Challenges of Securing and Auditing Control Systems

James W. Sample, CISSP, CISM
Manager of Information Security
Enterprise Risk Management
Objectives

- Control System Overview – SCADA and the Power Grid
- SCADA Cyber Security
- Is the SCADA Cyber Security Threat Real?
- Auditing SCADA
Control Systems Overview - SCADA and the Power Grid
Supervisory Control and Data Acquisition (SCADA)

CONTROL
• Generator Set Points
• Transmission Lines
• Substation Equipment

DATA
• Critical Operational Data
• Performance Metering
• Events and Alarms

Control Center
Provides network status, enables remote control, optimizes system
performance, facilitates emergency operations, dispatching repair crews and
coordination with other utilities.

Electric power application shown. Other
SCADA applications include gas and oil
pipelines, water utilities, transportation
networks, and applications requiring
remote monitoring and control. Similar
to real-time process controls found in
buildings and factory automation.

Communications
• Directly wired
• Power line carrier
• Microwave
• Radio (spread spectrum)
• Fiber optic
Interconnected Power System Operation

~140 Control Areas in North America
Control Areas

- Responsible for Meeting Load Demand

- Automatic Generation Control (AGC)
  - Real-time generation dispatch to match load
  - Minimize area control error (ACE)

- Ensure Actual Power Flow on All Tie-Lines Match Scheduled Flows

- Assist Other Control Areas in the Interconnection with Maintaining a Relatively Constant System Frequency
Power System Control Center

- **Supervisory Control and Data Acquisition (SCADA)**
  - Controls substations within service area
  - Provides operations and network status

- **Energy Management System (EMS)**
  - Determines generator dispatch
  - Optimizes system performance

- **Emergency Operations**
  - Dispatch repair crews, coordinate with other utilities
SCADA Functions

- Real Time Database
- Data Acquisition/Processing
- Supervisory Control
- Graphical Operator Interface
- Alarm, Sequence of Events, and Historic Event Processing
- Strip Chart Trending and Mapboard Interface
EMS Functions

- **Control**
  - Automatic Generation Control
  - Voltage Control
  - Interchange Transaction Scheduling
  - Load Shedding & Restoration

- **Analysis**
  - Short Term Load Forecasting
  - Economic Dispatch

- **Security Analysis and Production Planning**
California Independent System Operator
SCADA Cyber Security
Two Views of SCADA

**Engineering**

- **Focus**
  - Safety
  - 100% Availability
  - Electro-mechanical
  - No updating, Aged equipment
- **The Language**
  - RTUs, PLCs, IEDs
  - DNP, Modbus
  - Low Bandwidth
  - Analog & Digital
- **The Vendors**
  - ABB, Honeywell, Siemens

**Information Technology**

- **Focus**
  - Security
  - 99.5% Availability
  - Electronic
  - Continuous Updating
- **The Language**
  - Routers, Switches, Servers
  - IP, Ethernet
  - High Bandwidth
  - All Digital
- **The Vendors**
  - IBM, Microsoft, CISCO, Sun, Dell
Control Systems Can Be Vulnerable

- **Examples:**
  - Data often sent in clear text
  - Protocols are open, no security
  - Vulnerability assessments have demonstrated unauthorized access to SCADA, DCS, and other systems
  - Several cases of confirmed SCADA and PLC “intrusions”
  - Laboratory testing has shown that SCADA data can be intercepted and changed without notice
  - Control networks are being integrated with corporate networks

- **It is no longer a question of can control systems be hacked... but what happens when they are**
Microprocessor/Hardware Issues

- **Current microprocessor capabilities in typical electric utility systems**
  - Predominantly range from 8088 through 486
  - Security and RTOS vendors need at least 486 capability to incorporate security technology

- **Hardware constraint**
  - Minimum 486 capability assumes sufficient computing resources and memory can be allocated to security at specific times
  - However, no requirements as to how much memory or bandwidth needs to be allocated to security
Encryption and Control Systems Don’t Mix Well

- Existing encryption technology uses block ciphers
  - DES, 3DES, AES, and other encryption protocols
- Testing has shown unacceptable results
  - Too slow
  - Uses too much memory
  - Consumes additional bandwidth
  - Doesn’t include integrity checks
- Some existing systems can’t implement encryption
- Other technologies show promise
  - eg, Stream ciphers, modified AES, RSA RC5
Vulnerable Software and Protocols

- Control system operating systems
  - NT, 2000, Linux, Unix, Solaris
- Fieldbus, MODBUS, and other buses
- Vendor and third party customized software and hardware
  - eg, RTUs now IP-enabled
- Protocols and other communication vehicles
  - Inter Control Center Protocol (ICCP-TASE.2)
  - Common Information Model (CIM)
  - DNP
  - CORBA
Other Concerns

- ActiveX
- Remote Access
  - PCAnywhere, XWindows
  - Modems
- SSL (Secure Socket Layer)
- Proprietary protocols
- Telecom and other communication media
- Field implementation impacts security certification
- Market access to control systems
- Cyber not a design basis
- Uniform Computer Information Transaction Act (UCITA)
DOE Typical Vulnerabilities Observed

- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems (already ubiquitous, trend toward wireless)
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Exploitation of pathways that inadvertently allow access to critical assets
- Lack of sensitive information protection/disposal procedures
- Vulnerabilities related to “systems of systems” (component integration)

Source: Battelle – Pacific Northwest National Laboratory, U.S. Department of Energy
The Problem

- Due to rapid changes in technologies, organizations often overlook significant risks.

- Solutions used by system providers do not produce systems that are immune to attack.

- Staffing issues.

- Existing IT attack tools can be used against SCADA.

- Many control systems use default passwords and default SNMP community strings.

- Policy and law in cyber-space are immature and lag the pace of change.
It’s going to get worse

- Internet growth continues.
- More sensitive applications connected to the Internet.
- Real time constraints – Security technology can impact timing
- Market growth will drive vendors.
- Many IT departments have a poor understanding of process equipment or process networks.
- Lack of security expertise and domain expertise required.
Before it gets better

• Security Architecture for real time operating systems must continue to improve.
  • Security Technical Standards is Key
  • R&D and test bed facilities needed

• CERT like functions to track incidents

• Increase collaboration across the industry.

• Industry must require vendors to develop secure systems.

• Regulators starting to establish rules.
Is the SCADA Cyber threat real?
Successful Attacks With Damage

- **Electric Utility**
  - 17 Intrusions
  - 2 Denial of Service (DOS) Events
  - 3 Loss of Control Events
    - Switchgear controller
    - Boiler Deaerator controls
  - Slammer infected Davis-Besse nuclear plant in Oak Harbor, Ohio, in 2003. Plant’s process computer failed requiring over six hours to recovery. Control-system traffic was also blocked on five other utilities
  - Cyber breach in 1994 of the Salt River Project.
Successful Attacks With Damage

- **Wastewater Utility – Australia, March 2000**
  - Wireless hack by disgruntled ex-SCADA supplier employee
  - Release of millions of liters of sewage

- **Gas Company - Moscow, Gazprom, April 1999**
  - Hackers compromises World’s largest natural gas company
  - Lost control of gas flow

- **Oil Company – Anonymous, 2002**
  - Network hack by disgruntled ex-employee
  - Issued instruction to remote systems
  - Deleted sensitive files related to process control flow
Conclusions

- The Threat is real

- SCADA systems can be impacted by Hackers and cyber accidents
Auditing SCADA
How to Audit SCADA?

- Use security controls set by internal policies, NERC, NIST, and ISA

- Follow generally accepted auditing procedures, ISACA, AICPA, IIA

- Seek assistance from engineering staff or contract SCADA auditor
Audit Method

- Four Recommend Steps include:
  - System Characterization
  - Controls Review (Audit)
  - Risk Management
  - Monitoring
Audit Methods

- System Characterization
  - Gather SCADA system documentation
    - System Description
    - SCADA Engineering Drawing
    - Network Diagrams
    - Roles and Responsibilities
    - Equipment Inventory
Audit Methods

- Controls Review
  - Conduct Testing of Controls (Audit)
    - Management Controls
      • Security Awareness Training
      • Background Checks
      • Policy and Management Authorization
    - Operational Controls
      • Access Control
      • Redundancy and Continuity
      • Management Authorization
      • Physical Security
    - Technical Controls
      • System Configuration
      • Network Security
      • Logical security
Audit Methods

- Risk Management
  
  - Use Risk Assessment Techniques on Review Controls
    - Assess reviewed controls for risk
    - Rate risk of control deficiency to system (Risk = Threat x Vulnerability X Impact)
    - Create Remediation Plan in cooperation with engineering unit
    - Implement and monitor Remediation Plan
Audit Methods

- Monitoring
  - Develop SCADA Review Program
  - Periodic Review
    - Create annual and long term SCADA audit plans
    - Assess per regulatory requirements
    - Assess per best practices

- Change in System or Environment
  - Process to track changes in SCADA Environment
  - Impact Analysis to change in security posture
Does Your Organization Have SCADA?

- Are Security Controls in-place?
- What are the Legal, Regulatory and Corporate requirements to secure SCADA systems?
- Is management involved in the authorization of security controls?
- Are the required skills in-house or do you have to procure?
- Are there sufficient documents and diagrams to understand the system and its interconnections?
- Do employees and contractors have sufficient security screening?
- Are the systems reviewed on a periodic basis to ensure proper security controls are in place?
- Do your systems have sufficient redundancy and continuity?
Questions?
Acronyms

AGC - Automatic Generation Control
DPG - Data Processing Gateway
DCA - Distributed Control System
EMS - Electric Management System
ESISAC – Electricity Sector Information Sharing and Analysis Center
ECN – Electronic Communications Network
DNP – Distributed Network Protocol
DPG – Data Processing Gateway
HMI - Human Machine Interface
IED - Intelligent Electronic Devices
IOC – Intelligent Input/Output Controller
ISA - Instrument Society of America
LAN – Local Area Network
Modbus - Communications Protocol by Modicon
MTU - Master Terminal Unit
NERC – North American Electric Reliability Council
NIST –National Institute of Standards and Technology
PKI – Public Key Infrastructure
PLC – Programmable Logic Controllers
RIG - Remote Intelligent Gateway
RTU – Remote Terminal Unit
SCADA - Supervisory Control And Data Acquisition
SSL – Secure Socket Layer
WAN – Wide Area Network