AREVA
Securing Your System
Today and in the Future

Sharon Xia
AREVA T&D Inc.

January 17, 2008
Control System is Complex

A Simplified Energy Management System
Understand the System

- Network topology
- Hosts & devices
- Applications
- Communication channels and protocols
- Organization & people
Identify Assets and Risks

- Critical assets
- Risks to each critical asset
- Mitigation plan for each risk
- Commitment
Defense in Depth - Network Segmentation

Define security zones and security policies

[AREVA e-terraplatform Network Security Guide]
Defense in Depth
- Perimeter Protection

Apply firewall, IDS/IPS, malware protection at perimeters

[AREVA e-terra platform Network Security Guide]
Defense in Depth
- System Hardening

- Remove / disable unused services/applications, ports and accounts

[AREVA System Security Guides (CIS benchmarks)]
Defense in Depth
- Application Security

- Authentication and authorization
  - Strong authentication
  - Role-based authorization

- Security development lifecycle

- Security code review

- Penetration Test

- Security patches
Defense in Depth
- Data Security

▶ Protect Data in Motion
  ◇ Use standard security protocols
  SSL/TLS, HTTPS, SSH, SFTP, Secure-ICCP, Secure DNP 3, DNP 3.0 over SSL/TLS
  ◇ Upgrade to modern devices that provide better security features
  ◇ Use IPSec for TCP/IP and WPA for wireless

▶ Protect Data in Storage
  ◇ Protect business data and configuration data
    ● in files, in databases and in memory
  ◇ Use system built-in mechanisms
    ● ACL (Access Control List)
    ● EFS (Encryption File System)
    ● Crypto services
Security Management

Education

[AREVA provides e-terra platform Security Management training course to our customers]

- Enforce policies, standards, guidelines
- Apply security patches
- Auditing
- Change Management
- Backup and disaster recovery