Building more resilient and secure solutions for Water/Wastewater Industry

Steve Liebrecht
Rockwell Automation
Detroit W/WW Team Leader

Copyright © 2010 Rockwell Automation, Inc. All rights reserved.

Allen-Bradley • Rockwell Software

Rockwell Automation

Governmental mandated Security

Water and wastewater utilities have a long and distinguished history of protecting public health and the environment. Following the events of September 11, 2001 and subsequent natural disasters, all levels of government, as well as the private sector, are partnering with water utilities to prevent, respond, and recover from natural disasters and manmade (terrorist) threats.

Future water security?

What does security mean to you?

Webster's Dictionary Definition

- **the quality or state of being secure: as : freedom from danger : safety : freedom from fear or anxiety : freedom from the prospect of being laid off**

Current regulations include:

- 2002 Bioterrorism Act;
- Department of Homeland Security (DHS) Presidential Directive HPD-7 on Critical Infrastructure;
- 2007 DHS Regulation on Chemical Facility Anti-Terrorism Standard (CFATS), including the Chemical System Assessment Tools (CSAT);
- Cyber Security Act of 2009 (proposed).

Water Industry security areas

Most Water operations have historically focused on physical security- Providing physical secure, limited access to plant and distribution facilities.

- Monitoring the equipment and procedures that detect and respond to security breaches at the plant and distribution system facilities. Security equipment may include gates, cameras, motion sensing lights, door contacts, ladder and window motion detectors, and access hatch detectors.

Cyber Security is focused at protecting the control system infrastructure

Design, install and maintain ICS (Industrial Control Systems) and SCADA systems that can operate without loss of critical function both during and after a cyber attack. Control system components include:

- Computers, PLC's, DCS and Networks supporting critical plant operations.

Cyber Security Regulations for the Water Sector

security JACK MOYER, COLUMN COORDINATOR

and preparedness

BY RICK DAKIN, RICHARD NEWMAN, AND DANIEL GROVES

Dakin

Newman

Groves

AWWA Journal December 2009

The Case for Cyber Security in the Water Sector

52

As a critical infrastructure supporting a wide range of vital government, commercial, and consumer services, the water sector is a potential target for terrorist attacks. The Government Accountability Office (GAO) has identified significant vulnerabilities as well as the need for public- and private-sector stakeholders to cooperate in risk mitigation planning. Because the majority of water systems are owned by municipal entities or private-sector companies, federal regulations have begun to establish a baseline for all entities to build justified security controls into water sector systems. Those regulations include

- 2002 Bioterrorism Act;
- Department of Homeland

files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf). The vision of this cyber security program is to design, install, and maintain control systems that ensure the water sector can operate with no loss of critical function both during and after a cyber attack. The roadmap establishes a clear vision for a water-sector cyber security program and a framework to guide the development of industry-specific cyber security control objectives and metrics.

However, the detailed security engineering work to assess risks and design baseline security controls has not been completed. Each water system operator has the opportunity to contribute to this review and provide input into the

migration to off-the-shelf systems provided cost reductions, improved usability, and resulted in other benefits. However, these benefits were accompanied by increased vulnerabilities to cyber threats.

To improve operator efficiencies and accelerate response to system alerts, many of the critical control systems in the water sector can now be accessed remotely and/or accessed through the Internet, an intranet, or wireless communications. As a result, sensitive systems can also be accessed by unauthorized users who may misuse systems or data—as has happened in the financial, healthcare, and bulk electric sectors of the nation's critical infrastructure.

Although water systems do not

In the news 2010

Pentagon: The global cyberwar is just beginning

The Pentagon and its NATO allies are looking at how to improve their defenses against a cyberwar, but the basic question of how to define a cyberattack is complicating efforts.

A map is displayed on one of the screens at the Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado Springs, in July. US national security planners are proposing that the 21st century's critical infrastructure – power grids, communications, water utilities, financial networks – be similarly shielded from cyber marauders and other foes.

Rick Wilking/Reuters

More USA

At NATO summit, Obama's ride is talk of the town

Tech Center: Insider Threat

E-mail this page | Print this page | BOOKMARK

Security Incidents Rise In Industrial Control Systems

Even with minimal Internet access, malware and breaches are increasingly occurring in utility, process control systems

Apr 14, 2010 | 05:46 PM

By Kelly Jackson Higgins
DarkReading

While only about 10 percent of industrial control systems are actually connected to the Internet, these systems that run water, wastewater, and utility power plants have suffered an increase in cybersecurity incidents over the past five years.

A new report based on data gathered by the Repository of Industrial Security Incidents (RISI) database provides a rare look at trends in malware infections, hacks, and insider attacks within these traditionally cloistered operations. Cybersecurity incidents in petroleum and petrochemical control systems have declined significantly over the past five years--down more than 80 percent-- but water and wastewater have increased 300 percent, and power/utilities by 30 percent, according to the 2009 Annual Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems.

The database logs security incidents in process control, SCADA, and manufacturing systems, and gathers voluntary submissions from victim companies as well as from news or other reports.

Nearly half of all security incidents were due to malware infections -- viruses, worms, and Trojans, according to the report. With only a fraction of control systems connected to the Internet, these infections are occurring in other ways: "A lot of control systems are connected to their business networks which in turn may be connected to the Internet. It's several layers removed, but once there's a virus [on the business network], it finds its way into the control systems," says John Cusimano, executive director of the Security Incidents Organization, which runs the RISI database. "And you see USB keys bringing in malware" to the

Insider Threat Reports

3 Strategies to Protect Endpoints from Risky Applications
Most organizations have invested considerable time and effort in improving their endpoint risk management processes, but many are ill-equipped to handle myriad third-party applications that increasingly introduce the most risk into today's IT environment. As IT has reduced the risk profile of PC and server operating systems, cyber-criminals have started to look for greener pastures. Learn three strategies to effectively take control of organizational endpoints and mitigate the rising risk from third-party applications.

Inside Out: Protecting Your Partnerships -- and
Today's businesses depend on e-commerce amor
third parties to access internal networks may endar
IT security pros ensure that contractors, supplies ar
they need -- without becoming threats? This report

Rotten Apples: How To Detect And Stop Malicio
Organization
Most data leaks are unintentional - but in every ente
hard cases that defy this truism and threaten the ve
data.What can you do to stop these rotten apples fr
knowledge of your organization - and its data acces
havoc? This report offers a detailed look at how malicious insid
data, how they're motivated, and what you can do to stop them.

Other reports from the Insider Thr Center:

- Understanding The Insider Threat
- Well-Meaning Employees -- And How To Stop Them

Related Content

Sponsored by:

Anatomy of Insider Risk: Why You Could Be Your Worst
Organizations are typically aware of the problems they face f
firewall, but so many leaders focus on the risk of thieves and
employees that they leave too much room for error from the

Home | Topics | Blogs | Multimedia | Resources | About

Home › Compliance & Regulations ›

October 24, 2010, 12:39PM

SCADA Vendors Still Need Security Wake Up Call

by Paul Roberts

Share | Recommend(152) | Print | E-mail | Comment

Companies that make supervisory control and data acquisition (SCADA) and industrial control software are still dangerously lax when it comes to application security and vulnerable to attack, according to a researcher from security firm Tenable Inc. who warned that the use of coded administrative "backdoor" passwords of the type used by the Stuxnet worm isn't uncommon.

Speaking at the ToorCon Security Conference in San Diego, Jeremy Brown, a vulnerability researcher at security firm Tenable said that many SCADA software vendors lag far behind other IT firms in vulnerability research and lack even a basic awareness of modern security principles.
Despite the recent, high profile Stuxnet worm, which made headlines around the world by targeting Siemens industrial control system (ICS) software used in power plants and other critical infrastructure, SCADA vendors are not receptive to vulnerability reports from security researchers and often lack the internal processes to properly handle and address vulnerabilities discovered by outside researchers, Brown said.

In a world of near constant scrutiny of high profile operating systems and applications and real time security updates, the world of SCADA and ICS software still operates largely on assumptions made decades ago: that SCADA and ICS systems aren't of interest to malicious hackers, and that SCADA systems are isolated from the public Internet and, therefore, safe.
"Security is more often an add-on rather than a core component of SCADA systems," Brown said. "These are systems that are designed for long term deployments, in which software updates often require hardware updates."

As an example, Brown related a recent experience trying to report a remotely exploitable, stack based buffer overflow vulnerability in the BACNet building automation software by the firm SCADA Engine. That software, which runs on a variety of Windows platforms, is used to

Recommended Reads
Search Engine Finds Vulnerable SCADA Systems

2010 WINNER Forrester Groundswell Award threatpost

Today's Most Popular

- Google: No Cash for Trash Vulnerabilities
- PGP Disk Encryption Bricks Upgraded Macs
- NSA: Our Development Methods Are in the Open Now
- Adobe Readies Patch for Critical Reader, Acrobat Flaws
- Symantec: Stuxnet Likely Targeted Uranium Enrichment Systems

Don't be an accomplice! Find out if your IT department is enabling cybercrime. Get The Whitepaper » KASPERSKY

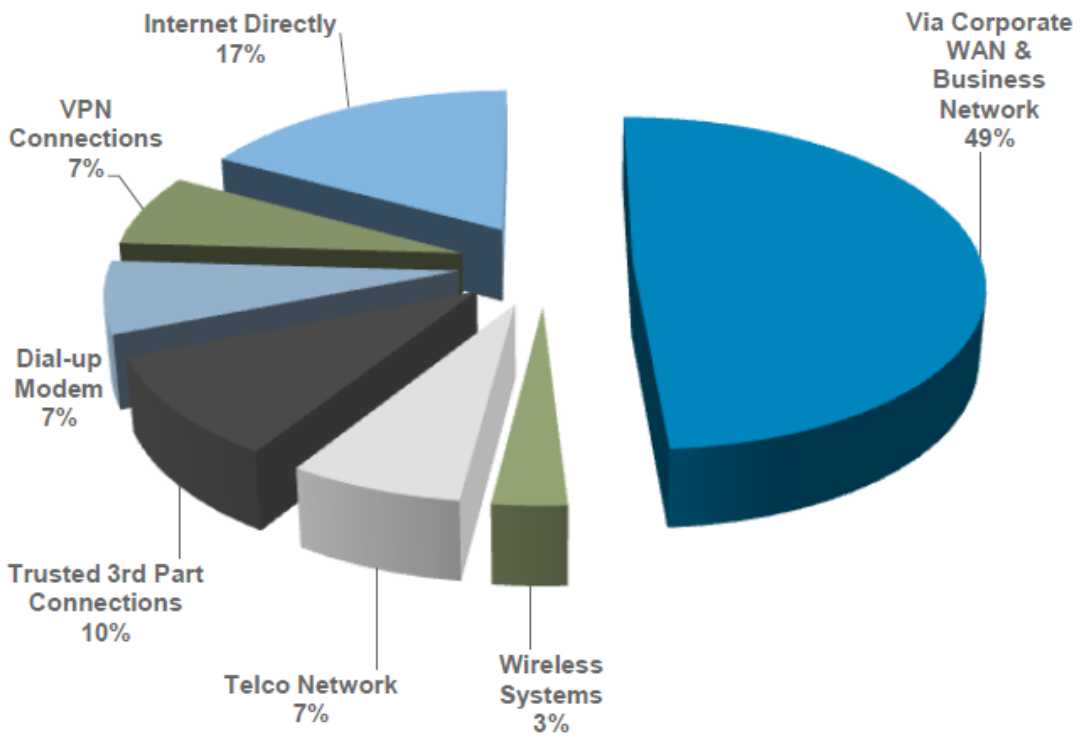
Newsletter Sign-up

Security news and analysis with expert opinion and perspective from the Threatpost editors.

Sources of Security Breaches

Industrial Security Incident Database

External Attacks on Control Systems



Source: Eric Byres, P. Eng, Byres Security, Inc, 05/08/08

History of Cyber Attacks in W/WW

- SALT River Project SCADA Hack
- Maroochy Shire Sewage Spill
- Software Flaw makes MA Water undrinkable
- Trojan/Keylogger on Ontario Water SCADA System
- Viruses Found on Auzzie SCADA Laptops
- Audit/Blaster Causes Water SCADA Crash
- DoS Attack on Water System via Korean Telecom
- Penetration of California Irrigation District Wastewater Treatment Plant SCADA
- SCADA System Tagged with Message, "I enter in your server like you in Iraq."
- SCADA Breach in Harrisburg, PA by an external hacker

Source: Guy Richards, Institute of Engineering and Technology, 11/08/08

Recent Activities

By the end of 2009 Repository of Industrial Security Incidents (RISI) indicated an increase in the incident rate in the water and wastewater cyber attacks by over 300%.

RISI is a subscription-based industry-wide repository for collecting, analyzing and sharing information regarding cyber security incidents that directly affect SCADA, manufacturing and process control systems.

Key Message from industry consultants

"In a world of near constant scrutiny of high profile operating systems and applications and real time security updates, the world of SCADA and ICS software still operates largely on assumptions made decades ago: that SCADA and ICS systems aren't of interest to malicious hackers, and that SCADA systems are isolated from the public Internet and, therefore, safe. "Security is more often an add-on rather than a core component of SCADA systems,"

Jeremy Brown, a vulnerability researcher at security firm Tenable- Speaking at the ToorCon Security Conference in San Diego

"None of the industrial control systems used to monitor and operate the nation's utilities and factories were designed with security in mind. Moreover, their very nature makes them difficult to secure. Linking them to networks and the public Internet only makes them harder to protect."

Said by Joseph Weiss, executive consultant for KEMA Consulting

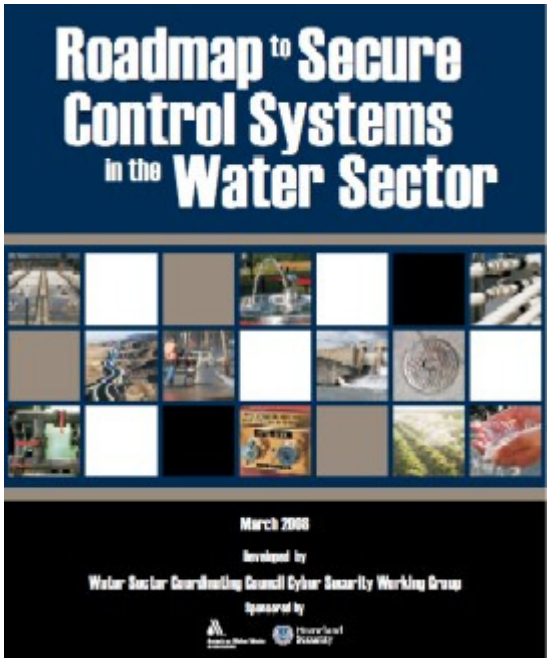
Quotes from "Roadmap to Secure Control Systems in the Water Sector"- March 2008

Key AWWA document –

-Per Kevin Morley National AWWA Security Program Mgr

Developed by Water Sector Coordinating Council

Cyber Security Working Group AWWA/HSA



Trends:

"Cyber threats to ICS are changing and growing. Computer attackers are seeking new targets and criminal extortion is increasing. ICS security is no longer simply about blocking hackers or updating anti-virus software. A new underground digital economy now provides a multi-billion dollar incentive for potential adversaries to exploit ICS vulnerability."

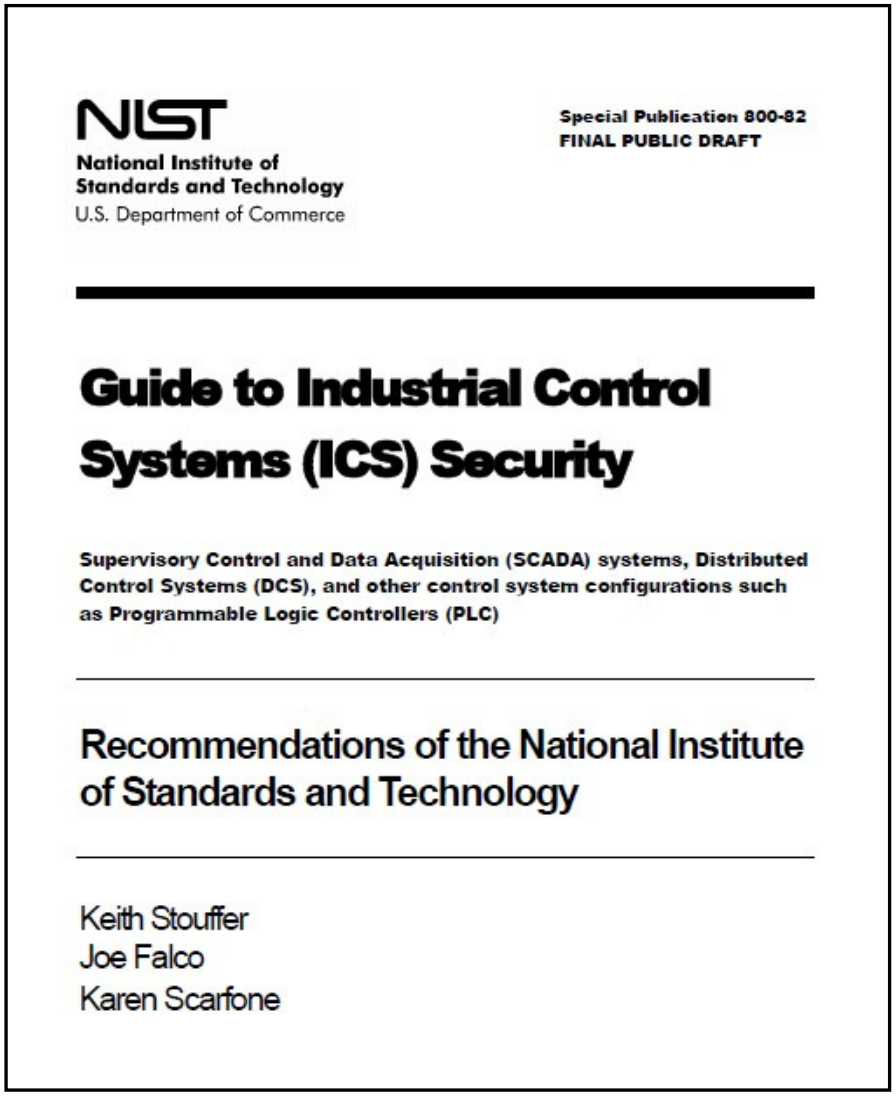
"While much security work has focused on physical security—fences, guards, intrusion detection, etc.— efforts pertaining to the resiliency of industrial control systems (ICS) have become more urgent. Advances in securing ICS must go far beyond the pressing security concerns of today by taking a comprehensive approach"

Roadmap Call to Action: The most comprehensive security improvements are realized with the development and adoption of next-generation ICS architectures, which are inherently secure and offer enhanced functionality and performance. These systems can provide defense-in-depth with built-in, end-to-end security, integrating the I.T and Process Control system.

Governmental Guidelines-NIST
National Institute of Standards and Technology

Guide to Industrial Control Systems (ICS) Security

- Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-82
FINAL PUBLIC DRAFT

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Recommendations of the National Institute of Standards and Technology

Keith Stouffer
Joe Falco
Karen Scarfone

What is NERC CIP?

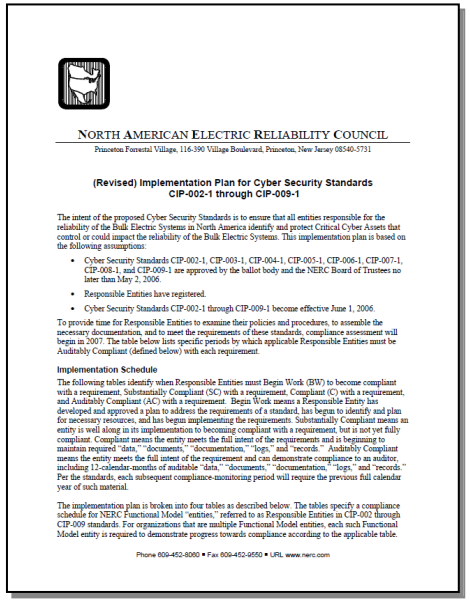
Federal Energy Regulatory Commission (FERC) to enforce operating standards in the bulk power sector. In 2006, FERC certified the existing North American Electric Reliability Corporation (NERC) to oversee power-system accreditation and operation in the United States.

The standards that specifically pertain to the identification and protection of cyber-critical assets are commonly called NERC CIP standards.

NERC CIP standards are migrating to many other critical infrastructure.

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S critical infrastructure into the following 18 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Dams
- Energy
- Government Facilities
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Telecommunications
- Transportation
- **Water and Water Treatment**



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1

The intent of the proposed Cyber Security Standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems. This implementation plan is based on the following assumptions:

- Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than May 2, 2006.
- Responsible Entities have registered.
- Cyber Security Standards CIP-002-1 through CIP-009-1 become effective June 1, 2006.

To provide time for Responsible Entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin in 2007. The table below lists specific periods by which applicable Responsible Entities must be Auditably Compliant (defined below) with each requirement.

Implementation Schedule

The following tables identify when Responsible Entities must Begin Work (BW) to become compliant with a requirement, Substantially Compliant (SC) with a requirement, Compliant (C) with a requirement, and Auditably Compliant (AC) with a requirement. Begin Work means a Responsible Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements. Substantially Compliant means an entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant. Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records." Auditably Compliant means the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records." Per the standards, each subsequent compliance-monitoring period will require the previous full calendar year of such material.

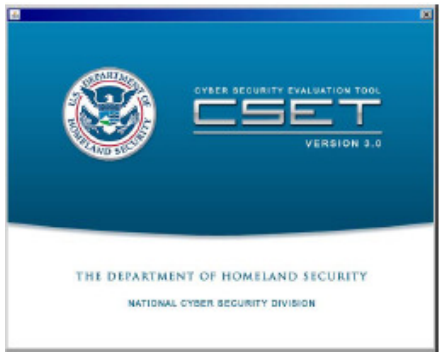
The implementation plan is broken into four tables as described below. The tables specify a compliance schedule for NERC Functional Model "entities," referred to as Responsible Entities in CIP-002 through CIP-009 standards. For organizations that are multiple Functional Model entities, each such Functional Model entity is required to demonstrate progress towards compliance according to the applicable table.

Phone 609-452-8060 ▪ Fax 609-452-9550 ▪ URL www.nerc.com

DHS-Cyber Security Strategy

Cyber Security Evaluation Tool (CSET)
Performing an Assessment

The future belongs to the efficient

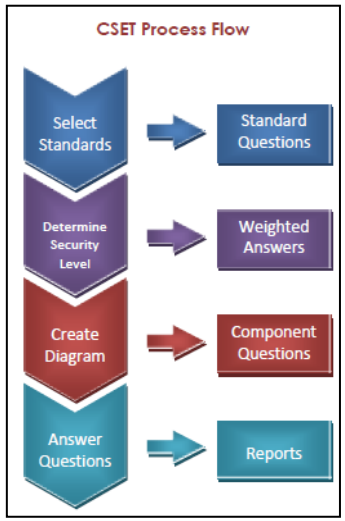


Evaluate existing system

- Follow AWWA Roadmap
- Use Dept Homeland Security CSET (Cyber Security Evaluation Tool) version 3.0 Self evaluation tool
- *http://www.us-cert.gov/control_systems/satool.html*
  - Identify plant vulnerabilities
  - Establish strategies to address vulnerabilities

Existing system-

- Look for ways to improve existing system robustness, resiliency
- How does my system respond to a power outage/equipment failure
- Is existing system backed up?



Security is best and least expensive if designed in… not bolted on…

New systems –

- Mandate new CIP projects include cyber security strategy- *Defense in Design*
- ***Establish partnership with a control system vendor***

W/WW Examples of Cyber Security

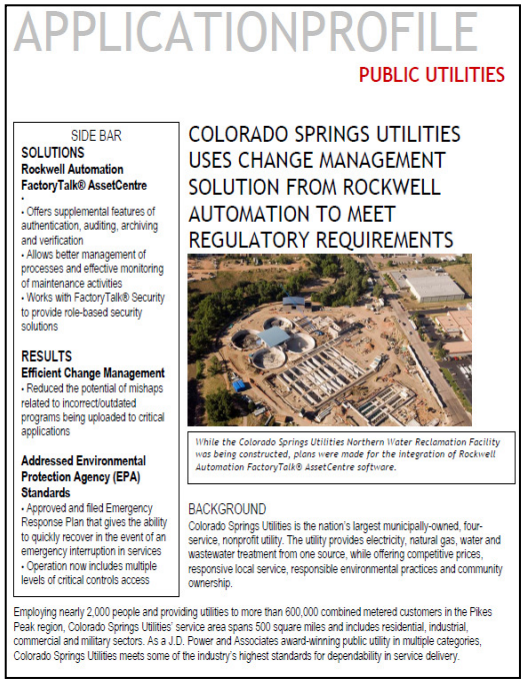
Goal- Secure remote Access

- **OCWRC-Oakland County Water Resources Commission**
  - Coordinated CSO Basin Command and Control Remote Access

Goal- More resilient control system

City of Trenton Michigan WWTP

- Process Control System Disaster Recovery
  - Small wastewater plant
- **Colorado Springs Utilities**
  - Process Control System Disaster Recovery
    - Multiple Water, Wastewater and power plants



APPLICATIONPROFILE

PUBLIC UTILITIES

SIDE BAR

SOLUTIONS

Rockwell Automation FactoryTalk® AssetCentre

- Offers supplemental features of authentication, auditing, archiving and verification
- Allows better management of processes and effective monitoring of maintenance activities
- Works with FactoryTalk® Security to provide role-based security solutions

RESULTS

Efficient Change Management

- Reduced the potential of mishaps related to incorrect/outdated programs being uploaded to critical applications

Addressed Environmental Protection Agency (EPA) Standards

- Approved and filed Emergency Response Plan that gives the ability to quickly recover in the event of an emergency interruption in services
- Operation now includes multiple levels of critical controls access

COLORADO SPRINGS UTILITIES USES CHANGE MANAGEMENT SOLUTION FROM ROCKWELL AUTOMATION TO MEET REGULATORY REQUIREMENTS

While the Colorado Springs Utilities Northern Water Reclamation Facility was being constructed, plans were made for the integration of Rockwell Automation FactoryTalk® AssetCentre software.

BACKGROUND

Colorado Springs Utilities is the nation's largest municipally-owned, four-service, nonprofit utility. The utility provides electricity, natural gas, water and wastewater treatment from one source, while offering competitive prices, responsive local service, responsible environmental practices and community ownership.

Employing nearly 2,000 people and providing utilities to more than 600,000 combined metered customers in the Pikes Peak region, Colorado Springs Utilities' service area spans 500 square miles and includes residential, industrial, commercial and military sectors. As a J.D. Power and Associates award-winning public utility in multiple categories, Colorado Springs Utilities meets some of the industry's highest standards for dependability in service delivery.

Colorado Springs Utilities- Colorado

Providing security in an unsecured world at Colorado Springs Utilities

Copyright © 2010 Rockwell Automation, Inc. All rights reserved.

Overview

- Service area - approximately 500 square-miles (gas)
- Electric customers - 194,000
- Gas customers - 169,000
- Water customers - 121,000
- Wastewater customers - 118,000
- Proposed 2005 budget - $948 million
- Employees - 1,978
- Total Asset Value - $2.6 billion ($1.3 billion debt)

Events leading to the ICS- Control system recovery systems installation

- 9/11/01 Terrorist attack USA
  - **Congressional authorization under the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (the Bioterrorism Act)**
    - conduct a vulnerability assessment
    - certify its completion
    - submit a copy of the assessment to EPA according to a specified schedule
    - prepare or revise an emergency response plan
    - certify plan to EPA within six months of completing a vulnerability assessment

Source: U.S. EPA(Confidential – For Internal Use Only) Copyright © 2010 Rockwell Automation, Inc. All rights reserved.

Events leading to the ICS- Control system recovery systems installation

- **Springs Utilities Action** (Funded by FY2002 supplemental appropriation funds)
  - conduct a vulnerability assessment ($115,000 grant) certify its completion
  - submit a copy of the assessment to EPA according to a specified schedule (03/2003)
  - prepare or revise an emergency response plan
  - certify plan to EPA within six months of completing a vulnerability assessment (09/2003)

Identified Vulnerabilities

- Springs Utilities Action (Funded by FY2002 supplemental appropriation funds)
  - vulnerability assessment review
    - Pipes and constructed conveyances
    - Physical barriers
    - Water collection, pre-treatment, treatment, storage, and distribution facilities
    - *Electronic, computer, or other automated process control systems that are utilized by the public water system*
    - The use, storage, or handling of various chemicals
    - The operation and maintenance of that system

Identified Plant locations to be covered by ICS-Disaster Recovery/back up

JD Phillips
WWTP
8 ControlLogix, 3 PLC5,
7 SLC500,13 MicroLogix
3 Workstations

Clear Spring

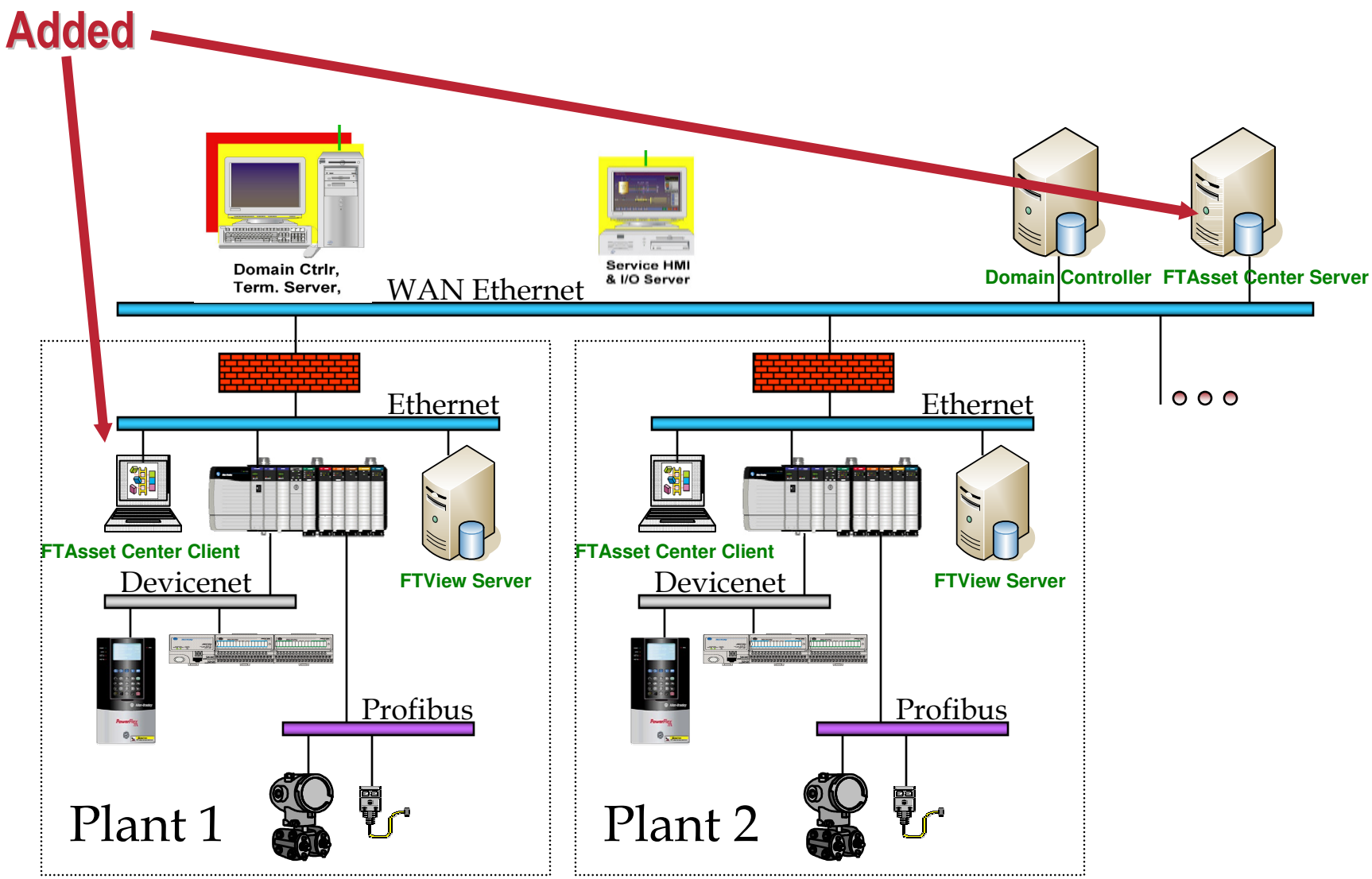
3 ControlLogix, 1 PLC5,
2 Workstations

Mesa
WTP
1 ControlLogix, 5 PLC5,
1 SLC500
2 Workstations

Fountain Valley
WTP
3 SLC500
2 Workstations

Internal Use Only) Copyright © 2010 Rockwell

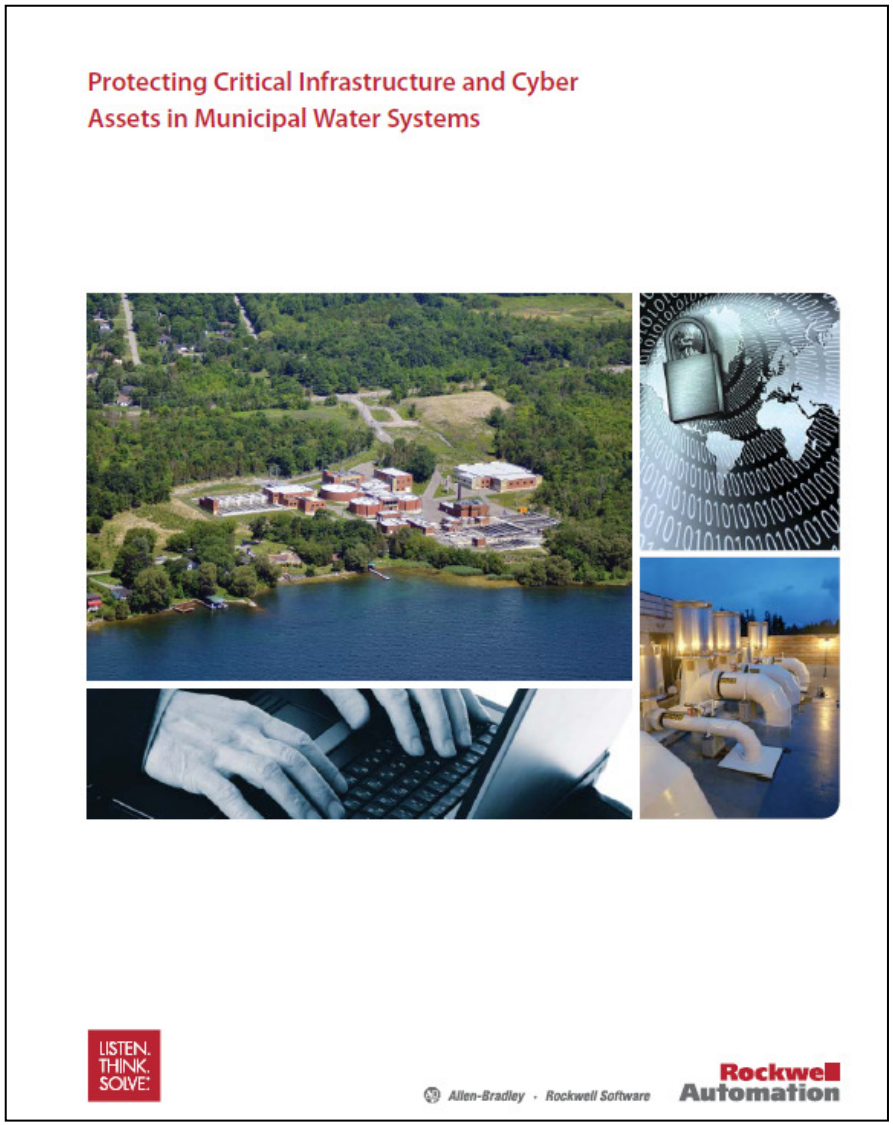
Strategies implemented to improve process control system robustness



Source: U.S. EPA(Confidential – For Internal Use Only) Copyright © 2010 Rockwell Automation, Inc. All rights reserved.

W/WW Security white paper

- Why Security matters
  - Security is not just an IT issue any more
- Evolution of risk
- Governing bodies requirements
  - What is NERC-CIP
- Compliance Strategies-
  - *Control solutions enhance system and device-level security by having products that support validated, defense-in-depth measures and design practices to enhance system and device-level security.*
  - Rockwell Security Tools
    - Hardware/software/services



Recommendations
AWWA Journal December 2009

Top 5 "Quick Hits" to Mitigate Cyber Threats

1. Inventory and diagram networks.
2. Lock system cabinets, and limit physical access to supervisory control and data acquisition (SCADA) systems.
3. Work with control vendors to "harden" systems.
4. Deploy malware protection.
5. Restrict remote access to the SCADA environment.