SCADA SYSTEM SECURITY: NAVIGATING RISK MANAGEMENT

Jason Davis, PE, McKim & Creed
SO YOU HAVE AN AGING SYSTEM?

Specialized, aged components

Isolated from other networks

Cybersecurity not needed
THE MODERN SCADA SYSTEM

- Not constrained inside plant
- Focused on functionality
- Work **Smarter** not harder
- SCADA resembles IT
THEORY – THE PERFECT JOB

Access Anywhere

Auto Mode = Auto Pilot

Life Is Good!
PRACTICE – THE REAL WORLD

\[ \text{Complexity} = \uparrow \text{Risk} \]

Many threats are obvious...

- Attacks
- Natural Disasters
- Equipment Failure

Other threats are more subtle...

- Disgruntled / Former Employees
- Human Error
WHERE DO YOU START?

I know the “What” but not the “How”

So many THREATS!

What is RISK?
SCADA SYSTEM SECURITY IMPROVEMENT PROGRAM

**RISK:** The potential loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability
SCADA SYSTEM SECURITY IMPROVEMENT PROGRAM

4. Document Assets and Architectures
5. Perform Vulnerability Assessment
6. Define Risk Mitigation Methods
7. Train Staff
STEP 1: BUSINESS CASE

Framework
• Framed around Business, Founded in Experience

Benefits
• Improved Security, Reliability, Availability

Threats / Consequences
• Prioritized Threats
• Physical, Economic, Social Consequences

Security Program
• Process / Costs / Resources
STEP 2: CROSS-FUNCTIONAL SECURITY TEAM

Attack Issues from Different Angles

Teammates

- Management
- Information Technology
- Engineering
- Operations
- Maintenance
- Security Consultant
STEP 3: DEFINE POLICY AND PROCEDURES

Organizational Cornerstone

Secure and Sustainable Environment
• Define clear objectives
• Enforceable personnel direction

CAUTION
Operations vs Security

Policies = Living Documents
STEP 4: DOCUMENT ASSETS AND ARCHITECTURES

- Identify Components
- Store Configurations
- Record Architectures
STEP 5: PERFORM A VULNERABILITY ASSESSMENT

Hire a Security Consultant
- Extension of Security Team
- Identify Unique Organizational Needs

Industry Standards
- NIST SP800-82
- ISA 99
- AWWA
- Dept. of Energy
- Guidelines instead of Law
STEP 5: PERFORM A VULNERABILITY ASSESSMENT

Policy / Procedure Vulnerabilities
• Incomplete or nonexistent policies/SOPs

Platform Vulnerabilities
• Flaws or misconfiguration of hardware/software

Network Vulnerabilities
• Flaws or misconfiguration of networks

Operational Vulnerabilities
• Operational scenarios resulting in downtime/loss
STEP 5: PERFORM A VULNERABILITY ASSESSMENT

Prioritize Threats
• Severity of Impact
• Likelihood of Occurrence

Execution Plan
• Budget Constraints
• Mitigation Effort

Report
• Tailored Around Client
STEP 6: DEFINE RISK MITIGATION METHODS

Management Controls

A Living Process!
STEP 6: DEFINE RISK MITIGATION METHODS

Operational Controls

• Implemented by People

Examples

• Personnel Security
• System Maintenance
• Contingency Planning
STEP 6: DEFINE RISK MITIGATION METHODS

Technical Controls
• Implemented by Systems

Examples
• Access Control
• Data Flow Control
STEP 7: TRAIN PERSONNEL

Operations vs Security
  • Awareness = Tolerance

Practice Makes Perfect
  • Sandbox
FOUNDATIONAL PHILOSOPHY

• Different Organizations Have Different Levels of Risk

• Document Everything: Components, Configurations, Architecture

• Approach Security as a TEAM

• Standards: One Size Does Not Fit All

• Operations vs Security
  → Don’t Create Your Own Prison

• Security is a Living Process
SECURITY: GOOD PLAN = GOOD IMPLEMENTATION
Thank you for the opportunity.

QUESTIONS?
Contact: Jason Davis, PE
jdavis@mckimcreed.com