between 2004 and 2009. RISI is a subscription-only database that collects, analyzes and shares information regarding cyber-security incidents that directly affect SCADA and process control systems.

According to RISI, almost half of all cyber incidents across all industries during that five-year period were caused by malware, including viruses, worms and trojans. But unauthorized access or sabotage by internal sources – such as disgruntled workers or contractors using access privileges to cause harm – rose considerably at the same time. Network anomalies also triggered failures in control-system equipment, RISI said.

The threats to water systems extend well beyond technology. Most municipal systems include miles and miles of pipes that carry water from the main plant to homes and businesses. Along the way are pumping stations and numerous other essential apparatus. If left unsecured, these physical components could provide access for anyone with the motive and the means to contaminate the water or otherwise sabotage the system.

According to RISI, almost half of all cyber incidents across all industries were caused by malware, including viruses, worms and trojans.

The Regulatory Environment

The water industry is far from the first to face major operational threats. Major elements of the U.S. economy and infrastructure have been attacked on the ground or from cyberspace, with often costly and sometimes devastating results. Hackers regularly rob consumers' user-names, passwords, credit card numbers and other personal information from financial, health care and other institutions.

Industrial espionage, once limited to dark corners and alleyways of the business world, is becoming more commonplace with frequent job-hopping and personnel changes. Digital information is a currency to be used for good or for bad. Broad-scale information availability, lax controls of sensitive, secret and mission-critical data and inadequate protection of network-enabled assets carries far-reaching implications for the nation's public infrastructure. Stuxnet, a worm created to circumvent and penetrate Microsoft Windows defenses, is the first known malware that spied on, subverted and attacked highly-engineered industrial control systems. It's also the first malware to include a programmable logic controller (PLC) rootkit, which masked the malware in the system and allowed it to stealthily achieve its pre-programmed goal.

In today's world where social-engineering and savvy reconnaissance are easily combined with state-of-the-art cyber technology, new threats are being created to prey on human nature and curiosity and ever-present weaknesses or oversights in control system design. The contemporary, wired-world must anticipate new threats like a Stuxnet 2.0. Furthermore, threats and potential attacks from both inside and outside the six walls of a facility must be considered and mitigated in order to help assure safety and operational integrity of the systems on which so many rely.

Experts agree that cyber terrorists and their malicious methods will become far more sophisticated in the years to come – just as they have since the federal government established the Critical Infrastructure Protection (CIP) program in 1998. The program, which was updated with the establishment of the Homeland Security Department in 2003, defines those physical and virtual systems that are “so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety.”

Among the entities covered by CIP are those involved with transportation, communications, law enforcement and municipal services – including water systems. So far, the major effect on the water sector has been the federal requirement that system operators assess their vulnerabilities to both physical and cyber attacks.

But the water industry can expect more regulatory pressures, especially if a high-profile event occurs, such as a cyber failure that presents a risk to society or leads to a major disruption of service. That’s what happened to the bulk power industry in 2003, after a blackout struck New York City and large areas of the Northeast. By waiting for more regulations to force the deployment of cyber safeguards, the water sector runs the risk of experiencing the same surprise impacts that hit the bulk electric sector.

Lessons from NERC CIP

In the wake of the 2003 Northeast blackout, the federal government enacted the Energy Policy Act of 2005. That act authorized the Federal Energy Regulatory Commission (FERC) to enforce operating standards in the bulk power sector. In 2006, FERC certified the existing North American Electric Reliability Corporation (NERC) to oversee power-system accreditation and operation in the United States.

Previously NERC’s guidelines were just that – guidelines. Today, NERC enforces standards that must be followed by companies responsible for the reliability and availability of the Bulk Electric System in North America. The standards that specifically pertain to the identification and protection of cyber-critical assets are commonly called NERC CIP standards.

While NERC CIP standards do not currently apply to industries outside of power generation, the requirements do provide a migration model for the water industry to help mitigate the risks of malicious attacks and accidental incidents.

The primary objective of the NERC CIP standards is to help assess the reliability of each facet within the power infrastructure, evaluate power companies’ preparedness in the face of an attack or unplanned interruption of operations, and to continue education and awareness for employees of these companies. As defined by NERC, CIP covers “the assets, systems and networks, whether physical or virtual, considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.”

Validating compliance with NERC CIP regulations can be challenging – and non-compliance can be costly. The silver lining is that regulations such as NERC CIP can notably reduce risks, and simultaneously help identify ways for asset-owners to sustain and improve operational efficiency.

The NERC CIP regulations are categorized into eight standards. While the NERC CIP regulations are specific to the power sector, they can serve as a helpful guide to the water sector in anticipation of future guidelines for their industry, as well.

Rockwell Automation finds that recategorizing these eight standards into three distinct groups helps to greatly simplify the understanding of the requirements that are applicable to industrial control-systems.

1) Plan to protect your cyber critical assets. CIP-003-1, -007-1, -008-1, and -009-1 all offer guidance on how to secure individual assets within a system. These standards include requirements for identifying the owners of cyber critical assets and for documenting exceptions to those cyber critical assets. They also have requirements for applying standards that help protect the



information associated with those assets and similarly include an annual evaluation of managing these security controls. Maintaining these security standards is also defined within this set of four standards, as are guidelines for reporting and responding to a system threat and recovery recommendations in the event that a company loses access to an asset.

2) Know what you've got and where it is. With CIP-002-1 and -005-1, the most important step companies can take is to understand what critical assets exist within a system, and what cyber critical assets are essential to the operation of those critical assets. Examples can include systems and facilities at master and remote sites that provide monitoring and control, real-time power system modeling, and real-time inter-utility data exchange. With those assets identified, companies must then ensure and document that every cyber critical asset resides within an electronic security perimeter. This perimeter needs to include electronically monitored access control, as well as an annual review of the perimeter's cyber vulnerability.

3) Tend to the physical security of your assets. While many already have addressed physical security, CIP-004-1 and -006-1 standards direct companies how to create and maintain a physical security plan that complements the cyber security measures already in place, with requirements for documenting physical access controls. Additionally, these standards address the need to ensure that companies have proper screening processes in place for hiring personnel, and that all employees are aware of the security measures used and are trained on how to use them.

As is the case with many regulatory standards, compliance can be both a burden and a boon. Generally speaking, it's sound business sense to regularly evaluate your systems, identify potential weaknesses within those systems, and take steps to strengthen those areas. While avoiding fines may motivate some, there are other business benefits to consider. For example, while municipalities design their systems to optimize efficiencies and maintain continuous operations, these standards should reinforce a sound practice of regularly reviewing critical systems for any potential vulnerabilities. It is important to address any detected vulnerabilities before they create an interruption of service or are used as an inroad for some malicious act.

Rockwell Automation Can Help

Security is most effective and least expensive when included in the basis of design. Having taken that critical first step in defining your cyber critical assets, look for the most efficient way to achieve and document your municipalities' compliance requirements and avoid risk.

Rockwell Automation can work with you to help protect your critical infrastructure by applying our industry knowledge, technology, services and solutions. We already offer products, solutions and services that help you fulfill the CIP compliance requirements. Our Network and Security Services team provides industry experience and consultation services to help you assess, design, implement, audit and manage a combination of process control and information systems.

Our field engineers and consultants collaborate with you to help manage the differences between process and IT enterprises and their associated risks. This can be done not only through technology, but also through policies, procedures and behavior – allowing you to achieve your production and business goals.

Our consultants consider where you are in your control system or security lifecycle, and develop a plan to help improve system reliability and increase overall equipment effectiveness. That plan can include everything from security-embedded hardware, to innovative software, to physical-site security.

Rockwell Automation and Cisco have partnered to create a blended approach to define contemporary network system architectures that help municipalities embrace and comply with today's standards.

From a product perspective:

Rockwell Automation products are designed to exacting standards and follow a rigorous design-for-security philosophy throughout the product development lifecycle. Furthermore, as new threats emerge or vulnerabilities are identified, Rockwell Automation continuous improvement processes strive to mitigate risks to help you maintain safe and secure operation.

Rockwell Automation contemporary products include an ever-growing array of features to help you enhance the security of your control systems. Many products provide capabilities to help protect key intellectual property, such as custom control-system routines and production data. Many also can provide means to control user-access to restrict and log changes to mission-critical aspects of the system. New enhancements are being introduced to restrict tampering and validate authenticity of the software that drives products.

Although most of these product-level features have little effect on your reaching CIP compliance, these capabilities complement the goal of CIP compliance to help protect both the critical infrastructure and those who depend on its safe and secure operation.

From a system perspective:

A number of Rockwell Software system-oriented applications in particular can help you meet CIP requirements. The FactoryTalk® software suite provides centralized role-based access-control through a software service called FactoryTalk Security. FactoryTalk Security operates in a similar manner to that of Microsoft Windows Active Directory (AD). It provides many of the same capabilities, plus additional features customized specifically for the needs of automation systems. It controls user access to applications and devices through user authentication and authorization. Using FactoryTalk Security can help address several NERC CIP requirements and if desired, it can directly use Microsoft's AD to help facilitate enterprisewide access control to key control system assets such as controllers, industrial PCs and human-machine interfaces (HMI). For example:

- **CIP-004-1 R4.2** calls for revoking access to cyber critical assets within 24 hours for personnel who have been terminated. With FactoryTalk Security, an administrator can revoke access to software products and devices immediately.
- **CIP-007-1 R5** contains several requirements in the area of account management. With FactoryTalk Security, you can meet all of these requirements.

FactoryTalk AssetCentre change management software provides you with a set of asset-centric focused tools to securely and centrally manage your factory and process automation production environments by tracking users' actions, managing asset-configuration files, and providing backup and recovery of operating asset configurations. With these capabilities, compliance with many CIP requirements is much easier.

- **CIP-003-1 R6** requires a comprehensive change control and configuration management process. FactoryTalk AssetCentre software serves as a key technical application of such a process. The FactoryTalk AssetCentre application has add-ons that support calibration management and process device configuration. The calibration management capability allows for a paperless calibration solution: managing calibration requirements, specifications, schedules, calibration results and reporting. Process device configuration allows you to access instrument parameters, aids in configuration and commissioning process devices and helps with diagnostics. Acting as a host system, or frame application, it gives you the ability to work with multiple vendors' instruments in one common platform.
- **CIP-009-1 R4** calls for a recovery plan to restore cyber critical assets to operation. Configuration backup and recovery is a core feature of FactoryTalk AssetCentre software, and can help make this plan much easier to execute. The application also provides control system backup that is integrated with source control to provide reliable and easy access to the latest control system configuration file. Both Rockwell Automation and third-party assets are supported.

Rockwell Automation also provides additional information and solutions to help you meet other requirements.

- **CIP-007-1 R2** – A list of TCP and UDP ports used by Rockwell Automation products is maintained on our Knowledgebase, helping you meet CIP-007-1 R2, "Ports and Services." Visit http://rockwellautomation.custhelp.com/app/answers/detail/a_id/29402 for more information.
- **CIP-007-1** – All TechConnectSM subscribers can access results of the Rockwell Automation patch qualification process, in which Microsoft operating system patches are tested for compatibility with Rockwell Automation software products. Using this service can help you meet CIP-007-1, "Security Patch Management."

Conclusion

The complexity and interconnection of water-industry control systems has increased dramatically in the digital age. While these advances carry many benefits, they have also heightened security risks surrounding life's most essential element – water.

By partnering with Rockwell Automation, municipalities and others who operate water systems can proactively address risk, identify vulnerabilities and help protect systems from known and unknown threats.

Rockwell Automation offers a holistic approach to industrial security, delivering layered solutions that help block intrusions, prevent security lapses and avoid costly accidents whose effects could range from a mere service interruption to a major disaster.

Our offerings are three-fold: security-enabled products and systems, innovative software, and expert consultation on everything from control system design, deployment and maintenance to establishing comprehensive disaster and recovery plans.

Our robust solutions help water suppliers ensure the integrity of their current systems, while offering the scalability necessary to meet future demands – and combat expanding and evolving security threats.

To learn more about Rockwell Automation capabilities, visit www.rockwellautomation.com/security. Here you will find information regarding our security products and services, including a link to our Network & Security Services team.

FactoryTalk and TechConnect are trademarks of Rockwell Automation, Inc.
Trademarks not belonging to Rockwell Automation are property of their respective companies.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846