



• August 15-18, 2010 • Dallas, Texas •
• Dallas Convention Center •



Industry Approaches and Resources for Securing SCADA/ICS

Agenda

- High level strategy
- 5 steps
- Resources



High level strategy

- Leverage existing security best practices with SCADA priorities in mind
- Employ administrative and technical controls and a defense-in-depth strategy to include:
 - vulnerability assessment
 - threat prevention
 - policy
- Defense-in-depth approach
 - Includes people, process and technology
 - The basic process is made up of five steps:
 - Evaluating threats
 - Establishing security policy and protections
 - Educating employees
 - Enforcing policy
 - Evaluating results

Step 1. Evaluate threats

- Threats to SCADA systems have recently become more tangible (see: Stuxnet)
- Resources exist to help orgs classify / categorize / evaluate their systems' levels of exposure and the types of attacks to which they may be subjected
- Risk analysis to prioritize the most critical areas to harden first
- Current threats must be documented with regular monitoring for new ones
- Establish baseline risk present in current configuration/systems for comparison in evaluation phase

Step 2. Establish policy

- Establish where the security gaps exist within the existing business policy
- Security must account for the SCADA's differences marked differences from IT systems, including real-time processing, maximum high availability requirements and fragility (razor-thin capacity margins on processor capacity, memory, etc)
- Put assessment results to work
- Network segmentation
- Deploy intrusion prevention technology including application-level protection for traffic that is allowed by the firewall and real-time alerting for additional levels of logging

Step 3. Educate the workforce

- Uninformed end-users often the weakest link in security
- Industry and other experts should be tapped to deliver security training to SCADA/ICS operators and other users of SCADA systems and the data they generate

Step 4. Enforce policy

- Automated scanning software can be used to help check/maintain system compliance
- With close coordination with SCADA engineers, automated scanning performs heavier scans on less critical systems and leverages redundancy to ensure no system downtime
- Recurring security assessments should (must) also be part of enforcement
- Assessments encompass internal and external network segments and application and network layers
- The results of these assessments can be used to constantly reevaluate risk reduction goals

Step 5. Evaluate results

- Organizations should conduct security audits to ensure continued compliance with their on policies as well as industry and government regulations
- Organizations should measure the overall reduction in risk as a basis for calculating overall return on investment from security solutions

Resources

- [DOE Roadmap to Secure Control Systems in the Energy Sector](#)
- [Open SCADA security project](#)
- Sandia National Labs' [Center for SCADA Security](#)
- Joe Weiss book: [Protecting Industrial Control Systems from Electronic Threats](#)

Disconnected, really?

“Sanitized” conversation with operator of a power plant (200–250MW, gas-fired turbine, combined cycle, five years old, two operators, and typical multi-screen layout):

Q: Do you worry about cyber threats?

Operator: No, we are completely disconnected from the net.

Q: That’s great! This is a peaking unit, how do you know how much power to make?

Operator: The office receives an order from the ISO, then sends it over to us. We get the message here on this screen.

Q: Is that message coming in over the Internet?

Operator: Yes, we can see all the ISO to company traffic. ... Oh, that’s not good, is it?



Thanks to:

Dr. Massoud Amin, U of Minnesota. “Securing the Electricity Grid”, The Bridge, Spring 2010

<http://central.tli.umn.edu/Securing-the-Electricity-Grid.pdf>

GovEnergy 2010

Andy Bochman
Energy Security Lead
IBM/Rational

[DOD Energy Blog](#)
[Smart Grid Security Blog](#)

Thanks! ... Questions?