U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

David Kuipers: Idaho National Laboratory (INL)
Shabbir Shamsuddin: Argonne National Laboratory (ANL)

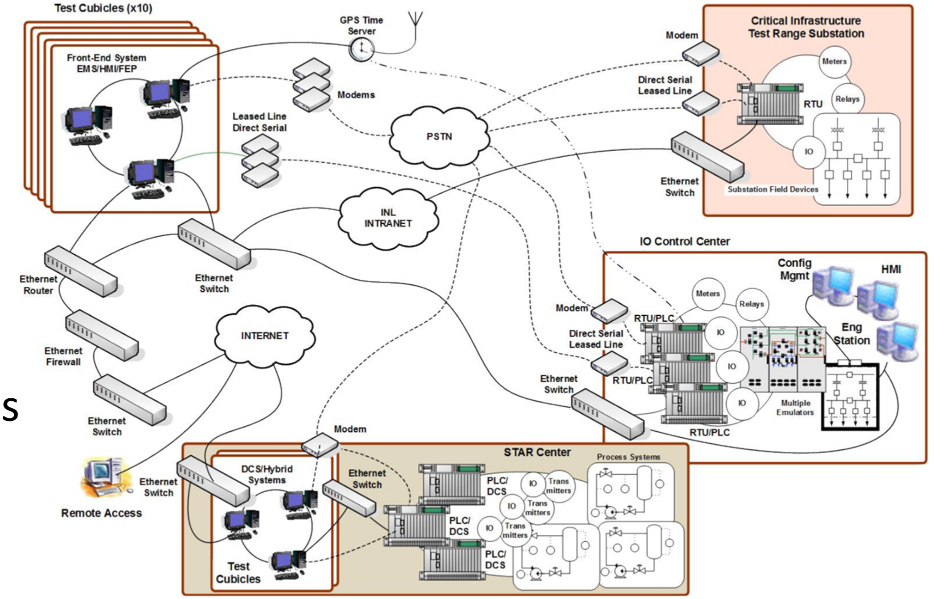
Control Systems Vulnerability Assessments

Idaho National Laboratory

INL/MIS-09-15784

Control System Cyber Security Vulnerability Assessments

- **Major Successes:**
  - Over 30 Assessments since 2003
  - Last Year:
    - 3 ICCP Vendor Products
    - 3 SCADA/EMS ICCP API Assessments
    - 2 SCADA/EMS System Lab Assessments
- **Roadmap Goals:**
  - Measure and Assess Security Posture
- **Outcomes:**
  - Specific vulnerability information to Vendors and Asset Owners
  - Common Vulnerability information for control systems for general evaluation and application of security controls



- **Schedule:**
  - 2 Assessments FY2010
- **Level of Effort:** $923K INL/$175 ANL
- **Funds Remaining:** $620K INL/$148 ANL
- **Performers:** INL/ANL ONG Support
- **Partners:** AREVA, Telvent, LiveData, SYSCO, ABB, Siemens, OSI, GE, Asset Owners

Technical Approach and Feasibility

- **Approach**
  - Partner with Vendors and Asset Owners to assess cybersecurity vulnerabilities associated with control systems and their communications architectures
    - Provide feedback to vendors and asset owners with mitigation suggestions to vulnerabilities identified
    - Provide common vulnerabilities report to summarize vulnerabilities found common to industrial control systems
    - Attend vendor user group meetings to support and educate in control system cybersecurity
- **Metrics for Success**
  - Asset owner members of vendor user groups initiating and/or participating in security working groups.
  - Reduction in vulnerabilities in subsequent assessments
  - Asset Owners participation in project funding

Technical Approach and Feasibility

- **Challenges to Success**
  - NDA and CRADA timely implementation
  - Vendor/Asset Owner partnership development schedule impact
  - Vendor/Asset Owners Development and Operational window schedule impact
- **Technical Achievements to Date**
  - Assessments include approximately 85% of Transmission Vendor SCADA/EMS
    - Current Technology Systems
  - Two phases of multi-vendor ICCP completed
  - Feedback and lessons learned through Assessment and Common Vulnerability Reports

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Continue outreach to current vendors and associated user groups
  - Develop outreach opportunities to new vendors/users
    - Invitations to new user groups through outreach presentations: Invensys
  - Participate in user group security working groups
  - Support funds-in projects from user groups for assessments
- **Plans to transfer technology/knowledge to end user**
  - Advance control system vulnerability metrics analysis
    - End User and Vendor Scoring of vulnerabilities
  - Incorporate scoring metrics in vulnerability assessment cyber templates

Next Steps

- **Approach For Next Year**
  - Complete 2 FY-10 Assessments in Q1/Q2
  - Plan 2 new Assessments in Q2-Q4
    - Develop plan to evaluate majority vendors in DMS, ONG and SG applications
  - Evaluate/transition SCADA/ICS Test Bed VM Modifications
    - INL funding
  - Plan Vulnerability Assessment process recommended practice for industry

Questions?