



Real World Security for SCADA and Process Control Systems



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Agenda

- Introduction
- Background & Drivers
- The Sky is NOT Falling but...
- North American Electric Reliability Corp. (NERC)
- Approach
- Resources



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008





Introduction

- Ed Goff, CISSP
 - System Architect – IT&T Security Analyst, Progress Energy, Inc.
 - Progress Energy – Fortune 250 electric utility Company operating principally in the Carolinas and Florida



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Official Use Only

Contains information which may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number (s) 2 . Approval by the Department of Energy prior to public release is required.

Reviewed by: Thomas Harper 03/5/07



What is SCADA & PCS? Now ICS

- SCADA: Supervisory Control and Data Acquisition systems
 - Automated Process Control Systems
 - Electric Grid control
 - Automated Manufacturing, Oil & Gas Production
 - Flow and Environmental Controls
- Distributed Control Systems (DCS) are included
- Industrial Control Systems (ICS)
 - Includes SCADA, PCS, DCS, etc.
 - Chemical, Manufacturing, etc.

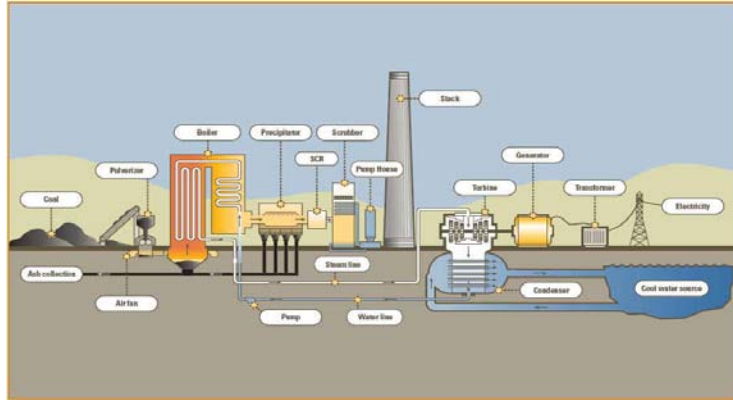


Ed Goff, CISSP
Real World Security for SCADA & PCS

B5 - April 27, 2008



Typical Power Plant with ICS



Background

- Originally designed and implemented as isolated, standalone systems
- Different times and different requirements
- Little to no security designed in until recently



- Bottom-line: Matured connectivity & use of ICS but not management & security



Drivers

- The 2003 Blackout
- 9/11
- Interconnectedness
- Attack Sophistication vs. Intruder Technical Knowledge



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Threats

- “Insider” threats including social engineering, espionage, and spoofing people with high access levels
- Competitors, contractors, corporations
- General malicious code threat
- Environmental groups
- Non state-sponsored terrorism
- Unintentional exposure of vulnerabilities
- Malicious code attack specifically directed against a Customer
- Nation states/Governments
- Organized crime



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008





Some Differences between IT and ICS

Category	Information Technology System	Industrial Control System
Risk Management Requirements	Data confidentiality and integrity is paramount	Human safety is paramount, followed by protection of the process
Time-Critical Interaction	Less critical emergency interaction	Response to human and other emergency interaction is critical
Communications	Standard communications protocols	Many proprietary and standard communication protocols
Managed support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Sources: NIST Guide to Industrial Control Systems (ICS) Security 800-82 Sept 07



The Sky is NOT Falling but...

- Not FUD (Fear, Uncertainty & Doubt)
- Actual Events
 - Jan 2003 *SQL Slammer* Davis-Besse nuclear plant
 - Oct 2003 Attacker brought down the Port of Houston
 - Aug 2003 Virus on computer systems of CSX Transportation halting passenger and freight train traffic in Washington, DC.



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008





NERC Critical Infrastructure Protection Standards

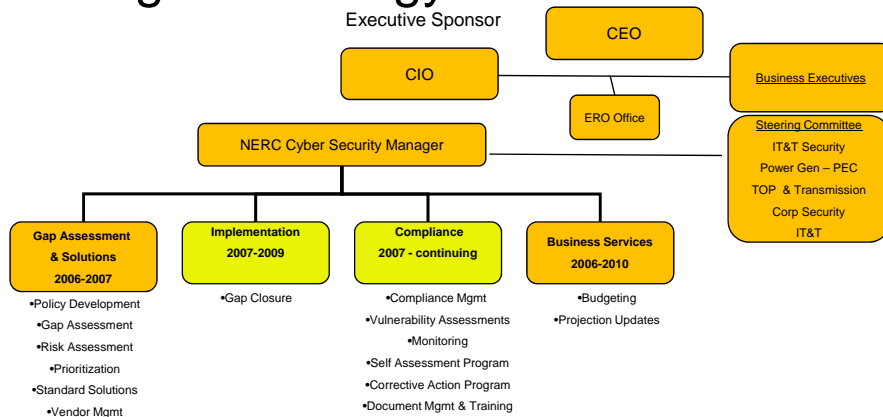
- Provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
 - CIP002 – Critical Cyber Asset Identification
 - CIP003 – Security Management Controls
 - CIP004 – Personnel and Training
 - CIP005 – Electronic Security Perimeters
 - CIP006 – Physical Security
 - CIP007 – Systems Security Management
 - CIP008 – Incident Reporting & Response Plan
 - CIP009 – Recovery Plan



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Progress Energy team



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Approach

- Do your homework
 - Online resources, books & magazines
 - Get plugged in to industry groups
- Partnering with Control System Engineers
 - Regular peer collaboration sessions
 - Discovering where IT can add value – not just for regulatory requirements
- Study and self assessment

Approach – cont.

- Visit another company who has already been successful and learn what they did right/wrong
 - DOW Chemical visit,
 - DuPont, Detroit Edison, Southern Company
- Cross-functional teams
 - Executive leadership
 - All stakeholders must be at the table designing the solutions or are onboard with the direction
 - Starts with the leadership of the stakeholder groups



Approach – cont.

- Recognize the opportunities for low hanging fruit
 - Some IT solutions/capabilities can be leveraged
 - You will run out of \$\$ before you run out of problem
- Not 100% secure – 80/20 rule for Security
 - The first 80% of threat vectors are relatively inexpensive to secure against
- Functionally aligned teams
- Do not over rely on vendors



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Industry Expert Recommendations

Eric Byres – CTO, Byres Security Inc.

“Just hiding behind a perimeter defense is suicide. For years the IT world has known that a big corporate firewall is just not enough when it comes to security. It is time that the control and SCADA world brings the strategy of critical edge protection to the control system, giving the most important devices in our plants (the PLC, DCS, HMI and so on) the same defense in depth security the IT department gives the receptionist’s desktop.”



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008





Industry Expert Recommendations

Peter Allor - program manager IBM ISS

“The indication is that there is a very real threat to the control systems and SCADA networks that monitor and regulate these industrial systems. Like the financial institutions that are being exploited daily, these control systems are Internet connected and are therefore susceptible to any number of malicious attacks. Private-sector security firms have conducted real-world penetration tests with large power plants, oil companies, manufacturers, and other users of control systems and have demonstrated that these systems are indeed at risk to Internet-based attacks.”



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008



Industry Expert Recommendations

Eric Cosman - Engineering Solutions Arch., DOW

“To establish (or confirm) a solid and effective working relationship involving the support organizations are responsible for IT and industrial automation systems security...including defined roles and responsibilities, is a critical prerequisite. The pitfall to be avoided is rushing right into implementation of security measures without a firm and shared understanding of who is responsible and accountable for what, both immediately and in the longer term.”

“...also considering the need for written policies and procedures that will be required to sustain the changes.”



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008





Resources

- Securing SCADA Systems by Ronald L. Krutz, PhD
- Electric Power Substations Engineering By John Douglas McDonald
- NIST SP 800-82, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security - <http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf>
- Digital Bond – www.digitalbond.com
- Process Control Systems Forum - <https://www.pcsforum.org/>
- Idaho National Laboratory – Control System Security Program - <http://csrp.inl.gov/>
- Final Report on the August 14, 2003 Blackout in the United States and Canada - <https://reports.energy.gov/>
- 21 Steps to Improve Cyber Security of SCADA Networks - <http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf>
- Department of Homeland Security – <http://www.dhs.gov/dhspublic/>
- ISA – <http://www.isa.org/>



Ed Goff, CISSP
Real World Security for SCADA & PCS
B5 - April 27, 2008

