State of Cyber Security in SCADA/Control Systems

Göran Ericsson, PhD
goran.n.ericsson@svk.se

September 8, 2008
SANS SCADA EU Summit
Amsterdam, The Netherlands
Agenda

Purpose: Highlight the electric utility perspective on cyber security for SCADA/Control Systems

• Background
• Evolution of SCADA systems
• Problem Statements
• Proposal for further works

Acknowledgement: Hans Hol, Marc Tritschler
Göran Ericsson

- Swedish National Grid 1997-
  - Manager IT Security (As of 2007-01-01)
  - Former Data- and Telecommunications: various positions
- 1996 PhD: "On Communication in Power System Control"
  - Chairman WG D2.22 on Information Security (2006 – )
- IEEE
  - Senior Member Power Engineering Society 2006
  - Power System Communications Committee
- Has published >30 papers in international forums, both within and outside IEEE. Mostly utility perspective:
  - Information Security for Power Control Systems
  - Power System Communications (the "life nerve")
Swedish National Grid (Svenska Kraftnät)

- Svenska Kraftnät is a public utility
- Our core business is power transmission on the national level 220kV, 400kV
- 16,000 km power lines
- Interconnections w/ Norway, Finland, Denmark, Poland, and Germany
- Svenska Kraftnät has provided telecom network services to external customers since 1994
- Optical fiber network 8,000 km WRAP, OPGW
Background

- Electricity is of paramount importance for our society
- Digital threats are increasing
- SCADA systems and substations are being increasingly interconnected with other systems
- In earlier projects, IT-security was not considered to a great extent
Chain of dependencies

[Diagram showing a chain of dependencies with various images and arrows connecting them]
Physical and Logical Security

- Physical security – easy to grasp
- Logical, digital security – how about that?
- Is it possible to hack a substation over Internet? – YES!
- Set up technical solutions
- Impose new rules + Follow up
General trends

• From proprietary to COTS (Commercial Off The Shelf)
• Increasing use of standard products (PC, operating system, networking equipment, …)
  • Well-known knowledge, not only on one/two persons
  • No ”security-by-obscurity” anymore
• Use of broadband connections – new possibilities open up
• BUT: Is everyone aware of both POSSIBILITIES and RISKS?
• Does everyone make an active decision?
Development of Industrial Control Systems 1(2)

1. Islands of operation

2. Interconnected

3. Partially Integrated
Development of Industrial Control Systems 2(2)

4. Today. Full integration, due to open system requirements

5. De-coupling between Operational SCADA/EMS and Admin IT, to secure operational
Development of communication capabilities

From

• Small, narrowband paths in the wood

To

• Broad, 7-lane highways
Access points to SCADA system
Interconnected systems

- Administrative
- Settlement info
- Maps

- SCADA/EMS
- Drawings
- Engineering
- Maintenance

Administrative Network and Systems

Power System Control Systems

External connections
Evolution of SCADA systems

- Being available over Internet
- Now based on the same technique as common administrative office IT systems: COTS
- Being integrated with administrative IT-system
- \(\Rightarrow\) Same vulnerabilities for SCADA systems as for administrative IT systems!

- What to do?
- Disturbances can affect essential infrastructures:
  - Electric power, water, heat, gas, transportation
  - Inter sectorial
  - How many authorities have responsibility in a country?
- CIP = Critical Infrastructure Protection
- CIIP = Critical Information Infrastructure Protection
Evolution of SCADA systems

- Cost – bespoke platforms were becoming too expensive to develop and maintain
- Time-to-market
- Increased hierarchical architecture requirements – data transfer, monitoring and management
- Broadband communication capabilities
- Vendors increasingly use COTS products
Problem Statement – Utility perspective

• Awareness already there?
• Substation security is weak
  • What kind of equipment is being installed? Is IT cyber security included?
  • Overload of firewalls, switches?
  • How can a utility rely on that the vendor’s knowledge of security is sufficient?
• Resources
  • Staffing
  • Money
• SCADA systems not designed *from the beginning* to be secure
• ”Security-by-obscurity” is not enough
Problem Statement – Utility perspective

• Previously: Systems deployed by ”fit and forget”

• Now:
  • Systems must actively managed and maintained
    • Evergreen approach?
  • Systems have a great deal of complexity
  • Do we always know what we end up buying?
    • Systems based on vendor developed + third-party software
    • Difficult to have detailed knowledge of all aspect of a system
  • Do vendors have detailed knowledge?
Problem Statement – Utility perspective

• Security vulnerabilities are a moving target
  • Many, Varied, Complex, ...

• Security aspects must be treated from the very beginning in projects – even before procurement

• Who takes responsibility for security when deploying a new system:
  • Utility?
  • Vendor?
  • Both?
  • None?
Problem Statement – Utility perspective

• Deploy technical secure solution +
• Make people aware and committed +
• Introduce routines for security

• How do we introduce and enforce standards among power utilities?
Proposal

• Security is a new, always on-going issue that needs to be taken care of
• Awareness
• Fully support from top management
• Active decisions, based on risk assessment
• Resources (both at utilities and vendors)
  • Staffing
  • Money
Proposal

- Users must address security within a structured framework
  - Technical
  - Policies, procedures, compliance checks, ...
- Users must push vendors
- Both control systems and IT skills needed to understand technical vulnerabilities, risks and possible solutions
Proposal – System design and support

• Centralized logging
  • Tools
  • Automated alarms on incidents

• Forensic possibilities
  • Save information for later analysis

• ”Evergreen” approach

• Patch service
  • Applications: Allocations, Operating System, 3rd party SW, share ware, ...
  • Tested patches: Time consideration

• Support 24-7
Proposal

• Use country / EU electric power organizations to stress cyber security
• Security part of procurement
• Risk assessment at major changes and regular intervals
• Use a standard framework/similar in the area of control systems
  • ISO 27000 (17799), NERC CIP, NIST SP800, ...
• Routines and processes in place
• Part of daily operation
• ”Personal responsibility”?
Awareness

- Entire Swedish National Grid
  - Web-based education
  - Part of incentive program
- Management
  - Need for funding
  - Need for staffing!
- Critical system governance
  - Importance of following the work processes
  - Importance of good order
- Cooperation with other companies
Sweden: Governmental coordination on SCADA Security

Based on existing organizations, develop existing expertise, coordinate relevant resources, utilize international experience and knowledge.

• Extended cooperation on SCADA security within the government
• Further develop on-going cooperation on SCADA Security between Swedish and foreign authorities
• Raise the awareness on Cyber Security among users and vendors of SCADA systems
• Develop technical and administrative recommendations and guidelines, and participate in international standardization works.
CIGRÉ experiences

- Convenor of WG D2.22 on Information Security
  - Frameworks. Security Domains (Logical)
  - Risk Assessment
  - Security Technology considerations
  - Output: Technical Brochure (TB) 2009
    - Recommendations
Securing your operation is hard and continuously on-going work

- Include in daily operation
- Learn from other people’s mistake
- You don’t have time nor money to do them yourselves
Final recommendations

• Speak the language that gets and retains corporate attention
  • "Risk management", "Governance" etc.,
  • not "Firewalls", "Encryption" etc.
Therefore has a better chance of getting budget

• Make on-going management of security part of the new "business as usual" for control systems

• Build a structured framework for the management of control systems security within an overall control systems governance framework, from the control centre to the end devices in the field

• Embed security requirements into projects and security related roles into project teams right from the start

• Make sure that control systems support teams have the right skills, which include large amounts of IT and network engineering skills
Questions?