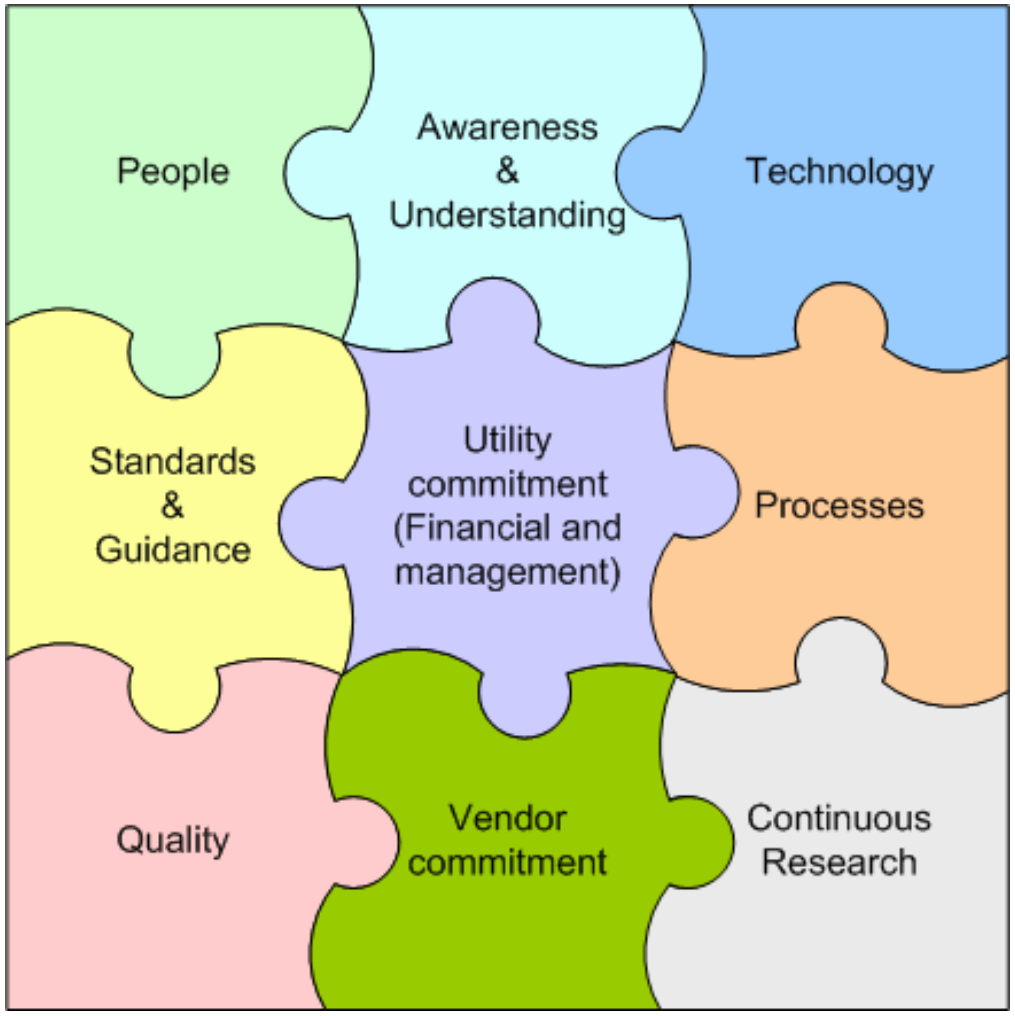
Control System Security
ABB's Vendor Perspective

Dr. Ragnar Schierholz

Industrial Software Systems
ABB Corporate Research

ABB's view on Cyber Security



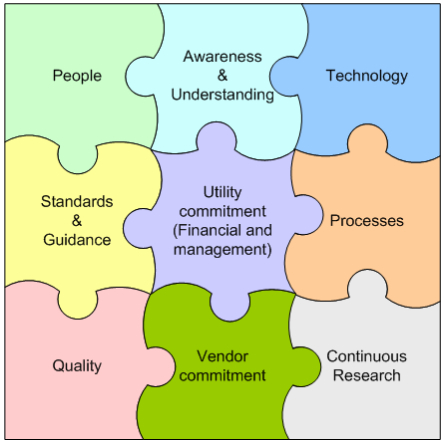
ABB's view on Cyber Security

What is the real risk?
- No shared understanding of actual risks
- Base decisions on true understanding of the issues!

Operators vs. IT staff
- Different objectives, terminology
- Need to work together (better)

Human Errors
- Misconfiguration, misbehavior,…

Security is a process
- Attacks & countermeasures evolve continuously
- Operating and maintaining a security architecture is crucial



Recent technology allows secure operation, given
- Correct deployment and configuration
- Continuous monitoring

Research
- Security concepts must constantly evolve to keep up With current threat situation

Variety of standards
- Different aspects of the system
- Different industries
- Overlapping, contradicting each other

Quality
- Quality mgmt must address security properly
- Continuous, well specified security testing

Enabling secure operations is vendor responsibility
- Requirements management
- Secure system architecture
- Verification of security offerings

Secure operations is customer responsibility
- Assessments
- Security Management Systems
- Employee training
- Financial commitment

ABB's position on Cyber Security

- As technology leader, ABB fully understands the importanc and its responsibility in Cyber Security for industrial control systems.
- ABB is actively anticipating the security challenges imposed by the changing landscape of the markets.
- ABB is constantly adapting our systems to the latest developments in security and is engaging with external partners for security testing and consulting.
- ABB has been involved in cyber security for control systems for over a decade – long before the hype.

There is no control system on the market that is 100% secure. ABB is actively working to maximize cyber security in our offerings.

Security standardizations activities

- **IEC 62351** – Data and Communications Security
- **ISA S99** – Security for Industrial Automation and Control Systems
- **IEEE P1686** - Substations IED Cyber Security Standards
- **IEEE P1711** - Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access
- **Cigre B5.38** – The impact of implementing security requirements using IEC 61850
- ABBs involvement with NERC
  - Participation in NERC CIPC (Critical Infrastructure Protection Committee) meetings
  - Participation in Revision of NERC CIP standards (activities starting in 2008)
  - Participation in Development of NERC Security Guidelines (actives starting in 2008)
  - Organization of Expert Panel with NERC for IEEE PSRC

Security Testing

- Device Security Test Center
  - ABB has built up a centralized security test center to assure a consistent approach in providing security for systems and devices
  - The test center is working independently from the development centers, but cooperating to implement best practices
  - Validates code quality in order to improve the robustness and security of protocol stacks

- System Tests
  - First vendor to have system tested at Idaho National Laboratories SCADA test bed
  - Tests started in 2004
  - In 2008 tests with customer consortium

ABB Consortium is 2007 National Cyber Security Leadership Award Winner

In January 2008, at the SANS (Systems and Network Security) SCADA Summit in New Orleans, the chairman Alan Paller identified the ABB Consortium as a 2007 National Cyber Security Leadership Award Winner.

ABB Corporate Research

- Examples of current and past research projects
  - New protocol for access control
    - Centralized Management
    - Minimal device configuration overhead
    - No secret on device
    - No online connection to centralized server
  - Threat Modeling for embedded devices
    - Collaboration with University of St. Gallen
    - Tool supported methodology
    - Allows for validation and verification
    - Tailored for development of embedded devices
  - Security Workplace for 800xA
    - Integration of security health monitoring with process control systems
  - Involvement in EU projects

Summary

- Security is **not just a matter of technology**, it is primarily about people, relationships, organizations and processes working in tandem to prevent an attack
- Effective security solutions require a **joint effort** by vendors, integrators, operating system providers and end users.
- There is **no single solution** that is effective for all organizations and applications.
- **Security is a continuous process**, not a product or a one-time investment
- IT Security mechanisms **can be circumvented**, therefore
  - **Defense-in-depth** demands multiple barriers against each type of attack
  - Security architecture requires **protection** and **detection** of circumvention
  - An attack **cannot be 100% avoided**
- **Security is about risk management** - perfect security is neither existent nor economically feasible

Contact for questions and comments

Dr. Ragnar Schierholz GCIA

Scientist
Industrial Software Systems

ABB Switzerland
Corporate Research
Segelhofstr. 1K
CH-5405 Baden 5 Dättwil
Telefon +41 58 586 82 97
Mobile +41 79 733 67 47
E-Mail: ragnar.schierholz@ch.abb.com

Power and productivity
for a better world™