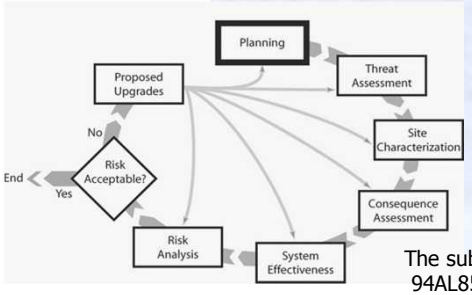
SAND2005-7292C

CONTROL SYSTEM SECURITY

Raymond Parks
Information Operations, Red Teaming, and Assessments Department
Sandia National Laboratories

October 6, 2005



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

SCADA Security

Outline

- Part I: Introduction
- Part II: Security Administration
- Part III: Technical Good Practices
- Part IV: Disaster Recovery
- Part V: Discussion

Part I: Introduction

- Sandia's Center for SCADA Security
- Definitions
- Current Security Vulnerabilities
- Components of Sustainable Security

Where is Sandia?
…distributed across many sites

Albuquerque, New Mexico

Yucca Mountain
Nevada

WIPP, New Mexico

Tonopah Test Range
Nevada

Kauai Test Facility
Hawaii

Livermore,California

Sandia National Laboratories

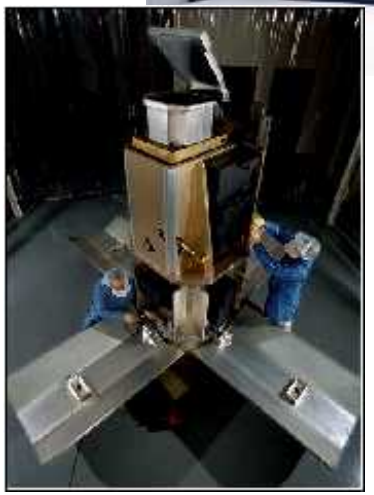
SCADA Security

Sandia has five main lines of business supported by science and engineering

- Nuclear weapons
- Nonproliferation and materials control
- Emerging threats
- Energy and critical infrastructures
- Homeland Security

Lab on a chip

Airborne sensors



Multi-Thermal Imaging Satellite (MTI)

Critical infrastructures

SNL and Government Initiatives in Control System Security

PCCIP Report Completed
October 1997
(SCADA systems identified as vulnerable)

PDD-63 Signed
May 1998

EPA/AWWARF Sponsor Water System SCADA/Physical Assessments and Methodology (RAM-W) Development 2001

DOE OEA Initiates Surveys of Critical Energy SCADA Systems 2002

GAO Reports
GAO-04-140T
GAO-04-354

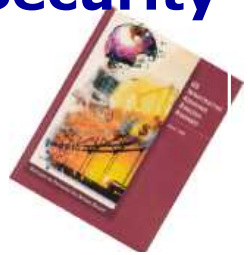
DHS formed 2003
HSPD-7 signed

DHS forms CSSC 2004

DHS form LOGIC 2004

DHS forms PCSF 2005

DOE OEA/NETL Fund National SCADA Test Bed May 2004



IEC Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

IDART Information Design Assurance Red Team

- -1997 Prosperity Games
- -1998 US Infrastructure Assurance Roadmaps
- -1998 DOE designates SNL as US rep to IEC TC57
- -1998 SCADA Surety Research and SCADA test bed initiated
- -1999 Assessment of SPR
- -2000 Assessment of USBR's major dams
- -2000+ Assessment of utilities
- -2000 SCADA Encryption Research
- -2001 Develop RAM-W
- -2002+ VRAP Surveys for DOE/OEA and DHS
- -2002 Assessment Training
- -2003 NISAC Support
- -2004 SNL co-lead of NSTB
- -2004 Support DHS

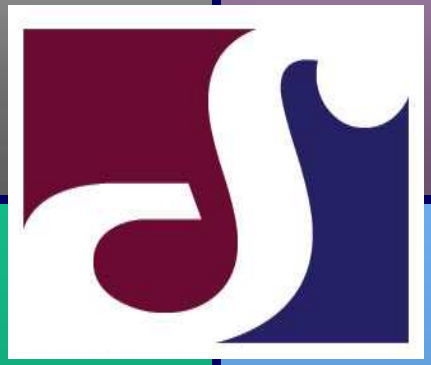
Sandia National Laboratories

SCADA Security

Center for SCADA Security

Assessments and Testing

Standards, Outreach and Training

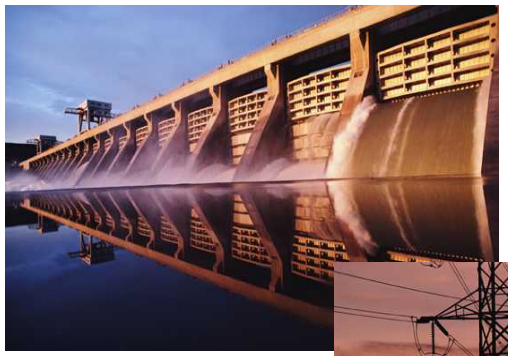
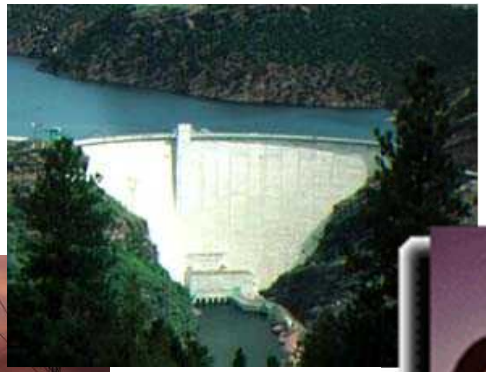


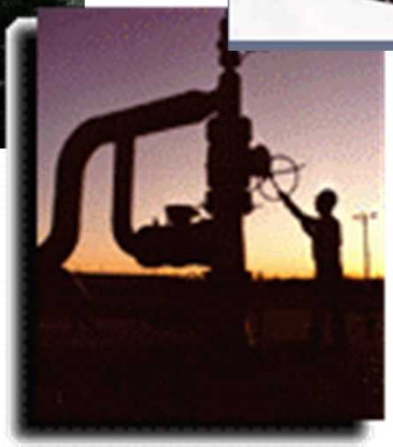
Laboratory and Test Bed Facilities

R&D

SNL's Experience in PCS Assessments

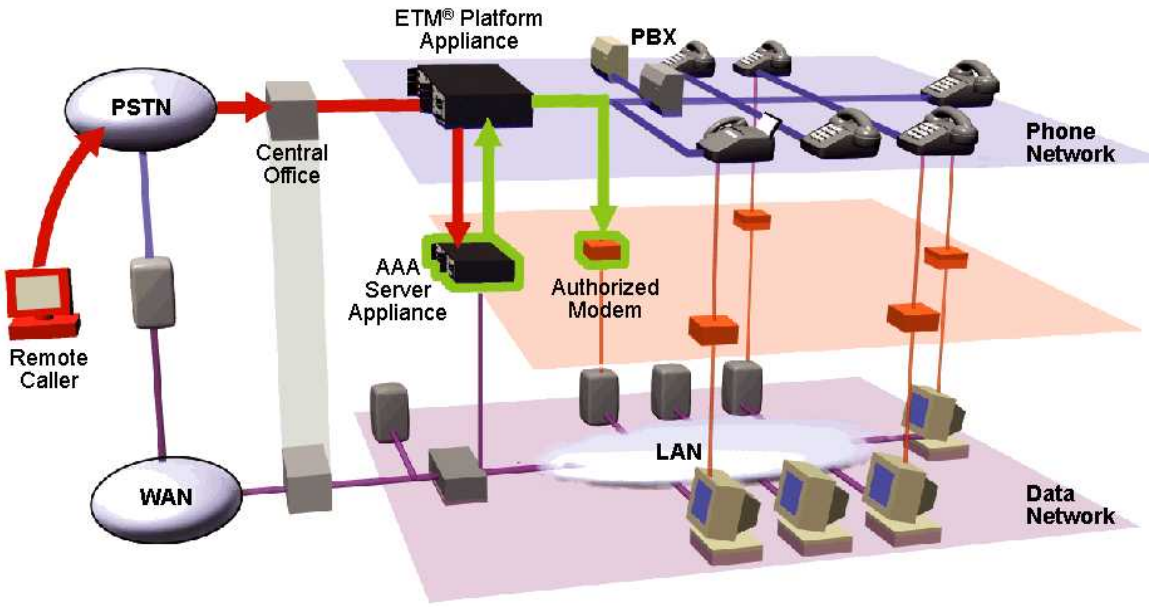
- Electric power generation, transmission, and distribution
- Oil and gas pipelines
- Water treatment and distribution
- Transportation systems
- Refineries

Testing and Evaluation of SCADA Security Technology – One Example

- Dial-up access firewall technology
- Red Team assessment
  - Unprotected
  - Out of the box
  - High security



Sandia National Laboratories

SCADA Security

Supporting Standards and Guideline Development

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

- IEC 60870-6 TASE.2 for Intercontrol center communication.
- IEC 61850 for substation automation and also being considered for DER communication and control.
- IEC 62351 Data and Communication Security

- IEEE Std C37.1-1994 - IEEE standard definition, specification, and analysis of systems used for supervisory control, data acquisition, and automatic control.
- IEEE 1379-2000 – substation IED communication.
- IEEE P1525 – substation automation.
- Communication and Controls subgroup associated with IEEE P1547 DRAFT Standard for Distributed Resources Interconnected with Electric Power Systems.
- IEEE C0TF1 – Committee on substation data security.

- **SP99 Manufacturing and Control System Security.**
- **1164 SCADA Security Best Practices.**

- **AGA12-1 Encryption standard for natural gas SCADA systems.**

Education and Training

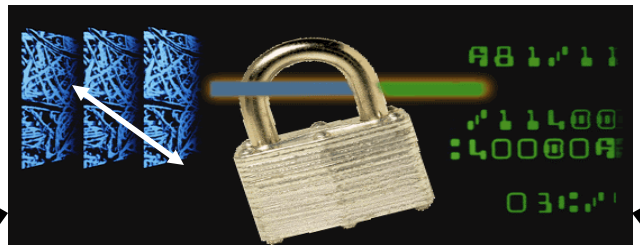
- SCADA Security Assessment Course
  - Broad SCADA application
  - Given to industry and government
  - Identifies areas of potential vulnerability
- SCADA Security Good Practice Course
  - Industry guidelines for SCADA security good practices
  - Includes good practices for policies, procedures, and technology application
- Self-assessment Tool Training

NETL

Sandia National Laboratories

SCADA Security

Cyber Security for Utility Operations



SHORT-TERM GOAL:

- **Demonstrate proof-of-concept devices for key exchange, authentication, and encryption of data in SCADA systems.**

LONG-TERM OBJECTIVE:

- **Bring a cost-effective, high performance, commercialized solution to overall utility critical infrastructure cyber security, including EMS/SCADA and all related business functions.**

APPROACH:

- **Evaluate and update current utility security requirements**
- **Assess and update cyber security system design**
- **Integrate state-of-the-art and best-of-breed products of Sandia, TecSec, and Mykotronx into system design**
- **Demonstrate proof-of-concept security system at utility facilities**
- **Refine commercialization plan for cyber security system**

SPONSORS:

- **DOE Office of Energy Assurance (OEA)**
- **National Energy Technology Laboratory (NETL)**

TEAM:

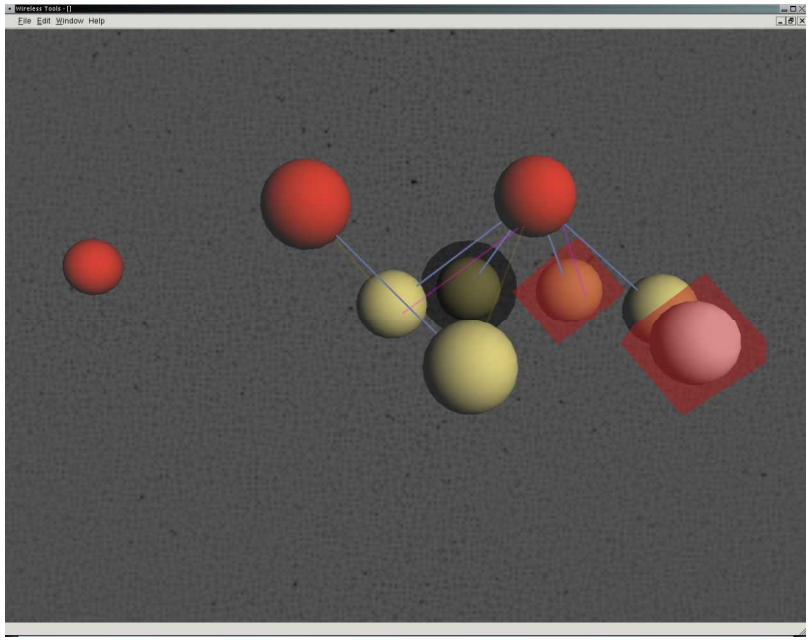
- **OPUS Publishing – Utility industry consultants**
- **TecSec – Maker of the Constructive Key Management (CKM) technology**
- **Mykotronx – Developer of cryptographic hardware**
- **Sandia National Laboratories**

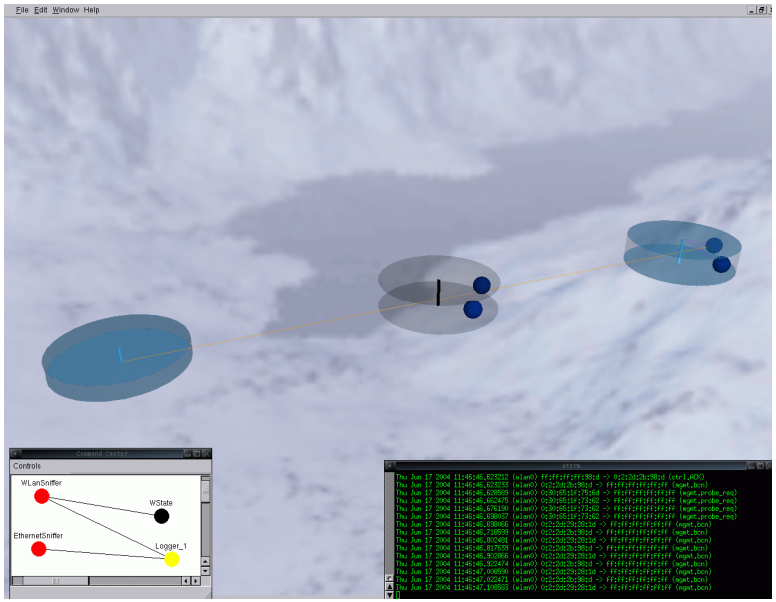
UTILITY PARTNERS:

- **Peoples Energy – Diversified energy company headquartered in Chicago**
- **DTE Energy – Energy and energy technology provider headquartered in Detroit**

Wireless Network Security

Identification of associated and malicious wireless nodes



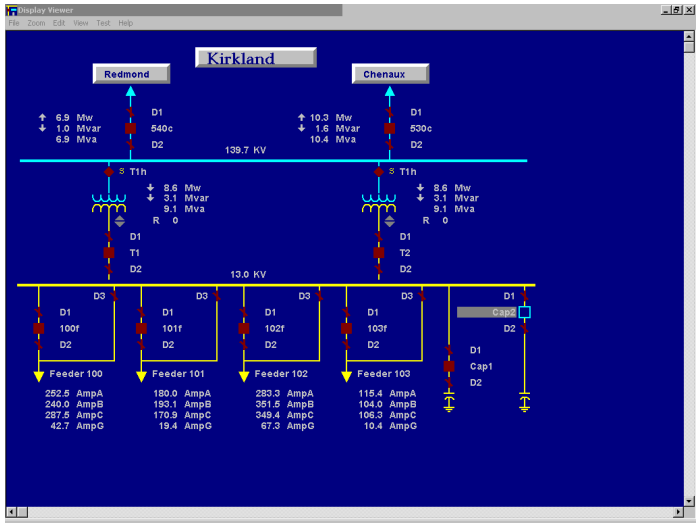


Statistical analysis of anomalous wireless network behavior

Sandia National Laboratories

SCADA Security

Virtual SCADA Environment (VSE)



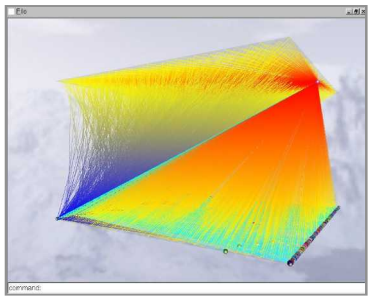
- Supports large scale analysis
- Combines physical and virtual environments
- Network and infrastructure analysis and simulation

Sandia National Laboratories

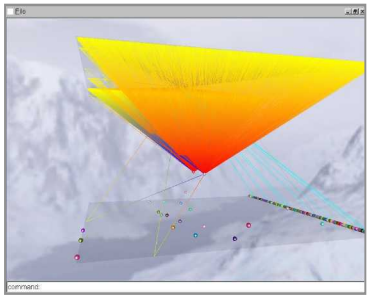
SCADA Security

Network Visualization Tools

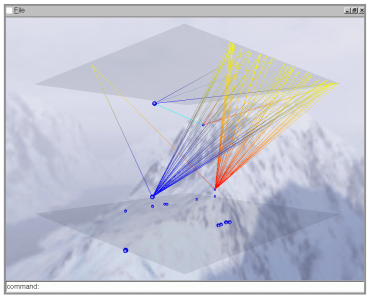
Host-Based Views



Network under DDoS attack



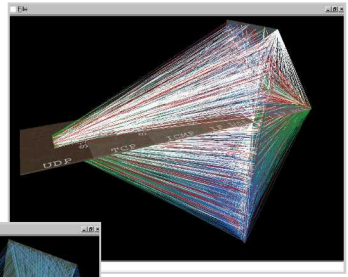
Network being port-scanned by NMap



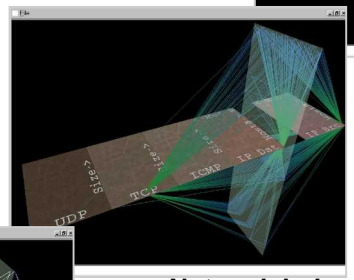
NMap firewall probe of Network

- Development of graphical tools that allow a human analyst to rapidly assess large amounts of real-time data.
- Application of technology to demonstrate cyber security impacts on SCADA systems.

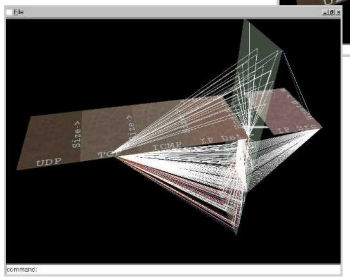
Network-Based Views



Network under DDoS attack



Network being port-scanned by NMap



NMap firewall probe of Network

Sandia National Laboratories

SCADA Security

SCADA Scenario Demonstration System

- Reconfigurable, portable SCADA system
- Comprised of four primary elements
- Using modern Digital Control System (or SCADA) components
- Has multiple uses
  - Security awareness demonstrations & training
  - Red team attack development tool
  - SCADA protocol analysis tool
  - Security component evaluation tool

Other Research

- Combining Cyber and Physical Assessment
  - Questionnaire tool for self-assessment
  - New methodology
- Control Systems Forensics
  - Forensics of PCS software on COTS platforms
  - Forensics of embedded PCS
- Interactions between protocols and firewalls/VPNs
- Correlation algorithms to transform security events into attack knowledge
  - Events from IDS, firewalls, PCS itself
- SCADA Linux Appliance - SLAP

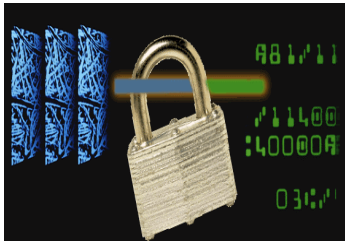
SNL Assets Supporting the CSS

IDART™
Information Design Assurance Red Team

Attack Resource Centers

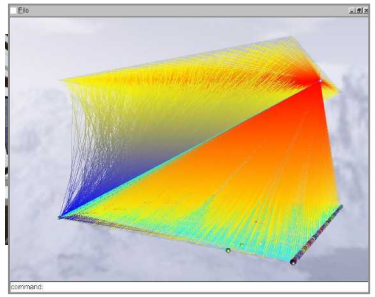
NISAC

Operational Generation & Load Assets



Cryptographic Laboratory

Center for SCADA Security



Center for Cyber Defenders

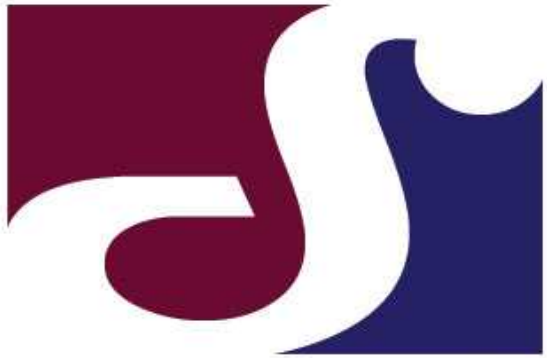
Network Laboratory

AISL
advanced information systems laboratory

Intelligent Infrastructure R&D

Sandia National Laboratories

SCADA Security



The Center for SCADA Security

www.sandia.gov/scada

scada@sandia.gov

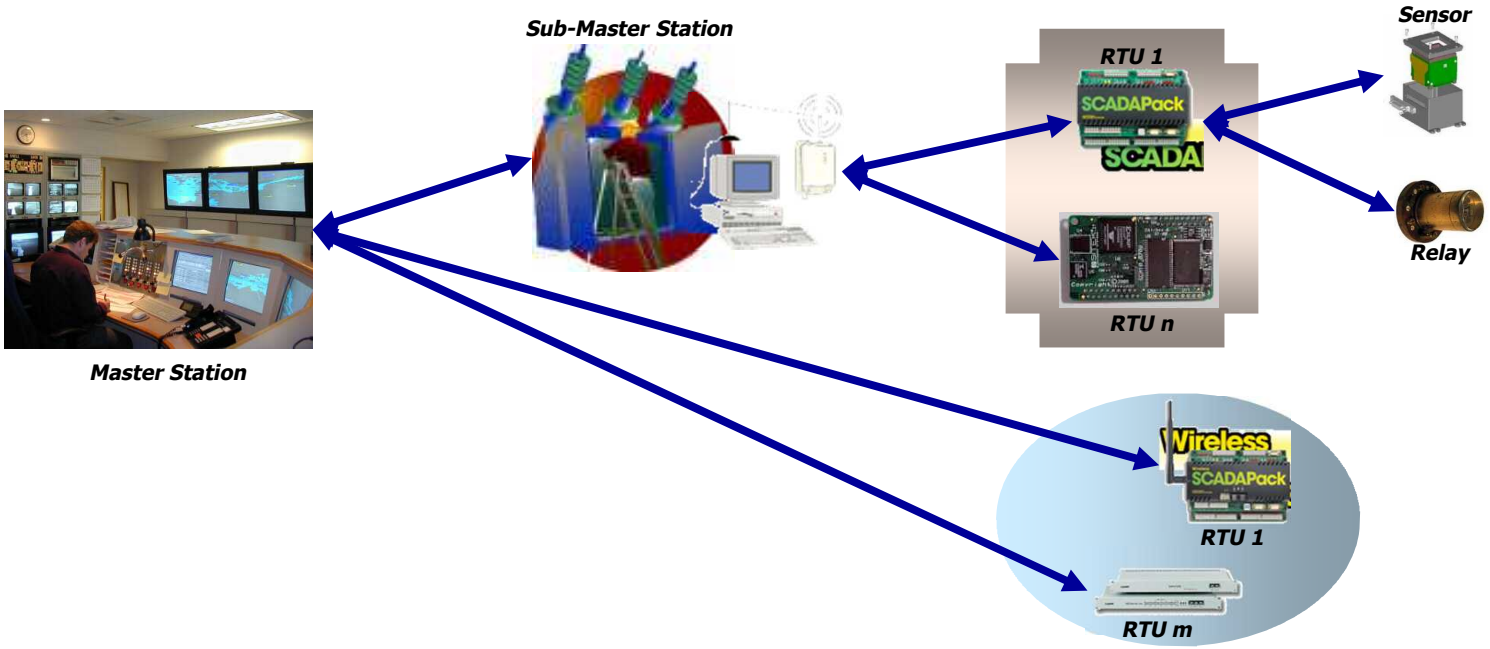
Ray Parks
rcparks@sandia.gov
505-844-4024

Sandia National Laboratories

SCADA Security

Control Systems

Any subsystem that electronically measures state, alters process control parameters, presents / stores / communicates data, or the management thereof

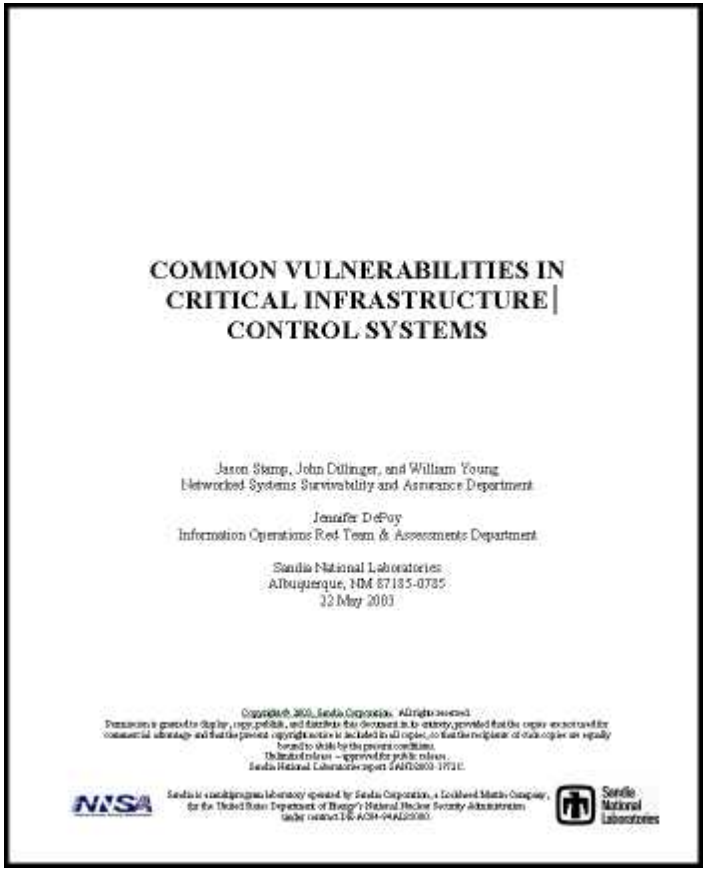


Control Systems in Electric Power

- SCADA
  - Supervisory Control and Data Acquisition
  - (All-encompassing government term for control system)
- EMS
  - Energy Management System
- Protection
  - Relaying
- AGC
  - Automatic Generation Control
- WAP
  - Wide Area Protection
- Etc.

Vulnerabilities Exist

- SCADA equipment, IT equipment upon which SCADA depends, software, processes, policies, communications, etc…
- Common Vulnerabilities in Critical Infrastructure Control Systems, SAND2003-1772C
- More vulnerabilities exist than have been found
- www.sandia.gov/scada



COMMON VULNERABILITIES IN CRITICAL INFRASTRUCTURE CONTROL SYSTEMS

Jason Stamp, John Dillinger, and William Young
Networked Systems Survivability and Assurance Department

Jennifer DePoy
Information Operations Red Team & Assessments Department

Sandia National Laboratories
Albuquerque, NM 87185-0785
22 May 2003

Future PCS Security

- Security administration
- Better security technology
- Third-party assessments

Security Administration

- Security administration is paramount to manage security risks
  - Exploited vulnerabilities are directly related to implementation and operation of a particular SCADA system
  - SCADA use and operations are managed by people whose actions are defined and controlled by the system's security administration
- Unrealistic to expect any PCS operation to be free of vulnerability and immune to threat
  - In the fluid IT environment, changing conditions demand constant vigilance
  - Only through constant evaluation and maintenance can security be sustained
- Effective and sustainable security for PCS depends on effective security management

Security Administration

- Modern PCS must be addressed and managed in a style appropriate for a critical IT system
  - PCS no longer enjoy freedom from concern for security
  - Information Age has introduced malevolent human threat
- Need for dedicated security personnel
  - Ineffective for PCS administrators and managers to also bear the responsibility for security
  - Cutbacks in staff and increasing system complexity in most cases deny adequate attention to security from PCS operations personnel
  - PCS security staff has a heavy training burden to keep abreast of threat and vulnerability developments
  - PCS security administrator must have clear authority to alter running configurations to mitigate vulnerabilities
  - That authority must derive from clear and direct policy

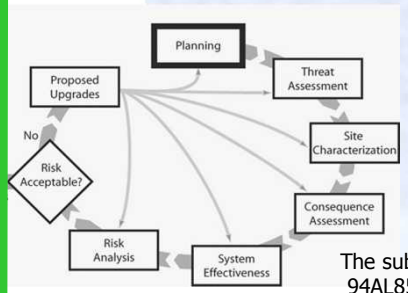
Improved Technology

- Critical to embrace the role of technology to achieve overall security for future SCADA
- Development of secure technology, protocols, and standards will equip SCADA security personnel with necessary tools for secure implementation
- Some advancements may include:
  - Secure protocols
  - Low-cost encryption for serial SCADA
  - Application-layer stateful inspection for SCADA firewalls
  - Accounts and logging for RTUs
  - Control-specific attack correlation

Third Party Assessments

- Internal auditing and assessment of security administration and system implementation are essential
- Regular external evaluations are also critical to catch residual problems caused by organizations being too close to issues or unaware of new tactics and tools
- Contemporary security assessments may not be helpful to organizations with emerging security programs
- For now, an assessment process that focuses primarily on security management and organizational culture while addressing only glaring vulnerabilities in implementation is the best balance for most

Part II: Security Administration



Unlimited release – approved for public release.
Sandia National Laboratories report SAND2005-1001C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

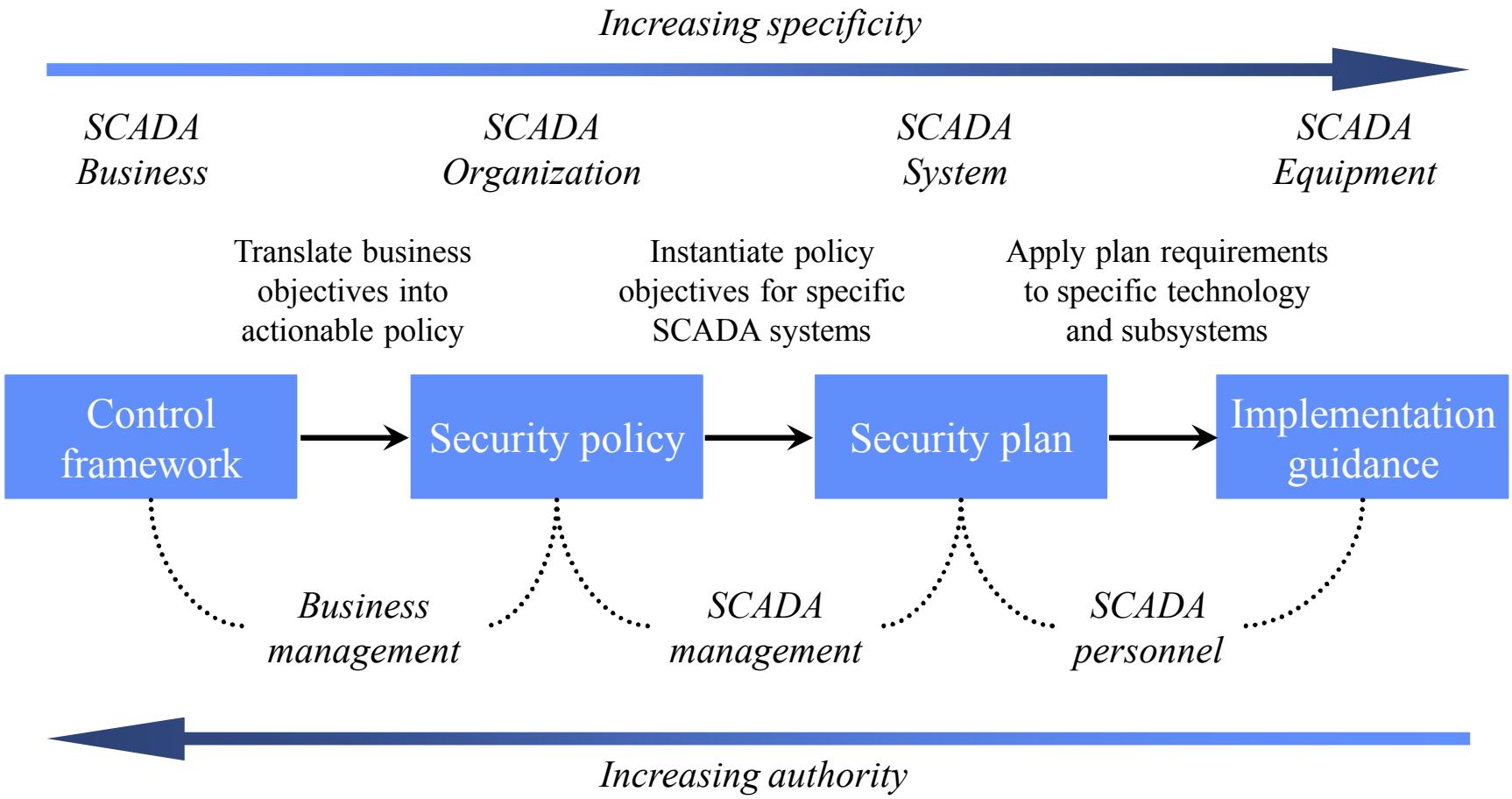
Part II: Security Administration

- Security Policy
- Security Plans
- Implementation Guidance
- Configuration Management
- Auditing and Assessment
- Security Enforcement

Administration For Sustainable Security

- Governance and control framework
  - A starting point for the business administration of the enterprise employing SCADA
  - Security is addressed as part of the company's comprehensive risk management program
  - Coupling the need for security to the organization's business model is the most direct way of evaluating security investment
- Enforcement
  - Security policy
  - Security plans
  - Implementation guidance
  - Configuration management
  - Auditing/assessment
  - Technical security controls
- Security policy is key: it bridges the control framework to enforcement

Sustainable Security



Part II: Security Administration

- ***Security Policy***
- Security Plans
- Implementation Guidance
- Configuration Management
- Auditing and Assessment
- Security Enforcement

Security Policy

Security policy for PCS administration translates the desired security and reliability control objectives for the overall business into enforceable direction and behavior for the staff to ensure secure PCS design, implementation, and operation

- An organization should have one security policy with authority over all PCS systems, connected elements, and personnel
- Unique characteristics of PCS necessitate a complete policy separate from the normal company information policy
- Formulated by the PCS management staff, with input from the business leadership
- Fosters a strong link between the control framework and the policy

What is Policy?

- A formal statement of what will (and will not) be done
- Mandatory rules that will be followed... **not suggestions or guidelines**
- Product and vendor independent

- It does not include system security settings, configuration rules, or computer setup rules

Justification for Separate Control Policy

- Acceptable use of control system should be narrower than IT systems due to:
  - Different mission
  - Different sensitivity of data
  - Different criticality of function
- Control systems have more immediate physical consequences therefore:
  - Interconnections must be better controlled
  - Access and CM more strictly enforced and monitored
- Administration and enforcement is simpler with a separate policy
  - Don't embellish IT... this just gets messy when trying to include all of the caveats for control system
  - Tension between control systems and IT security

Justification for Separate Control Policy

- Smaller, different audience
  - PCS engineers
  - PCS operators
  - Not business administrators, HR, regular employees
- Legislative requirements on control systems are different
  - Currently, security plans, policy, etc are not required, but...
  - With current concerns fueled by incidents like the blackout in the northeast, regulation is coming
  - It's better to have the administrative controls in place before they are required by legislation

Policy Elements

- Definitions for critical organizational elements
- Positions in the control systems security administration
- Data categorization and ownership
- Description of important elements of the control architecture
- Creation and enforcement of the risk management program for control system security
  - Evaluating vulnerabilities and their security controls
  - Security investments
  - Residual risk
  - Review cycle (which contributes to ongoing security through risk reevaluation)

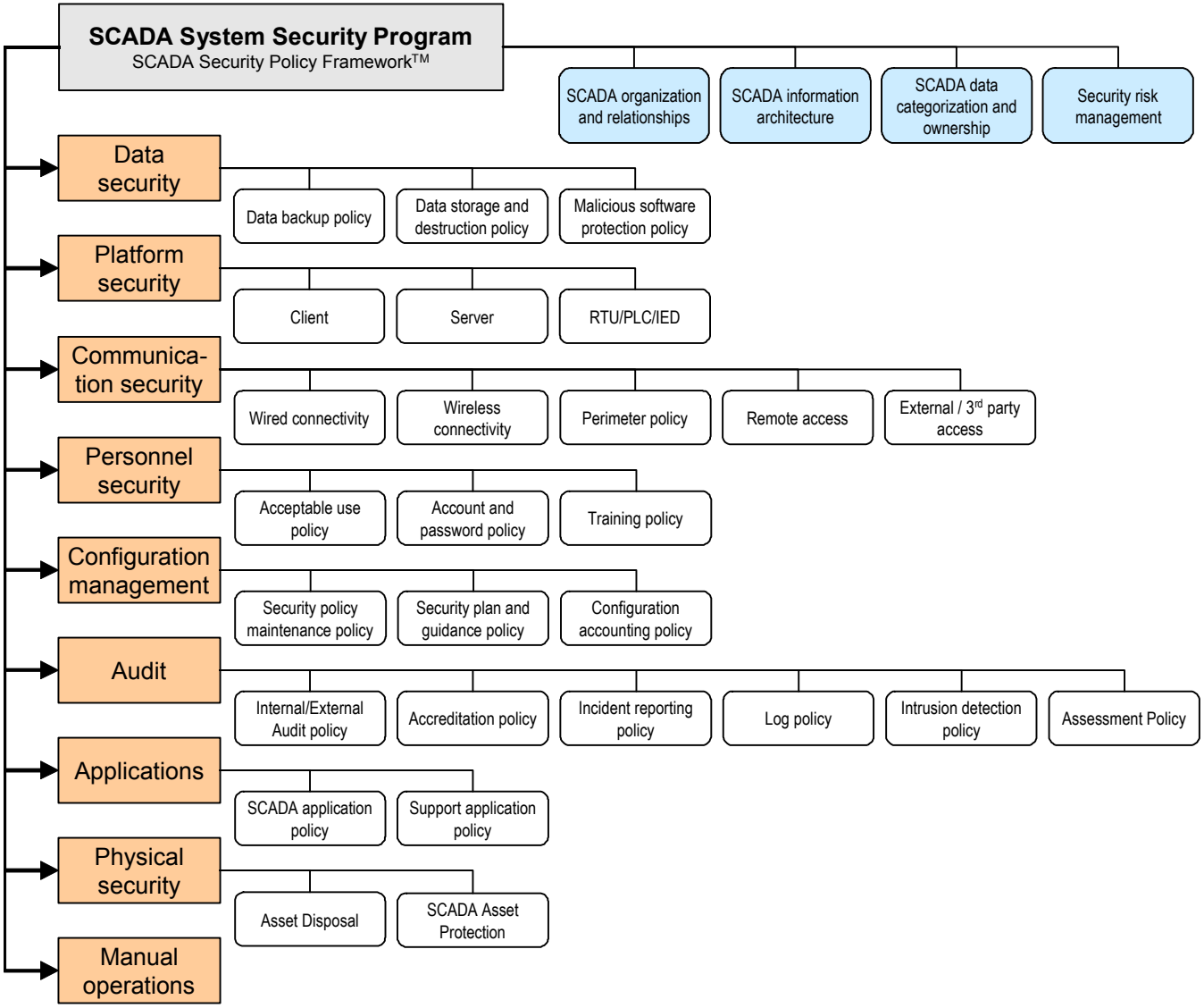
Policy Sections

- Data security - CIP-002, 003
- Platforms - CIP-005
- Networks and communications - CIP-005
- Manual operation (including exercises)
- Personnel - CIP-004
- Security training - CIP-004
  - Essential for understanding policy and requirements, and staff compliance is predicated upon adequate awareness
- Enforcement - CIP-007, CIP-008
  - Security plans for specific systems or subsystems
  - Implementation guidance for specific technologies
  - Configuration management
  - Auditing/assessment

Policy Framework

- Why a framework?
  - Allows for a systematic approach
  - Convenient
  - Hierarchical
  - Easy to sort
- Created for control systems
  - History of assessments
  - Multiple industries
  - Multiple iterations

Policy Framework



Part II: Security Administration

- Security Policy
- ***Security Plans***
- Implementation Guidance
- Configuration Management
- Auditing and Assessment
- Security Enforcement

Security Plans

The PCS security plan enumerates specific security guidelines for systems or groups of systems based on fundamental concepts from the security policy

- Relates policy to reality
- The plan is the core security document for implementation, operation, and maintenance
- Very similar in concept to the NIST definition
- Details the collection of controls and control practices necessary to meet the control objectives of the security policy and control framework
- Considerably more technical than policy
- Elements of the security plan can be garnered from statements of industry practice or good practice

System Identification

- System Name/Title
  - Unique identifying information
- Responsible organization
  - Organization from security policy responsible for the system
- Contact information
  - Sufficient information so that a responsible party can be located.
  - System owner will be designated here

System Identification

- Security Personnel
  - The contact information for the person ultimately responsible for the security of the system
- Operational Status
  - The system (or parts) may be in development or maintenance phases
- Description
  - General description and purpose of the system
  - Software, hardware, and vendor information

System Identification

- Environment
  - Any details about the operating environment that raise security concerns (i.e. connected to the Internet)
  - What hardware or software is used to secure these connections
- Interconnections
  - Include up-to-date network diagrams
- Laws, regulations, and policies
  - This ties back to the *Organization and Relationships* portion of the security policy
- Sensitivity
  - For both information and system
  - Use the data categories defined within the policy

Management Controls

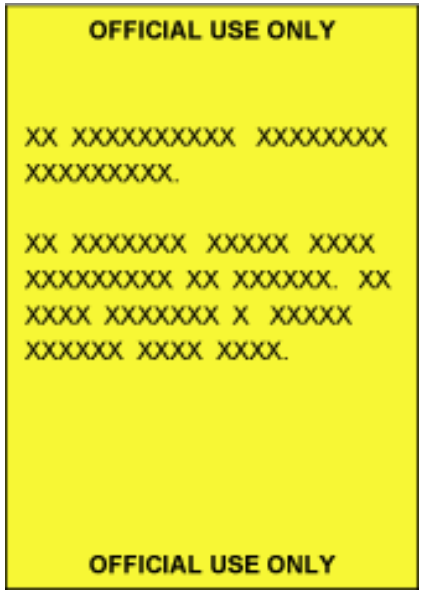
- Assessment and auditing management
  - List known/identified threats and vulnerabilities
  - Include dates, results, planned dates, etc for auditing and assessment
- Assessment and audit results
  - Both internal and external
  - Include dates if changes are necessary
- Rules of Behavior
  - Employees should sign a copy of this and review often
- Accreditation details

Management Controls

- Planning for system lifecycle
  - Describe how security has been implemented for all phases of the system
    - Initiation
    - Development/Acquisition
    - Implementation
    - Operation/Maintenance
    - Disposal
  - Configuration management issues need to be considered for all phases

Operational Controls

- Personnel security
  - Background checks
  - Least privilege/need-to-know
  - Computer room access
  - Termination procedures
- Physical & environmental controls
  - Physical access
  - Emergency preparedness
- Data protection
  - Audit trails, marking, transportation, etc.



Part II: Security Administration

Sandia National Laboratories

SCADA Security

Operational Controls

- Contingency Plans
  - Backup & recovery
  - Disaster recovery
  - Manual Operations Plan
- Maintenance Controls
  - Configuration management
- Access controls
  - Parts of this will be covered in rules of behavior and technical controls sections

Operational Controls

- Data integrity and validation controls
- Documentation inventory
  - Vendor documents
  - Administrative documents (policy, procedures, etc)
- Security training
- Incident response capability and handling procedures

Technical Controls

- Identification/authentication
  - Passwords, smartcards, etc.
- Logical access controls
  - Who or what can have access to specific system resources
  - Remote access controls
  - Screen saver locks and banner requirements will also be included here
- Audit trails / logs
  - What must be logged by what devices
  - Who has access to the logs
  - Review and retention cycle

Part II: Security Administration

- Security Policy
- Security Plans
- ***Implementation Guidance***
- Configuration Management
- Auditing and Assessment
- Security Enforcement

Implementation Guidance

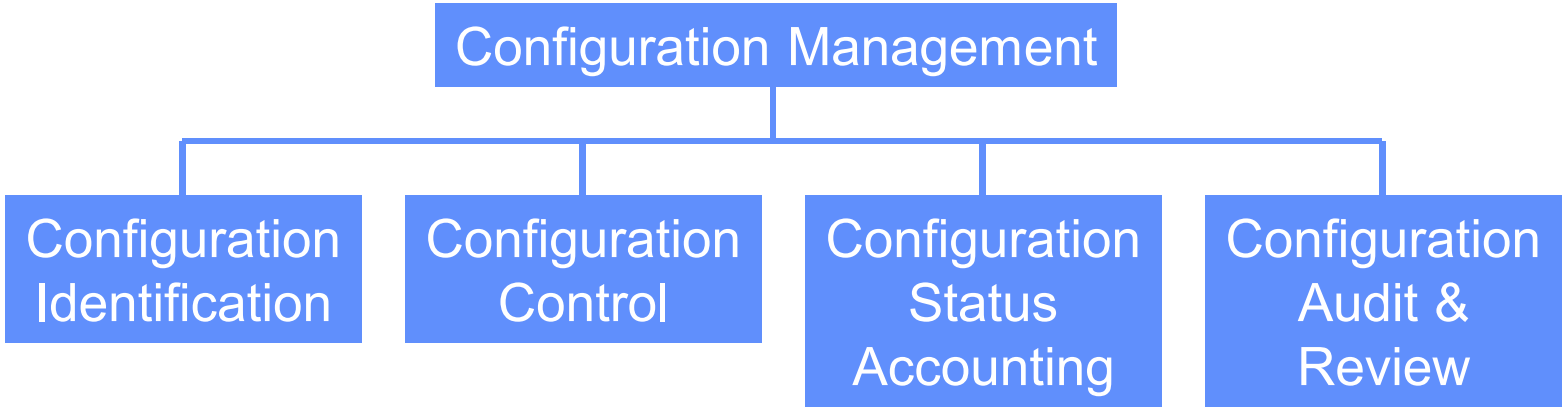
Implementation guidance enforces the security plan and policy for the implementation of specific technologies

- A compilation of directives for the configuration, installation, and maintenance of equipment or software
- Almost entirely technical
  - Example: an implementation guide for the application of password checking software on some particular computing platform
  - The need for the software and its configuration are necessary to meet the requirements of the security plan, which in turn satisfy the demands of the PCS security policy, derived from the control framework based on the business objectives of the company
- Other implementation guides
  - Network cabling
  - Ethernet switches
  - PCS applications
  - Operating systems
  - Computing platforms, etc.
- Adherence to implementation guidance and the security plan is tabulated in the system's configuration management

Part II: Security Administration

- Security Policy
- Security Plans
- Implementation Guidance
- ***Configuration Management***
- Auditing and Assessment
- Security Enforcement

Definition



"Configuration Management is the process of identifying and defining the items in the system, controlling the change of these items throughout their lifecycle, recording and reporting the status of items and change requests, and verifying the completeness and correctness of items."

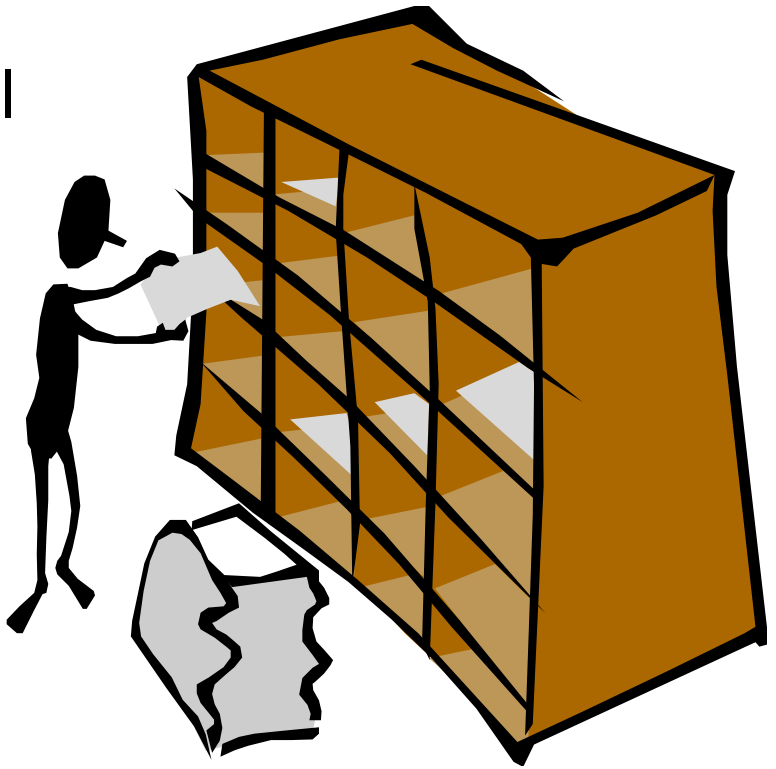
[IEEE Std 729-1983 updated as IEEE Std 610.12-1990]

Benefits of Configuration Management

- Configuration management trades a one-time upfront cost and a little operational overhead for…
- Money saved by avoiding unnecessary improvements and upgrades
- Time and money saved by avoiding complications during necessary improvements
- Time and money saved in maintenance
  - Without configuration management:
    - A simple disk failure turns into a system-wide upgrade
    - A one hour job turns into a week-long effort
    - A short control system downtime becomes loss of service
- Configuration management is a tool
- Enables change and operational crisis management

Configuration Identification

- Select configuration items for a system and recording their functional and physical characteristics
- Uniquely identify configuration items
- Establish standard, reproducible characteristics for configuration items
- Collect into baseline systems



Asset Inventory

- Any configuration management program must start with a complete inventory of the equipment, software, hardware, etc in the system
- All relevant information must be recorded: software versions/patch level, hardware model number, OS level, firewall rules, router ACLs, etc.

Item Identifiers

- All configuration items must be recorded and assigned a **unique** identifier to assist in tracking
- Unique identifiers can be
  - A unique inventory number
  - A combination of identifying information
    - Serial number + date of purchase + ?
- This will assist all members of the team when it comes time to patch. Unique identifiers will allow the team to track which machines have been patched/upgraded.

Access Control

- You need to keep track of the access control environment – both networks and platforms
- Router ACLs, firewall rules, and user password files are important configuration items
  - Remember to **protect** this information - it is invaluable to an adversary
- Configuration management will help you keep track of who made changes, when, and why

Baselines

- Baselines will be a secure configuration that has been rigorously tested by the PCS engineers
- Baselines can be used in disaster recovery or for new equipment added to the system
- Develop the baseline configuration once configuration identification is complete

Common Operating Environment

- Developing a COE for all equipment is a necessary evil
- This will establish a stable starting point for all new machines introduced into the system
- PCS Security Administrators can remove any unnecessary services, applications, etc at this time
- The COE is the software environment built using the implementation guide
- Ideally, the COE can be installed with a simple process on new or old systems
  - Disk imaging programs such as Ghost
  - Install scripts such as Kickstart
  - Phased implementation: OS - Application - Configs

System Changes

- Changes to operational systems come in two flavors
  - Functional improvement
  - Maintenance
- Functional improvement is usually incremental and limited in scope
  - Examples: adding new PLCs, changing network rules, changing device safety settings
  - Configuration management can help understand the consequences and improve the process

Maintenance

- Maintenance – The recurrent, periodic, or scheduled work necessary to repair, prevent damage, or sustain existing components of an information or control system
- This is the most likely use of configuration management in an operational system
- The next few slides will go into more detail about the maintenance process

Requesting Change

- Who can request change?
  - Operators, PCS engineers, business managers, security managers
- Tracking requested changes
  - Record and assign identification to each change request
  - Avoid losing track of changes which makes configuration control impossible
  - Prevent losing important changes that could drop through the cracks

Evaluating Change

- Changes aren't always feasible
- Even when changes can be made, often they can't all be made at the same time
- Prioritizing, planning, and organizing work is easier if changes are evaluated
- One method - the person responsible for the affected component performs a change request analysis
  - Estimate feasibility
  - Estimate cost of making the change
  - Estimate effects on other parts of the system
  - Configuration Control Board (CCB) approves and prioritizes based on the analysis
  - The CCB doesn't have to be formal

Developing and Testing Change

- Once a change is approved, engineers can develop the change
- Using configuration management, they can start with the current status of the system
- As they develop the change, they can determine what must be released to the operational system
- Testing, either by the developers or (better yet) by a separate testing group ensures the proposed release will work

Releasing the Change

- The CCB looks at the results of development and testing and decides whether or not to release the change
  - Some type of reporting is necessary - at least verbal reports
  - All involved have to remember that changes have pros and cons - make sure the pros beat the cons
- Developers then release the change into the operational system and notify the requester
  - This is important to close the cycle

Configuration Status Accounting

- If you have done configuration identification, recorded that information, and have a change control process then you have everything necessary for Configuration Status Accounting (CSA)
- This part of configuration management is what saves money and time
  - Being able to find out original configurations
  - Knowing your system state as you analyze changes

Patching Cycle

- Patching software is a major cause of change requests
- Software patches are a frequent headache for PCS system engineers
  - PCS applications' release cycle is often much longer than platform patch cycles
  - PCS applications tend to be sensitive to underlying platform changes
- In a perfect world, patches would be unnecessary; in our world, it is an important part of system maintenance
  - Anyone familiar with modern operating systems knows that patches occur with regular frequency
  - These patches are released to solve a number of bugs, security holes, or other software problems
- PCS applications are becoming multipurpose and the code-base is larger. As a result, patching will become even more critical in the future.

Patching Cycle

- How do you know when you need to patch your software?
- Mailing lists are a great resource for keeping up to date
  - Vendor mailing lists have the highest value
  - Security mailing lists are less effective, requiring more time to sift through the irrelevancies
- These lists will often be the first to issue information on patches or updates in software or hardware
- Maintenance contracts with vendors can also help
  - Some vendors will give early warning to those with active maintenance contracts
  - Also, some vendors will only release patches to clients who have maintenance contracts

Applying Patches

- What if this breaks my system?
  - It is possible that a patch will have a bug
  - Will break your existing system
  - Will turn on features or services you don't want
  - Possibly, just not work
- Installing the latest greatest patch without testing is a recipe for disaster...
- You need to make an informed decision - What is the impact of a bad patch on your system versus not patching?
- If the patch brings down every computer you own, it is probably much more costly to install the patch!
- Which all brings us to...

Test Labs

- So how can you be sure that the patch issued 5 minutes ago will work for YOUR stuff...
- You need to test... and test with your environment, not an ideal network that does not adequately represent your system

What Goes in the Test Lab

- Ideally – an exact replica of your entire system is best
- But in reality:
  - Workstations and servers for every OS that you use
  - A sample of your network equipment (1 router, 1 switch, 1 firewall, ...)
  - One of each type PLC, RTU, sensor, etc.
  - Some system data
    - An old capture of sensor data works well
    - Data must be similar to what you collect/use/process on a day to day basis
  - All of these should be configured to be an accurate representation of your system

Part II: Security Administration

- Security Policy
- Security Plans
- Implementation Guidance
- Configuration Management
- ***Auditing and Assessment***
- Security Enforcement

Definitions

- Audit
  - The function of measuring something against a standard
  - Auditing enforces configuration management, security plans, and implementation guidance
- Assessment
  - More arbitrary and subjective: how well do the policies/implementations secure the system
  - Overall, assessment (internal and external) enforces the entire chain of security administration

Auditing vs. Assessment

- Audit
  - Works with standards and good practices
  - Checklists to determine if you do what you say you do
  - Done to you
- Assessment
  - Works with experts in the field and the implementation staff to find vulnerabilities
  - Tries to break the security on the system
  - Done with you

In traditional IT, either of the two may include penetration testing and vulnerability scans. This is strongly discouraged on PCS systems.

Tools

- Search your old labs and storerooms - track down your old-timers
  - Legacy systems
  - Serial (RS-232, RS-488), odd settings
  - Old, slooooow modems
  - Old software (zmodem, kermit, VT100 emulation)
- Specialized equipment
  - Custom interface cards
  - Non-standard cables
  - Microwave and packet radio
  - Specialized protocols

Tools II

- Active tools can be dangerous
  - Why do you need to use an active tool?
  - Can you get that information some other way?
- Real world examples
  - Robot arm
  - Wafer Fab
  - Gas utility
- Data mining tool for network topology discovery
  - We use ANTFARM
    - Accepts data from many sources
    - Models network topology
    - Limit data collection to passive methods

Methods

Activity	Usual Methods	CS Preferred Methods
Identification of hosts, nodes, and networks	**Ping sweep (e.g. nmap)**	**1. Examine CAM tables of switches** **2. Examine router configs or route tables** **3. Physical verification (chasing wires)** **4. Passive sniffing or IDS (snort) on network**

Methods II

Activity	Usual Methods	CS Preferred Methods
Identification of services	**Port scan (e.g. nmap)**	**1. Local port verification (e.g. netstat)** **2. Port scan of a duplicate development or test system**

Methods III

Activity	Usual Methods	CS Preferred Methods
Identification of vulnerabilities within a service	**Vulnerability Scan (e.g. nessus, ISS, etc.)**	1. **Local banner grabbing with version lookup in CVE.** 2. **Scan of duplicate development or test system**

Protect

- The information in an audit/assessment report would be highly valuable to any attacker
  - It identifies the weaknesses and existing controls protecting your system
- These results should be protected at a high level
- Before beginning an external audit/assessment, determine what the external company will do with the results
  - Is this an acceptable risk for your system

Read

- There have been instances where an assessment/audit is performed and the *interested parties* do not have the time or inclination to read the results... Why bother?
- There are other cases where a 200 page penetration/vulnerability test has been delivered... again why bother?
- A good assessment/audit will produce a concise report that must be read and acted upon

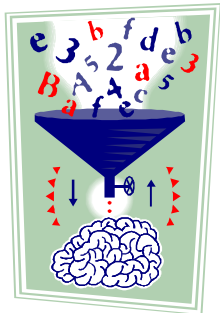
Use

- An assessment is a waste of time, resources, and money if the findings are not used
- A detailed report of what the assessment team found will assist the organization
  - Problems should be addressed in order of criticality
  - Fixes or mitigation strategies must be determined and implementation teams and deadlines assigned
  - After the fixes have (presumably) been completed, a follow-up assessment should be performed

Logging

- Ideally, logs should be recorded for any device/application that has the potential to be misused
- Reality
  - Not all devices/applications have logging capability
  - Logging DOES impact system performance
- Logging must be tailored to ensure that operational jobs are still performed adequately
  - This may require some tweaking and time to get the right balance between logging and operations

Using Logs



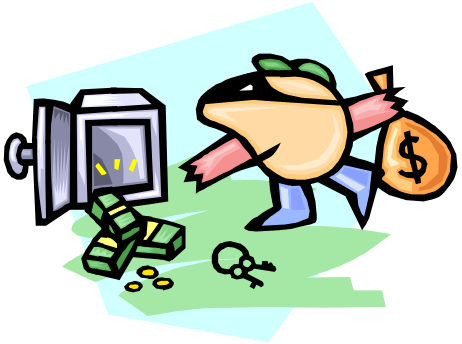
- Once you have all these log files sitting around, what do you do?
- Logs can generate massive amounts of data to sort through
  - Logs need to be reviewed for evidence of malicious or incorrect behavior – this can be a full time job!
  - There are tools that can assist in this process
- If you don't look at the logs, you are wasting resources by collecting them

Concerns

- Where to store the logs
- How long to store the data
- Who will review the data
  - How often will this be done
- What is the classification for log data
  - This affects storage, review, and destruction procedures

Incidents

- You've collected the log data, reviewed it, and you see evidence of a break-in. What now?
  - Immediate Response
  - Preserve & backup
  - Notify
  - Lock down
  - Investigate



Immediate Response

- Follow your response plan
  - Develop the response plan in advance
  - Considerations -
    - You might make it worse (cut off users)
    - You may destroy evidence
    - You need to preserve functionality
  - Options -
    - Wait
    - Pull the plug - disconnect PCS from outside
    - Isolate system

Preserve/Backup

- Both the logs and an image of any affected machines should be copied for analysis
  - This will give you time to investigate later plus more stuff for prosecution
- Try to get the copies on write-once media so there is no doubt about their integrity
  - This can assist in prosecution
- There are several tools available to assist in this process*:
  - dd
  - Commercial - Ghost, Encase, FTK, etc.

* *Independent Review of Common Forensic Imaging Tools*, Mark Scott, August 2003.

Notify

- Do not head out on your own vigilante style
- Have procedures of who to contact and when
  - System admins
  - Security people
  - Law enforcement
  - Users (maybe)

Lock Down

- Secure the affected system
  - This may require severing network connections
  - This may require wiping the system and reinstalling from the baseline (see configuration management)
- Use the backup system in the interim

Investigate

- Now, take the time to fully investigate the logs and images of the systems

- This process will ensure that users suffer a minimal downtime and evidence is retained for possible prosecution. It will also give investigators sufficient time to properly investigate the incident.

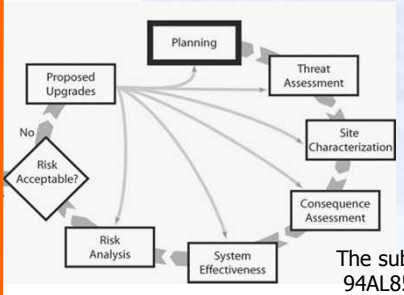
Part II: Security Administration

- Security Policy
- Security Plans
- Implementation Guidance
- Configuration Management
- Auditing and Assessment
- ***Security Enforcement***

The Enforcement Cycle For PCS Administration

- The IT control framework enforces the business direction of the company
- The PCS security policy enforces the IT control framework
- Security plans and implementation guidance enforce the security policy
- Configuration management enforces the security plan and implementation guidance
- Auditing enforces configuration management, security plans, and implementation guidance
- Overall, assessment (internal and external) enforces the entire chain of security administration

Part III: Technical Good Practices



Unlimited release – approved for public release.
Sandia National Laboratories report SAND2005-1001C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

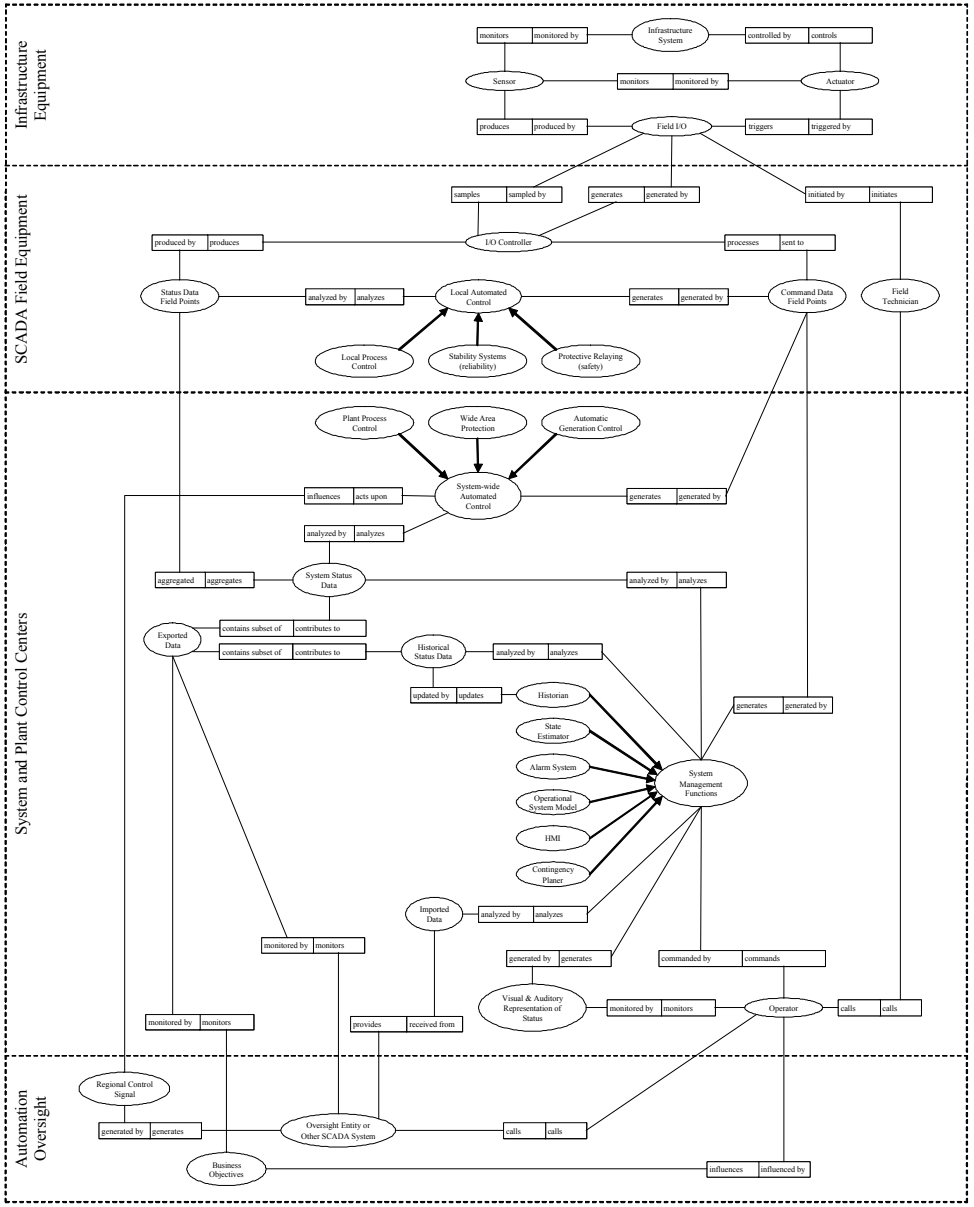
Sandia National Laboratories

SCADA Security

Technical Good Practices

- Four categories:
  - Data Security
  - Architecture and Design
  - Platforms
  - Networks and Communication
- Each section covers:
  - Introduction
  - Suggestions

Control Reference Model



- Describe data and functions
- Map these to locations and equipment
- Develop general good practices for security

Part III: Technical Good Practices

Sandia National Laboratories

SCADA Security

Technical Good Practices

- ***Data Security***
- Architecture and Design
- Platforms
- Networks and Communications

Data Security: Introduction

- Rationale for data classification
  - Is payroll information more important than a FYI memo?
  - Is an archived gate signal more important than a valve control signal?
- Determination of data sensitivity is based upon mission
- Evaluation of CIA (Confidentiality, Integrity, Availability) requirements for data

Data Security Categories

- Live/Real-time
- Safety/mission critical
- Other operational status and control
- Administrative
- ACLs
- Authentication information
- Other configuration settings
- Input/output database (points)
- Archived
- Trending data
- Warranty and maintenance data
- Accounting information

Data Security Sensitivity

- Proposals refer to confidentiality
- Integrity is necessary for all classes
- Consider availability
- Includes need-to-know/use
- Highest level of protection listed first

Data Security Sensitivity

Private

- Shared with a small group within the work area
- Specific to a function or task
- Examples
  - Security controls information
  - Safety critical commands or measurements
  - Operator control directives
  - Administrative passwords on control systems
  - Points database

Restricted

- Shared within a group (perhaps including customers or suppliers)
- Specific to certain functions or areas
- Examples
  - Contaminate levels
  - Equipment status
  - Performance information
  - Accounting usage information

Public

- Shared with anyone
- General in nature
- Examples
  - Reservoir level
  - Gross plant output
  - Regulatory compliance

Exceptions and Caveats

- Regulated industries may have specific classifications
- There may also be legal requirements for data protection

Technical Good Practices

- Data Security
- ***Architecture and Design***
- Platforms
- Networks and Communications

Architecture and Design: Introduction

- Architectures are specific to mission
  - Secure and reliable storage, processing, and transmission of system data
- Designed to implement some consistent security policy
- The system security plan is related to its architecture
- Implements enclaves consistent with data sensitivity
  - An enclave is the "container" for data elements of like security characteristics
  - Enclaves can be implemented as perimeters
  - An enclave can be implemented as access controls on storage media or platforms

Architecture and Design: Suggestions

- Mature policy and governance essential
- Control and data hierarchy
  - Eliminate global access/privilege requirements
  - Use principle of least privilege
  - Access level commensurate to level of data sensitivity
- Interconnections
  - Control direct connections behind the perimeter
  - Never violate security enclaves
- Principle of single function
- Evolution
  - Risk assessment when adding new functions

Architecture and Design: Suggestions

- Heterogeneity
  - Diverse implementations improve survivability
- Situational and operational security awareness
  - Operators/personnel aware of security issues
  - Training
- Redundancy
  - Continuity of operations
  - Backups for critical data
  - Backups for critical communications
  - Backup platforms for critical nodes

Technical Good Practices

- Data Security
- Architecture and Design
- ***Platforms***
- Networks and Communications

Platforms: Introduction

- What is a platform?
  - A platform is a collection of hardware and software that can run a program
- Platform software includes its OS and applications
- Examples of platforms:
  - Routers
  - IEDs / PLCs / RTUs
  - Servers and clients

How Exploits Work

- Attack opportunities
  - Buffer overflows
  - Input validation errors
  - Social engineering
  - Leverage existing bugs
- Types of malware
  - Trojans
  - Viruses
  - Spyware
  - Worms

- Results:
  - Additional access
  - Corruption or compromise
  - Privilege escalation
  - System failure / denial of service
  - Command injection

Platforms: Suggestions

- Authorization
  - Restrict execution privileges for programs
  - Access controls
    - Acceptable passwords
    - Cryptographically secure password storage
    - Secure remote authorization
- Necessary/unnecessary services
  - DHCP, SSH, Telnet, FTP, TFTP, BOOTP, SMTP, SNMP, HTTP, etc.
  - Disallow or secure remote management
  - Carefully consider file sharing
- Logging
  - Remote or local
  - Review logs for anomalies or attacks
  - Appropriate retention periods
  - Meets standards and requirements

Platforms: Suggestions

- Host-based Intrusion Detection (HIDS)
  - Rootkit detectors
  - File integrity checkers (run from read-only media)
  - Anomaly detection
    - Rule-based
    - Learning
    - Combination
- Malcode detection
  - Virus detection
  - Spyware detection
- Platform firewalls
  - Software
  - Hardware
- Issues - performance, interoperability, management

Platforms: Suggestions

- Physical security
  - USB ports, pen drives, guns/guards/gates
  - Physical access by an adversary means a compromise was possibly (if not likely)
- Patch management
- Backups
  - Incident response
  - Disaster recovery
  - Attack recovery/law enforcement imaging
- Resources
  - SANS guides
  - NSA guides
  - NIST guides
  - GOVCERT
  - Etc.

Platforms: Suggestions

- Limitations of security for RTU/PLC/IED/legacy equipment:
  - Not developed with security in mind
  - No user accounts
  - No logging
  - Typically, no encryption services
  - Usually a single privilege level (maybe two)
  - Passwords from small set of characters
- Workarounds
  - Wrappers for applications
  - Terminal servers for access
  - Change passwords often
  - Increase physical security (cameras, doors, locks, guards, guns, etc…)

Technical Good Practices

- Data Security
- Architecture and Design
- Platforms
- ***Networks and Communications***

SCADA Reliance on Networks

- System operations
  - Logical interconnection of SCADA elements for status/control telemetry
  - Transmission of performance data
  - Remote operations
    - Limited offsite operations and maintenance
    - Extend monitoring and control to corporate offices
- System administration and maintenance
  - Configuration management
  - Patches, updates, and upgrades
  - Remote contractor maintenance access
- Business integration
  - Provide network applications (e.g., email) to operational environment
  - Integrate business activities with operations (e.g., forecasting and automated billing)
- Networks must maintain data attributes (confidentiality, integrity, availability, authentication, non-repudiation)

Protocols

- Legacy SCADA Protocols
  - ASCII, byte or bit based
  - Run over serial links
  - Oldest "protocols" are tones or current loops
  - No security services (hashes, encryption, etc.)
  - Hundreds of varieties because of legacy, manufacturer-specific stovepipe SCADA installations
- Modern SCADA Protocols
  - May run over serial, but increasingly support IP stacks
  - Often are object-oriented
  - Based on open or de facto standards
  - Still largely absent of intrinsic data security services
  - Greater functionality than legacy protocols

Wireless Connectivity

- Licensed band wireless
  - Microwave
  - Satellite
- ISM unlicensed band wireless
  - 802.11(a, b, g, etc…)
    - WEP, WPA, 802.1x (EAP, LEAP)
  - Packet radios
- Other wireless techniques
  - Frequency hopping
  - Spread spectrum
- None of these are secure by themselves
- Treat all wireless as untrusted comm path

Perimeters

- Electronic Security Perimeter
  - Based upon trust and data sensitivity
  - Defines perimeters and boundary points of systems/subsystems
  - Enforcement by router, firewall, application proxies, other filters
    - Address, service, content
    - Stateful, stateless
- Need-to-know data flows may cross boundaries
- Serial communications
  - Bulk encryptor plus physical security at endpoint
  - Wrap communication into a packet
  - Application proxy testing

Remote Access

- Evaluate the business case first
- Options
  - VPN
  - Dial-up, call-back
- Activities
  - Remote data
  - Platform management
  - Application usage

- Protection mechanisms
  - Positive ID for authorization
  - Authenticate user/device
  - Token cards/one-time passwords
  - Encrypt traffic
  - Log all usage
  - Use access timeouts & lockouts, activity timeouts, time periods
  - Minimum privilege
  - Deactivate when unnecessary

External/3rd Party Access

- Evaluate the business case first
- External vendors
  - Through protected mechanisms only
    - Authentication
    - Access controls
    - Application proxies
    - Etc…
  - Minimum privilege
  - Deactivate when unnecessary
- External sources of data
  - Application proxies and validity checking
  - Procedures for operation when receiving invalid data
  - Receive as analog
- Providing data to external systems
  - Use archived data
  - Send as analog
  - View-only terminals

Other Security Suggestions

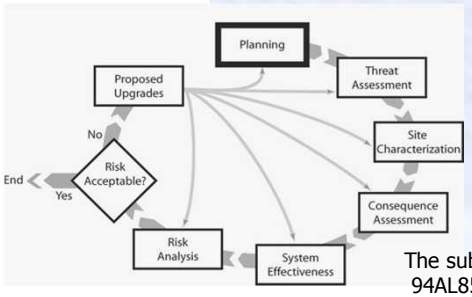
- Implementation guidance should mandate secure default configurations on all network devices
- Force "good" passwords and eliminate default passwords
- Disable in-band management (SNMP, Telnet, FTP/TFTP, web, etc.)
- Disable services
- Disable routing of private network addresses
- Control switch and hub connections

- Use PPN/VPN/LPN
  - Adequate physical security
  - PPN can't be shared
  - VPN/LPN can be shared
- IDS
  - Technologies
    - Signatures
    - Anomaly detection
  - Advantages
    - Can catch known attacks
    - Good research tool
  - Disadvantages
    - False positives and negatives
    - Can compromise the architecture
    - Manpower intensive

Firewalls, VPNs, and PCS protocols

- Simple protocols make more secure firewalls
- Network Address Translation (NAT)
  - Complicates DNP3 and ModBus IP address settings
  - OPC won't work with this at all
- VPNs resolve address problems
  - Specialized appliances may allow large numbers of VPNs
- VPNs require
  - Entity Authentication
  - Address Management
  - Encryption
  - Key management
- Solutions
  - Client VPNs (don't allow split tunneling)
  - PPP inside SSH (low-cost)
  - IPSec (low-cost, kernel or hardware encryption)
  - Application (TLS, user-space encryption)

Part IV: Disaster Recovery



Unlimited release – approved for public release.
Sandia National Laboratories report SAND2005-1001C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

SCADA Security

Useful things before

- Security Policy
- Security Plan
- Security Implementation
- Configuration management
  - Asset inventory
  - Backups of software, control system, and network configurations
  - Network and cabling diagrams
  - Pictures
- Disaster Recovery Plan
- Secure, off-site storage for above

Asset Inventory

- Complete list of what you have where
  - Hardware
  - Software
  - Configurations
  - Licenses
  - Security files
  - Cables
  - Communications
- Created as part of configuration identification
- Updated through configuration status accounting

Diagrams & Pictures

- Remember, your network is an asset
  - Make sure you can rebuild your network
  - Have diagrams of the IP network and the serial network
- Boring pictures and movies can be important
  - Take digital pictures of your equipment in place
  - Make movies showing equipment with commentary by engineers familiar with that equipment
  - Store these with your off-site backups

Disaster Recovery Plan

- Plan to recover process and control system from any abnormal event
- Control System disaster recovery different
  - Most guidance is for standard business systems
    - NIST Special Pub 800-34
    - FEMA 141
    - Other templates/guides
  - CS disaster recovery starts after that guidance -
    - You should have a Business Continuity Plan
    - You will work from your Emergency Operations Center
    - You have called in your disaster recovery teams…

Disaster Recovery Plan

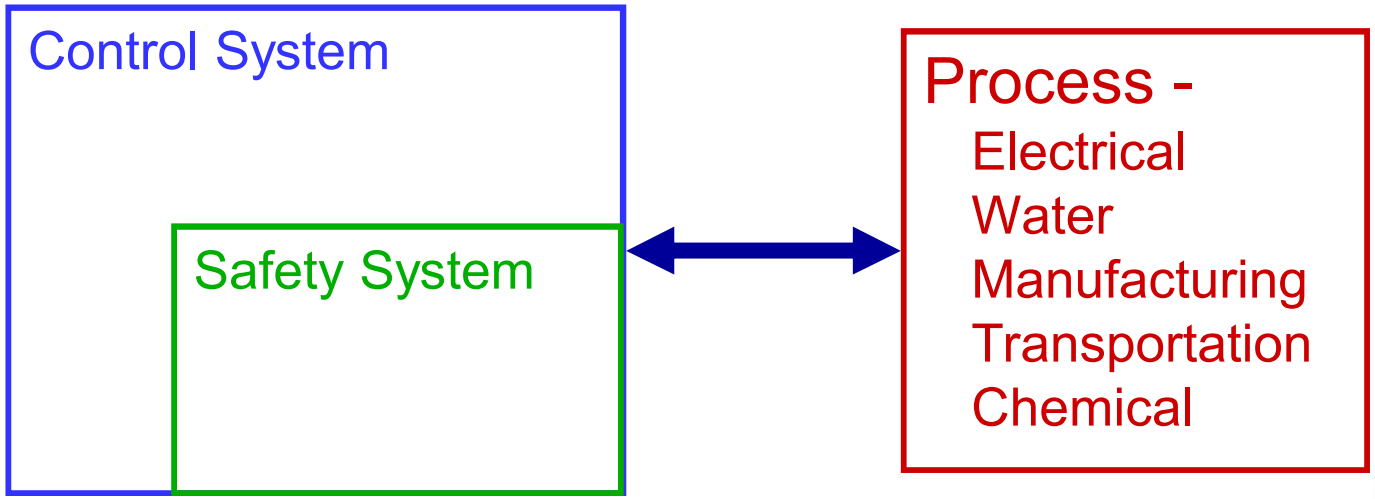
- Remember, you probably won't be able to just start things up all at the same time
- Base the plan on the sequence of events you need to perform a cold start of your entire process and control sysem
  - Use the sequence from installation
  - Use the sequence of your last cold start
  - Bring your control system engineers, process experts, and IT folks together and brainstorm
- Brainstorming
  - Pretend you're building your facility from scratch (that may be close to reality)

Disaster Recovery Plan

- Have a series of -
  - steps or
  - locations or
  - subsystems
  - to be repaired, calibrated, configured, tested and started
- Loads and process sequence may dictate the steps for recovery
- In a very few cases, there may be only one recovery step or location.

Disaster Recovery Process

- Process flow includes security at every step
  - but it is not security-centric, it's operations oriented
- Priorities should be -
  - Safety first
  - Process restoration second
  - Business third



Disaster Recovery Process

- Damage assessment
- Modify plan
- Physical security
- Process system recovery
- Safety system recovery
- Start safety control system
- Process control system recovery
- Startup
- Lessons Learned

DISCUSSION

Fundamentals For Control System Security

- System data
  - Fundamental element of any information system
  - System security is applied to preserve data attributes (AAI&C)
- Security administration
  - Encompasses non-control system functions as documentation and procedure
  - Components include security plans, implementation guidance, configuration management and security enforcement & auditing
- Architecture & design
- Platforms
- Networks and communications

Policy Section Headings

- Purpose
- Scope
- Policy
- Responsibilities
- References
- Revision History
- Enforcement
- Exceptions

Trends and Observations

- Sites with no data categorized
  - All information is available to anyone
- Security controls are usually commensurate to the levels determined
  - Often there are none
- PCS are more "important" than other systems, but the data is still not categorized
- Non-PCS has categorization, while PCS does not

Trends and Observations

- Not based on any security policy
- Bolt-on security doesn't work well (if at all)
- Usually *could* be secured to a reasonable level, with good governance
- Evolution of systems introduce vulnerabilities
  - Point solutions fix some perceived problem
  - Interactions not anticipated
  - Data enclaves not considered

RTUs / PLCs / IEDs

- Collect data from sensors and forwards commands to devices such as relays and valves
- Can also aggregate data from other RTUs at remote sites and plants
- More intelligent RTUs are becoming more prevalent
- Pressures for RTU advancement:
  - Reduce duplication of functionality (points may be sampled many times over in a substation)
  - Network and processing power ample for distributed control
  - Simplified operation and management
- Trends for RTUs
  - Similarity to other IT devices
  - Increasingly Ethernet or wireless
  - SCADA peer connections used for data transfer to/from other devices and for distributed control

SCADA Servers

- Functionality
  - Send signals to acquire data
  - Receive data from the system
  - Calculate and disseminate signals for system-wide control
  - Current system values stored in a memory database
  - Drive operator displays
  - Populate data archives
- Implementation
  - May be custom hardware for legacy systems, or an older OS (VMS, etc.)
  - Often, modern systems run on Windows or Unix
  - Platform for SCADA servers may be the same as those for display or archives

Types of SCADA Servers and Clients

- Human-Machine Interface (HMI)
- Automated control
  - EMS
  - WAP
  - AGC
- Alarm and events reporting
- Front-end processor (FEP)
- Data archives
- Engineering workstation

Trends and Observations

- No configuration guidance
- Administrator accounts
- Shared accounts
- Logging not enabled
- Unnecessary services
- Inadequate patching
- Default OS installations
- Etc.

Trends and Observations

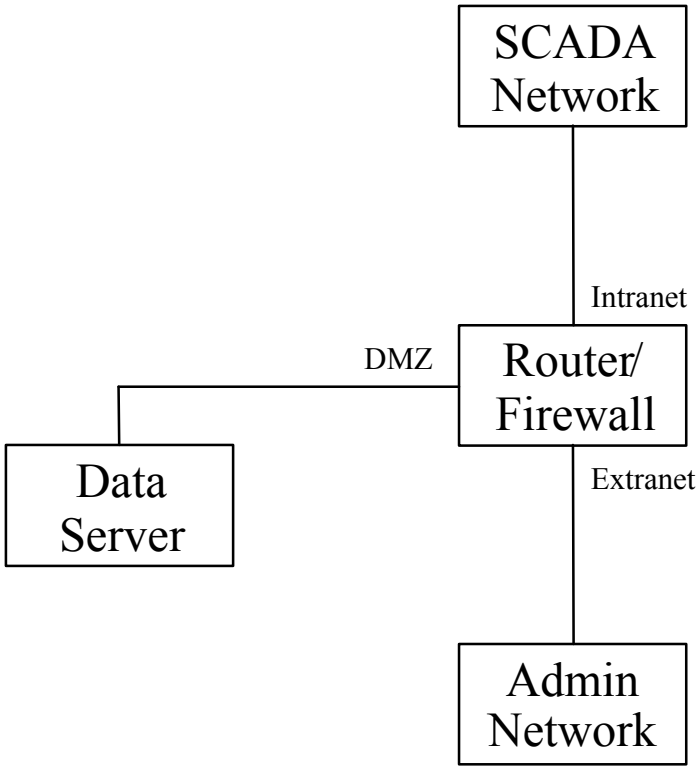
- SCADA networks are increasing in scope and function
- Increasing automation (remote locations)
- Adoption of TCP/IP networking
- Transition to public and virtual-private networks
- Use of SCADA networks for other purposes (alarm)
- Near real-time control
- Outsourcing network (and system) administration
- Shrinking boundary between business and operational networks

SCADA Dependence On the Internet

- Significant and growing
- System operations
  - Connectivity among SCADA elements
  - Connectivity between SCADA systems
  - Remote operation through VPN access
- System administration and maintenance
  - Example: contract network management
- Business integration
  - Example: publishing data directly from SCADA to the Internet

Internet/Intranet Connection

- Evaluate the business case first
- Strict access controls determined by required data flows



- Example router/firewall DMZ configuration:
  - Need to archive data for administrative usage
  - SCADA pushes data to archive machine
  - Users pull data from archive machine
  - Connections allowed from SCADA to DMZ
  - Connections allowed from admin to DMZ
  - All other connections denied
  - Only necessary and valid services, messages, content, and addresses allowed to the DMZ

Internal

- Lower cost
  - Staff time is the greatest cost here
- No privacy concerns
  - Staff has already been certified to see the data on the system
  - If there are different levels of data classification, ensure that staff performing the audit are permitted to see all levels
- Day-to-day experience with the system can reveal problems that should be addressed
  - Other staff may be more willing to talk with internal auditors
- Less educational down time since staff is already familiar with the system

External

- Can be more comprehensive since the audit/assessment team must learn the system from scratch
  - This can lead to a more complete picture of the system
- External parties may be aware of new tools and techniques
- Not hampered by internal politics
- Fewer blind spots
  - They have no special interest in any part of the system
- Trust**
  - This may work for or against the auditors/assessors

Types of Audits

- Conformance
  - How well system conforms to policies/procedures
  - Policy
  - Configuration
  - Good practice (other than security)
- Security
  - Measure policy/procedures against security good practices
  - Physical
  - Cyber
- Code
  - Generally only in software development environments

Types of Assessments

- Threat Assessment
  - Identify the threats (internal and external)
- Vulnerability Assessment
  - Identify vulnerabilities for a specific system in a normal operating environment
- Risk Assessment
  - Risk = threat * vulnerability * consequence
- Red Team Assessment
  - Identify high consequence vulnerabilities in a malicious threat environment