

Information Security Issues for Industrial Control Systems

ISA

Houston, TX

September 10, 2001

Joe Weiss

Technical Manager, EPRI EIS Program

650-855-2751

joeweiss@epri.com

Why is Information Security a Problem

- Control systems, system architecture, and communication buses were designed for functional performance, information sharing, and user configureability
 - Control systems are vulnerable by design
 - Open architecture/open systems can be even more vulnerable
- Security and performance are often mutually exclusive
- Backfit of security is usually not an option
- Very few personnel with control system AND information security expertise
- Control system security issues are unique and information security technology companies have not addressed them

Is it Real?

- Electric utility and paper company vulnerability assessments have demonstrated unauthorized access of DCS and SCADA systems
- Networking technology, remote access, and web-enabled technologies make control systems vulnerable
 - Assessments have confirmed a significant number of previously unknown and unaccounted for remote access points

Technical Issues

- Determinism (interrupt timing) for security applications
 - Secure Real Time Operating Systems (RTOS)
- Response time/messaging requirements
- Security requirements for system design
- Security procedures for field testing
- Standards
 - IEEE/ISA
- Intrusion Detection Systems
- Firewalls

Other Issues

- Remote access
 - Modems, PCAnywhere, XWindows, etc
- Culture/Awareness
 - Senior management, operations, contractors, etc
 - Integration of IT and operational organizations
- Security policies and procedures for operational systems
- Configuration management/configuration control
- Confidentiality issues

Organizations

- Process Controls Security Requirements Forum (PCSRF)
 - NIST, NSA, DOE, EPRI, Petrochemicals, Paper, Water
 - Develop protection profiles for process controls equipment
- International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15
 - SCADA/EMS suppliers, National Lab, EPRI, Consultants
 - Develop protection profiles for SCADA/EMS
- Open Group
 - Aerospace Corp, Miter, Boeing, DISA, Raytheon, EPRI, Texaco
 - Real time security group to develop security API guidelines for RTOS
- EPRI EIS Program
- IEEE/ISA