

Resilient and Secure Solutions for the Water/Wastewater Industry

Ron Allen
DA/Central and
Steve Liebrecht
Rockwell Automation
Detroit W/WW Team Leader

- IT People
 - Geeks... How Many?
 - Nothing but trouble!
 - Acronym Handshake

Cyber Security

- Cyber Threat in the Year 2000
 - Year 2000 = 50,000 (aprox)
- Cyber Threat in the Year 2009
- **286,000**
- Cyber Threat in the Year 2015
- **1,000,000+**

Cyber Security

- Sophistication Level of Threat (Shotgun)
 - Email - I Love You
 - Anna Kournikova
- Sophistication Level of Threat (Worm)
 - Nimda (Database)
- Sophistication Level of Threat (Targeted)
 - StuxNet (Siemens)
 - Flame (The New One)

Cyber Security

- What Can I Do??
 - Firewall (Test your own Firewall)
 - www.grc.com – use ShieldUp
- INSTALL Microsoft Patches
 - Zero Day vulnerability
 - Secunia PSI
- Anti-Virus
 - Microsoft Security Essentials

Initial Federal Regulations ...

- **Congressional authorization under the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (the Bioterrorism Act) – post 9/11/2001**
 - 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

Current Security Regulations

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)



What is NERC CIP?



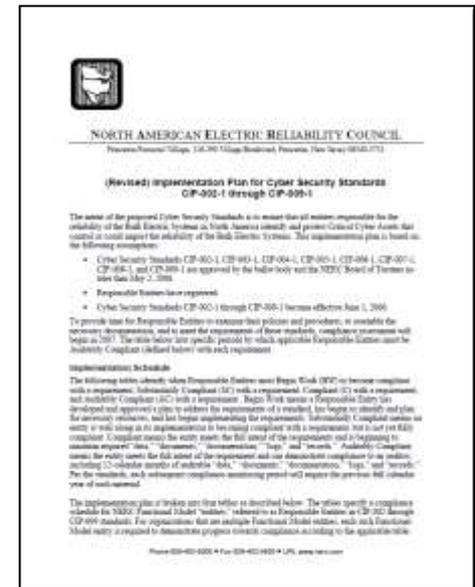
Federal Energy Regulatory Commission (FERC) to enforce operating standards in the bulk power sector. In 2006, FERC certified the existing North American Electric Reliability Corporation (NERC) to oversee power-system accreditation and operation in the United States.

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 infrastructures.

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**



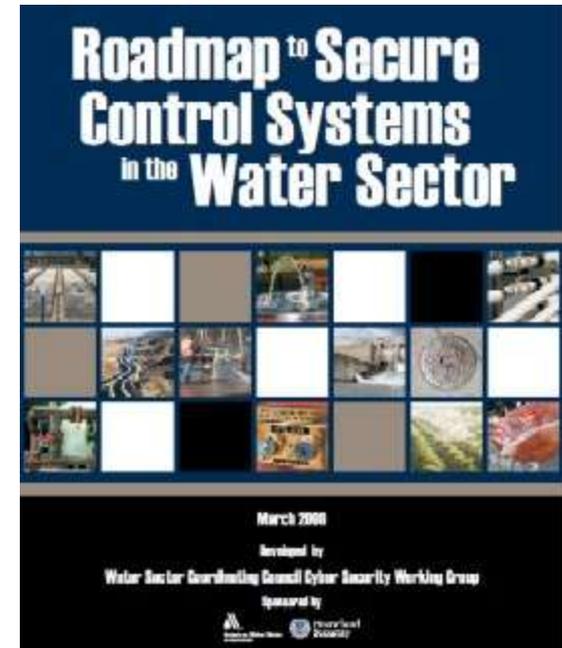
“Roadmap to Secure Control Systems in the Water Sector,” March 2008

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.**”

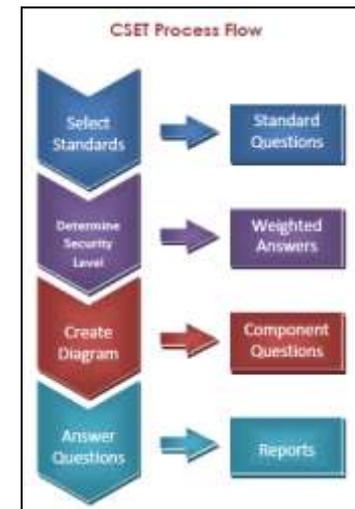
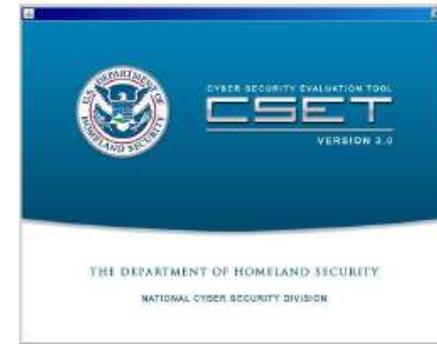


“Roadmap” Call to Action: The most comprehensive security improvements are realized with the development and adoption of next-generation ICS architectures, which are inherently secure and offer enhanced functionality and performance. **These systems can provide defense-in-depth with built-in, end-to-end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

Department of Homeland Security: Cyber Security Strategy

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
 - **Single largest vulnerability is from within**
 - Establish strategies to address vulnerabilities
- Look for ways to improve its robustness, resiliency
- How does it respond to a power outage/equipment failure
- Is your control system backed-up?



New systems

Mandate new CIP projects that include cyber security strategy -
Defense in Design

- **Establish partnership with a control system vendor**
 - Consider a holistic/plant wide approach to protecting the plant

Cyber Security Evaluation Tool
(CSET)
Performing an Assessment

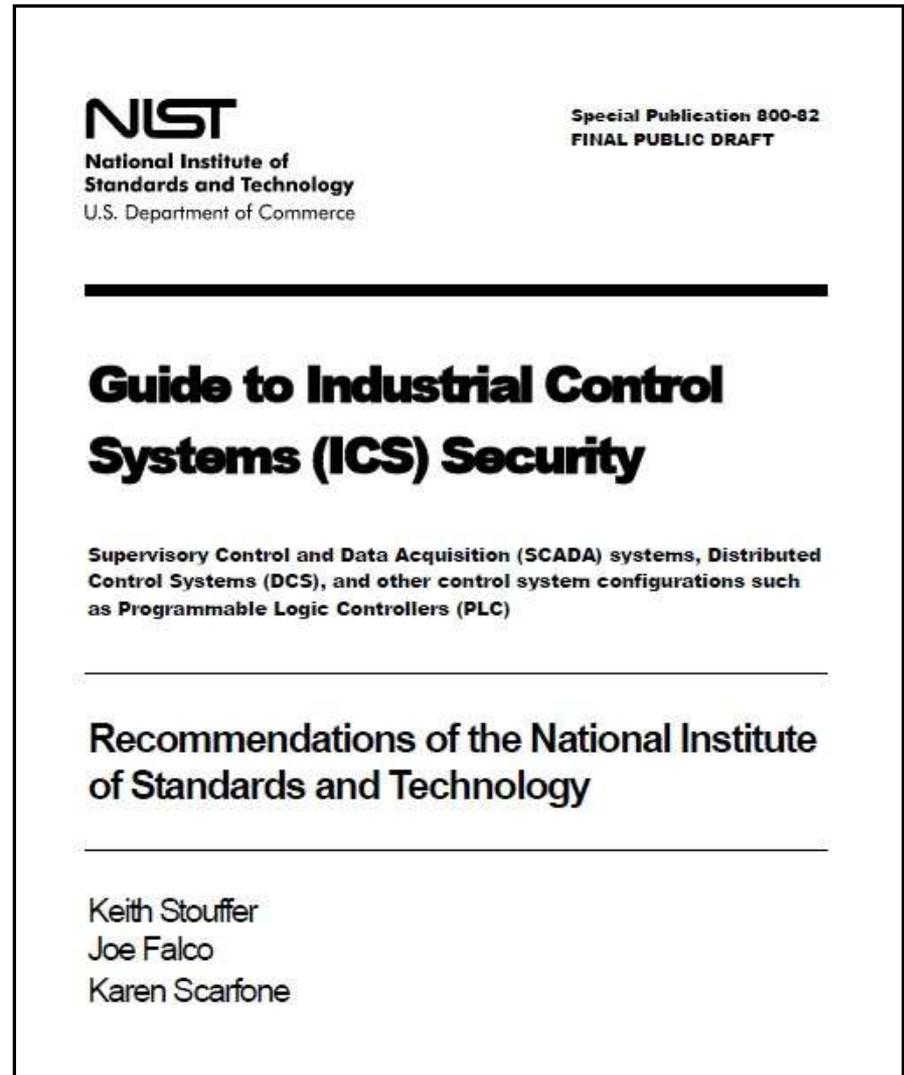
Single largest vulnerabilities may be from within

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)



Holland BPW & DHS CSSP Partnership

Doug Nibbelink, IT Security Specialist
Holland Board of Public Works

DHS Control System Security Program -
They're from the government, and they really
helped us.



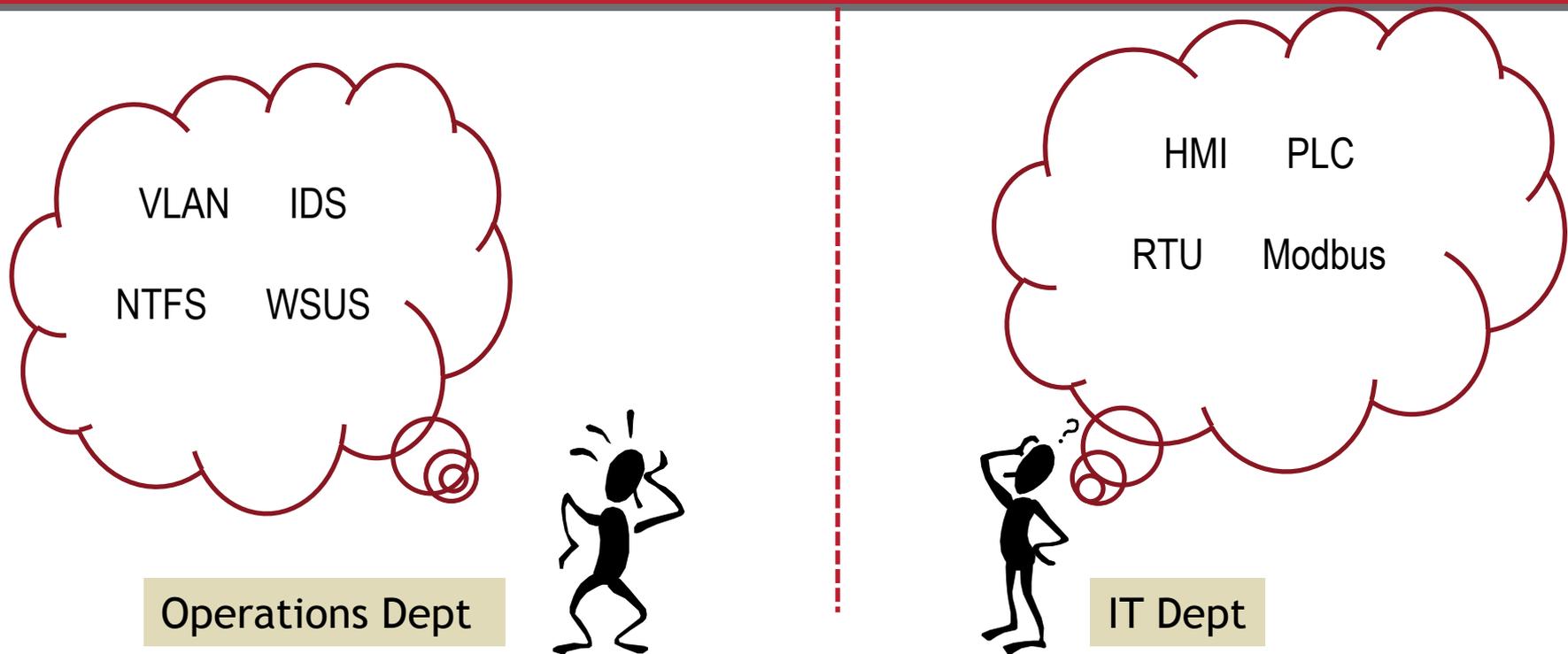
+



Control Systems
Security Program =

?

Challenges IT vs Operations



- Separation of Operations/Control Systems/SCADA vs. IT
- Different worlds/foreign languages and Gaps in shared knowledge
- How do you protect and secure what you don't understand?
Probably not very well...

Holland BPW Security Evolution

- Technology Director attended 1 day training on Control Systems Security put on by DHS CSSP-Instructor mentioned availability of DHS CSSP onsite assessment
- AWWA sent letter about availability of CSET software (Cyber Security Evaluation Tool)
- In 2010 HBPW staff began discussions with DHS CSSP about an onsite assessment
- In January 2012, 3 staff from DHS CSSP came to Holland to facilitate cyber security TTX.

W/WW Cyber Security References

Customer Success Story:

Colorado Springs Utilities

- Goal: More resilient control system
 - Process control system disaster recovery
 - Multiple water, wastewater and power plants

Public Utilities
Colorado Springs Utilities Uses Change Management Solution from Rockwell Automation to Meet Regulatory Requirements

Solutions
FactoryTalk® FactoryTalk® AssetCenter

- Offers supplemental features of authentication, auditing, archiving and verification
- Allows better management of permissions 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 installed 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

Background
Colorado Springs Utilities four-service, nonprofit utility gas, water and wastewater competitive prices, responsible practices and community

Employing nearly 2,000 people, 600,000 combined meters Colorado Springs Utilities includes residential, industrial, power and associated categories, Colorado Springs highest standards for deep

Protecting Critical Infrastructure and Cyber Assets in Municipal Water Systems



LISTEN THINK SOLVE

© Allen-Bradley

Rockwell Automation

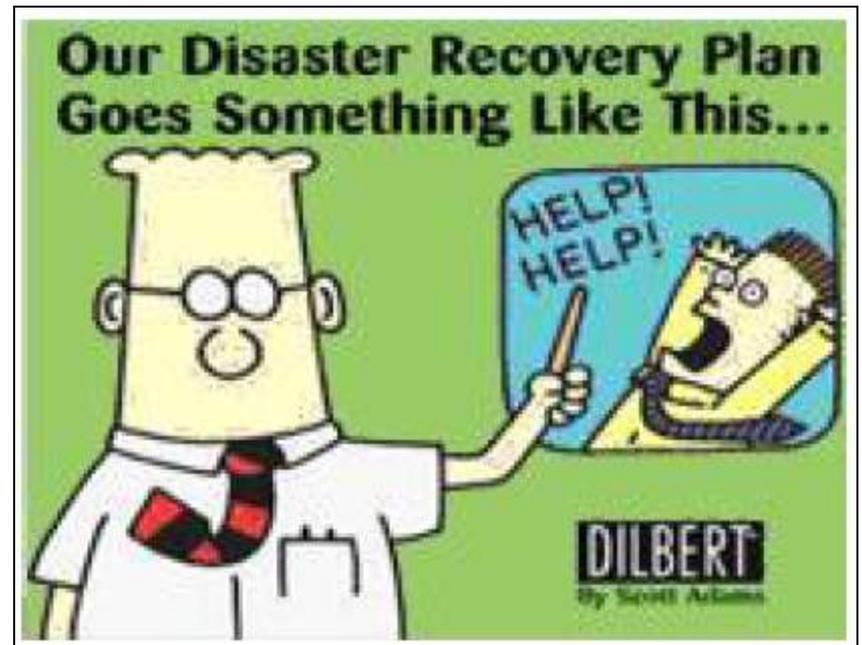
W/WW Security White Paper

- 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

Cyber Security-Take Aways

Key Questions

- How would your operations change if we did not have SCADA working?
- How sure are you that our SCADA systems are secure?
- When was the last time you performed cyber security vulnerability assessments?
- What would be the impact to your organizations if we were aware of vulnerabilities and did nothing?



Cyber Security-Take Aways-Suggestions

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
- Look for ways to improve its robustness, resiliency

New systems

- Work with Consultants to mandate new CIP projects that include a cyber security strategy - *Defense in Design*
- Establish partnership with a control system vendor

Rockwell Automation Security Key Points

- Practice 5 simple, actionable steps to enhance industrial security:



1. **Control who has access**
2. **Employ firewalls and intrusion detection/prevention**
3. **Patch and update your control system hardware/software**
4. **Manage your passwords**
5. **Turn the PLC processor key(s) to Run mode**

- Mandate new CIP projects include cyber security strategy - *Defense in Design*
 - Consider a holistic/plant wide approach to protecting the plant
 - Establish partnership with a control system vendor
- Rockwell Automation control products are developed following the latest governmental security guidelines using our design-for-security philosophy and include features to facilitate physical and logical access control
- We also provide free resources to help:
 - www.rockwellautomation.com/security
- We offer Network & Security Services to help you comply with security-oriented regulations and standards
www.rockwellautomation.com/services/security/



Enhance industrial security to improve robustness, reduce risk, and vulnerability

Resilient and Secure Solutions for the Water/Wastewater Industry

Thank You!



QUESTIONS



Ron Allen
DA/Central

Steve Liebrecht
W/WW Industry Team Leader Detroit

Rockwell Automation
sjliebrecht@ra.rockwell.com
Cell 419-340-6873