SCADA Security Self Assessments

Martin Stoddard, PE

Pacific Northwest National Laboratory

PROCESS CONTROL SYSTEMS FORUM

Collaborating to Advance Control System Security

Introduction

- **Why perform self-assessments?**
- **Scope of a security self-assessment**
- **Methods for security self assessments**
- **Security Metrics**
  - Some Metrics Examples

Why Perform Self-Assessments?

- To gain a better understanding of security posture
- To identify and correct security deficiencies
- To document system security measures in-place or recommended
- To proactively influence security standards and best practices
- Plus…

Avoid Potential Criminal Liability

Industrial "accidents" often result in the initiation of a criminal investigation. The more serious the impact on people or the environment, the more scrutiny the unfortunate company will receive from law enforcement. It is thus critical that attention be paid now, before any incident occurs, to the training, recording keeping, and maintenance requirements of the various environmental, health, and safety laws so that if the unthinkable happens, it can be established the conduct was accidental and not the result of criminal negligence or knowing conduct.

- Jane F. Barrett

From: "*Failure to Train Employees – Now a Federal Crime*"

Scope of a Self-Assessment

- **Organization and Policy –** Roles and responsibilities, documentation requirements
- **Design –** Network architecture, protocols, links
- **Configuration –** Operating System hardening, firewall rules, bench and operational testing
- **Operation –** Intrusion detection systems (IDS), log audits, virus protection, physical security, OPSEC
- **Maintenance –** Patch/Firmware management, penetration testing, system backups

Methods for Self-Assessments

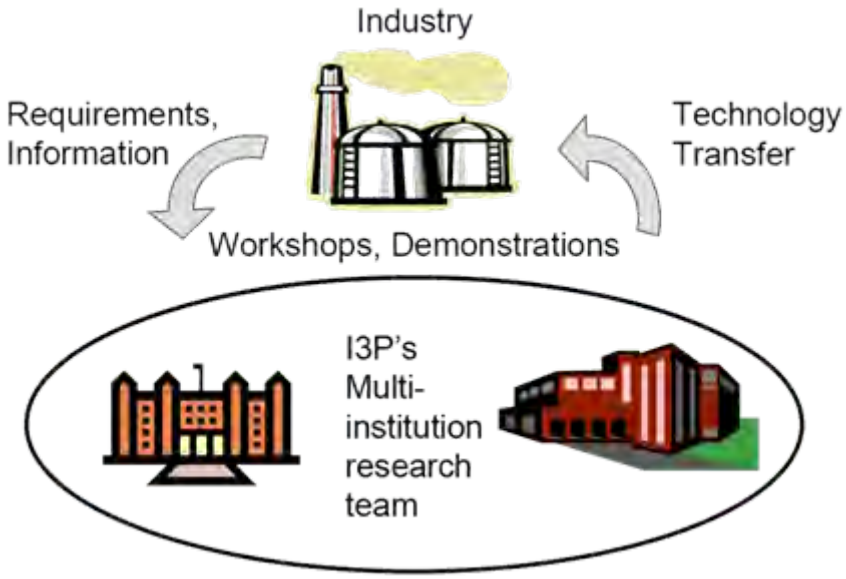
- Security questionnaire/audits (NIST SP800-26)
- Adoption of best practices (DOE 21 Steps)
- Blue team/Red team
- Risk assessments/security vulnerability assessments (RAMCAP, SNL RAM)
- Forensic investigation
- Security Metrics!

Security Metrics

- In their simplest form, metrics are measurements that are compared with a known scale or benchmark to produce a meaningful result.
- Metrics are used for Self-Assessment in many areas of an organization such as financial metrics, performance metrics, safety metrics, etc.
- This allows an organization to answer questions like “How productive are we?” or “How safe are we?”
- Which leads to, “How secure are we?”

I3P SCADA Security Research Project

- Topic-1: SCADA Risk Analysis
- Topic-2: SCADA Interdependency Models
- **Topic-3: SCADA Security Metrics**
- Topic-4: Secure SCADA System Design
- Topic-5: Cross Domain Information Sharing
- Topic-6: Technology and Knowledge Transfer



www.theI3P.org

Example Metrics

- **Organizational**
  - Frequency of audits
  - Number of security policy violations/failures
- **Operational**
  - Number of login attempts and failures
  - Percentage of dropped communication frames
- **Technical**
  - Operating system compliance with hardening guidance (SCORE)
  - Firewall rule compliance