Three Simple Steps to SCADA Systems Security

Presented by:
Gabe Shones, PE / Gilbert Kwan, PE

Rockwell Automation
Process Solutions User Group (PSUG)
November 14-15, 2011
Chicago, IL - McCormick Place West
“The opportunity to secure ourselves against defeat lies in our own hands.”

Sun Tzu
Strategist and Philosopher
(Chinese Military Text 6th Century BC)
Agenda

- Technical Background
  - Step 1 – Get Ready: Educate Yourself
    - Terminology
    - What is SCADA system security?
    - Why is SCADA system security important?
    - Government efforts
    - Standards
  - Step 2 – A-I-M: Lifecycle
    - A – Assess
    - I – Implement
    - M – Maintain
  - Step 3 – Meeting Your Objective
- Case Studies
  - Case Study I – Utility, Electric, Treatment and Collections
  - Case Study II – Wastewater and Water Collections
  - Case Study III – Physical SCADA Security
- Questions and Answers
Step 1 - Get Ready: Educate Yourself!

- Terminology
- What is SCADA system security?
- Why is SCADA system security Important?
- Government efforts
- Standards
Password Policy Does Not Help If...
Terminology

- Manufacturing zone
- Enterprise zone
- Industrial automation and control system (IACS)
- Zones
- Conduits
- Demilitarized zone for automation networks (DMZ)
- North American Electrical Corporation (NERC)
- Federal Energy Regulatory Commission (FERC)
- International Society of Automation (ISA)
What is SCADA system security?

• Cyber Security
  – Vulnerability
  – Prevention

• Physical Security
  – Vulnerability
  – Prevention
Why is SCADA system security important?

- SCADA is an operations tool
- System vulnerability to cyber incidents
- Regulations passed requiring enhanced cyber security
Control Systems Vulnerability

- Commercial off-the-shelf-technology (COTS) and protocols
- Increased connectivity
  - Enterprise integration
- Remote access demand
  - 24/7 access
- Public information
Actual Incident Types

Repository of Industrial Security Incidents (RISI)

Incident Types

Unintentional 76%

Outsider Failure 65%
Insider 11%
Outsider 24%

Malware (virus, worm, trojan)

Intentional 24%

Hacker

Disgruntled employee

Insider 53%
Outsider 47%

IT Department Technician

Network device, software

© 2009, Security Incidents Organization
US Government Efforts

- Department of Homeland Security
- Department of Energy
- United States Regulatory Commission
- United States Environmental Protection Agency
- American Water Works Association
- Water Environment Federation
Cyber Security Evaluation Tool (CSET)

- Control System Cyber Security Self-Assessment Tool (CS2SAT) - 2004
- Cyber Security Vulnerability Assessment (CSVA) - 2004
- CSET Issued by the U.S. Department of Homeland Security - 2009
- Self assessment performed by Utility

- http://us-cert.gov/control_systems/csetdownload.html
READY? Educate Yourself
NERC CIP 002 - 009

- NERC, 18 CFR Part 40, “Mandatory Reliability Standards for Critical Infrastructure Protection (CIP)”

Step 1
Critical Asset Identification and Risk Assessment

Step 2
Security Policy Creation / Update

Step 3
Disaster Recovery Planning

Step 4
Deployment of Protective Measures (Security and Recovery)

Step 5
Security Monitoring and Management

The Recommended Five Steps to NERC CIP Compliance
Standardization Efforts

- International Society for Automation (ISA)
- International Electrotechnical Commission (IEC)
- National Institute for Standards and Technology (NIST)
- Canadian Standards Association (CSA)
Industry Specific Roadmaps & Guidelines

National Infrastructure Protection Plan
Water Sector

Homeland Security Presidential Directive 7 (2009) 2 identified 17 critical infrastructures and key sectors (CIS), such as the Water Sector, that must be prioritized for protection, sharing of information, and development of joint strategies. This Roadmap provides a strategic framework to improve the security of the Water Sector.

Sector Overview
- The Water Sector is responsible for providing drinking water and wastewater services.
- The Water Sector is vulnerable to a wide range of threats, including physical and cyber attacks.
- The Water Sector is critical to the delivery of essential services and economic vitality.

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

Protection of the Water Sector from Security Threats
The Emerging Legal and Policy Frameworks

Security Guidance for Wastewater/Stormwater Utilities
December 9, 2004

Strategy for Securing Control Systems
Coordinating and Guiding Federal, State and Private Sector Initiatives
October 2009

Roadmap to Secure Control Systems in the Energy Sector
January 2009

Homeland Security
U.S. Department of Energy
National Cyber Security Division

Control Systems Security Program
National Cyber Security Division
Industry Specific Roadmaps and Guidelines

- Roadmap to Secure Control Systems in the Water Sector
- Roadmap to Secure Control Systems in the Energy Sector
- Interim Voluntary Security Guidance for Wastewater / Stormwater Utilities
- National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency
- Protecting the Water Sector from Security Threats: The Emerging Legal and Policy Frameworks
- Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
## ISA 99 Work Products

<table>
<thead>
<tr>
<th>ISA99 Common</th>
<th>Security Program</th>
<th>Technical - System</th>
<th>Technical - Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA-99.01.01 Terminology, Concepts And Models</td>
<td>ISA-99.02.01 Establishing an IACS Security Program</td>
<td>ISA-TR99.03.01 Security Technologies for Industrial Automation and Control Systems</td>
<td>ISA-99.04.01 Embedded Devices</td>
</tr>
<tr>
<td>ISA-TR99.01.02 Master Glossary of Terms and Abbreviations</td>
<td>ISA-99.02.02 Operating an IACS Security Program</td>
<td>ISA-99.03.02 Security Assurance Levels for Zones and Conduits</td>
<td>ISA-99.04.02 Host Devices</td>
</tr>
<tr>
<td>ISA-99.01.03 System Security Compliance Metrics</td>
<td>ISA-TR99.02.03 Patch Management in the IACS Environment</td>
<td>ISA-99.03.03 System Security Requirements and Security Assurance Levels</td>
<td>ISA-99.04.03 Network Devices</td>
</tr>
</tbody>
</table>

*Courtesy of ISA 99 Committee*
ANSI/ISA S99.02.01-2009

- Establishing an IACS Security Plan
Applying ANSI/ISA S99.02.01-2009 to ANSI/ISA-95

Level 4
Business Planning and Logistics
Plant Production Scheduling, Operational Management, etc.

Interface addressed in ISA 95.01 / 02

Level 3
Operations and Control
Dispatching Production, Detailed Production Scheduling, Reliability Assurance...

S95.03 Area

Levels 2,1,0
Continuous Control Systems
Discrete Control Systems
Batch Control Systems

S95 Reference to S88
STEP2: A-I-M!

- The Security Lifecycle
  - A – Assess
  - I – Implement
  - M – Maintain
A- Assess

- Risk assessments and critical asset identification
- Perform a SCADA assessment
- Perform a risk analysis
- Create a security policy
<table>
<thead>
<tr>
<th>Intent</th>
<th>Threat Source</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Existing Safeguards</th>
<th>Consequence</th>
<th>Severity</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Intentional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|        | Outsider      | Modify stored data (e.g. history, programs) | Network security breach | Corporate firewall/VPN, authentication | 1. Economic Loss  
2. Food Safety | High     | Med         | Med     |
|        |               | Install malware               | Network security breach | Corporate firewall/VPN, authentication | Loss  
2. Food Safety  
3. Personnel Injury  
4. Environmental Damage  
5. Corp Image | High     | Med         | Med     |
|        |               | Steal information             | Network security breach | Corporate firewall/VPN, authentication | 1. Economic Loss  
2. Corp Image | Med      | Med         | Med     |
|        |               | Cause a network disturbance   | Network security breach | Corporate firewall/VPN, authentication | Economic Loss | Med      | Med         | Med     |
|        |               | Modify a program/configuration | Network security breach | Corporate firewall/VPN, authentication | Economic Loss, Food Safety, Personnel Injury, Environmental Damage, Corp Image | High     | Med         | Med     |
|        |               | Make a physical change (e.g. plug, unplug, switch) | Physical security breach | Physical Security | Economic Loss, Food Safety, Personnel Injury, Environmental Damage, Corp Image | High     | Low         | Med     |
|        | Unintentional  | Introduce a virus             | Infected laptop, infected media, Internet download, email attachments | Anti-virus, Policy | Economic Loss, Food Safety, Personnel Injury, Environmental Damage, Corp Image | High     | High        | Very High |
|        | Employee       | Disclose information          | Spyware, file sharing  | Anti-virus, Policy, website filtering | Economic Loss, Corp Image | Med      | High        | Med-High |
|        |               | Cause a network disturbance   | Infected laptop, network utilities | Anti-virus, Policy, website filtering | Economic Loss | Med      | Low         | Med-Low |
|        |               | Make a programming/configuration error | Human error | Training, Configuration management, Backup/Restore | Economic Loss, Food Safety, Personnel Injury, Environmental Damage, Corp Image | High     | Low         | Med     |
|        |               | Modify stored data (e.g. history, programs) | Human error | Training, Backup/Restore | Economic Loss, Food Safety | High     | Low         | Med     |
I - Implement

- Design for desired security level
- Deploy protective measures
- Test security
M - Maintain

• Monitor and manage on an ongoing basis
  – Update assessment
  – Review and update risk analysis
  – Update security policy
  – Compliance
STEP3: Meeting Your Objective

- System in place
- Apply Standards to Future Projects
- Continue to Test your Protected System
I’m Protected! Yes!
Are you hitting the target?

Mislabeled Firewalls

Mis-Configured Firewalls

IACS

DMZ for CONTROLS

Infected Laptops

VPN Connections

Remote Support

Actively monitor System

External PLC Networks

RS-232 Links

Modems

ENTERPRISE

Internet

VPN Connections

Internet
• Public Utility
  – Two Treatment Plants
  – Three 115kV Substations

• Control equipment:
  – AB PLC’s; RSView;
  – Moscad RTU;
  – Local Ethernet and Fiber Backbone

• NERC Compliance
  – Homeland Security audit

• RTU radio FCC wide band
  – Migrate to narrow band

• Overall System Improvements
Case Study I: Utility Electric, Treatment, and Collections

Sample Existing SCADA Network

O&M

Dial in

FO

DSL

Plant 2

Motorola MOSCAD RTU

Plant 1

Motorola MOSCAD RTU

Typical (20)

Motorola MOSCAD RTU

Typical (3)

Copyright © 2011 Rockwell Automation, Inc. All rights reserved.
Case Study I: Utility Electric, Treatment, and Collections

- Performed a cyber security gap analysis
- Results
  - Physical and electronic security perimeter
- Staged approach
Case Study I: Utility Electric, Treatment, and Collections

Stage 1: Short term Firewall remote access, control access, NERC

O&M

Dial in

Sys Logs Monitoring, Access Monitor

Dial in

Internet

Plant 1

Plant 2

Typical (20)

Typical (3)
Case Study I: Utility Electric, Treatment, and Collections

• Plan in place
  – Documented policies and procedures
• NERC compliance
  – Homeland Security audit
• Phased approach
  – Centrally managed and easy to roll out plan
• SCADA migration path
Case Study II: Wastewater and Water Collections

- City Public Works
  - Water reclamation facility (45MGD)
  - 130 remote sites
  - New water treatment plant

- Control equipment:
  - AB PLC’s; SCADA Software
  - Moscad RTU;
  - Fiber Optic and Copper Ethernet Backbone

- Telemetry
  - 173MHz, 450MHz, 900MHz, 4.9GHz
Case Study II: Wastewater and Water Collections

• Used ISA99 as the guiding standard
• ANSI/ISA S99.02.01-2009 establishing an IACS security program
• Followed the 7 steps in assessment
  – 1. Assess existing systems
  – 2. Document policies and procedures
  – 3. Train personnel and contractors
  – 4. Segment the control system network
  – 5. Control access to the system
  – 6. Harden the components of the system
  – 7. Monitor and maintain system security
Case Study II: Wastewater and Water Collections
Case Study II: Wastewater and Water Collections
Case Study II: Wastewater and Water Collections

• Results
  – ANSI/ISA S99.02.01-2009– WEF (unregulated)
    • Through workshops establishing an IACS security program
    • Assessment report based on ISA99 structure
    • IT and SCADA group need to be involved – management buy in
    • ISA95 Model

• Critical recommendation
  – Stage 1: Implement immediately
  – Stage 2: Implement gradually
  – Stage 3: Internal COB cyber security team evaluation topics
Case Study II: Wastewater and Water Collections

ISA 95 to Organize ISA 99 Implementation

Diagram showing network architecture with levels 4, 3, 2, 1, and 0. Interfaces mentioned in ISA 95.01/02 and 595.03 Area. Public Works network with DMZ, WRF SCADA, Outback SCADA, and Boyd SCADA networks.
Case Study III: Physical SCADA Security

• Pacific Northwest correctional facility
• 58 different security stations (computers) on one control network
• HMI software product
Case Study III: Physical SCADA Security

- Security philosophy
  - Restrict access
  - Use PLC code to limit navigation
  - Cycle pass codes
  - No connection to other networks
Physical restrictions

- Restricted access to the site
- Restricted number of technicians responsible for maintenance
- No CD-ROM drive
- No internet access
- No keyboard – touch screen interface only
- Segregated control network, no connection to other networks
- Each computer is locked in a restricted room or cabinet
Software Restrictions
- No Windows games loaded
- Only runtime versions deployed
- Development computer located in a restricted access room
- Boot up automatically starts application in “run” mode
- In run mode the Windows key and alt key are disabled
- Only a unique key sequence can interrupt the runtime application
“The opportunity to secure ourselves against defeat lies in our own hands.”

Sun Tzu
Strategist and Philosopher
(Chinese Military Text 6th Century BC)
Thank You

• Contact Information
  – Gabe Shones, PE
    gabe.shones@harrisgroup.com
    503.345.4574
  – Gilbert Kwan, PE
    gilbert.kwan@harrisgroup.com
    206.494.9583