Secure Access and Device Management

US Utility Implements Corporate Wide Standard to improve Grid Reliability and Operational Efficiencies
Outline

• Executive Summary
• Project Guidelines
• Business Drivers
• Addressing Challenges
• Conclusion
Executive Summary

• Deregulation & Grid Modernization

• Advanced IED’s

• IED Management
  • Lifecycle Costs
  • Cyber-Security
  • Regulatory Compliance
Project Goals

• IED Management Standardization

• Multi-Vendor Integration
  • Integrate Existing Devices
  • Seamless Future Growth

• Engineering Time
  • Remote Access
  • Maintaining Security
Project Goals Continued

• **Device Management**
  • Within an Electronic Security Perimeter
  • Automated Password Changes
  • Configuration and Patch Updates
  • Security and Firmware Management

• **Cyber Secure Communications Path**
  • Use Vendor Interface
  • Full Control of IED
Project Application

- IED Application Driver
- Automates IED Connections
- Automated Credentials
- User Access with RBAC
- Command Blocking
Business Drivers

- FERC / NERC
  - Operational Reliability Standards
  - Security Policies

- Infrastructure Investment
  - Personnel Training
  - Device Growth and Replacement

- CIP-007
  - Yearly Password Changes
Current Operations State

- Disabling Remote Access
- Manual Password Changes
- Manual Fault Collection
- Onsite IED Management
- Higher Operational Costs
Project Challenges

- Automated Password Management
  - Multi-Vendor Relays
  - Communication Processors
  - Port Server
  - Network Switches
  - RTU’s

- Complex Multiple Firewalls and VLANS
  - Makes IED management more difficult
Project Challenges Continued

- **Baseline Firmware Pool**
  - NERC Compliant Firmware Storage Location
  - Firmware Upgrade Plan (CIP-010 Requirements)

- **Fault and SOE Data Collection**
  - Automated Data Collection
  - Notifications For Engineering and Operations

- **Secure Remote Engineering Access**
  - Despite Network Architecture or Communication Types
Addressing Challenges

- **Password Management**
  - Application Driver

- **Fault and SOE Data Collection**
  - Automated Data Collection
  - Notifications For Engineering and Operations

- **Remote Engineering Access**
  - Despite Network Architecture or Communication Types
Addressing Challenges

• NERC / CIP Compliancy
  • Secure Remote Access to IED’s
  • End to End Encryption
  • Legacy Protocols Using Clear Text

• Automated Task Scheduling
  • Password Changes
  • Event and Fault File Collection
Typical Network Setup

- **User PC**
- **Active Directory Server**
  - Group Policies
- **Client Access Server (CAS)**
  - Front end access to system
- **Database Server (DBS)**
  - Encrypted database
- **Device Communications Server (DCS)**
  - Security server for hosting endpoint connection to IEDs

**Networks:**
- Corporate LAN
- DMZ Isolation Network
- Wide-Area Network

- **Firewall**
- **Encrypted**
Benefits & Conclusions

• Reduced Operational Costs
  • Reducing Personnel and Equipment Traffic to Site
  • Reducing Manual Tasks

• Secure Engineering Remote Access
  • Encrypted Data Collection, Password Changes and IED Configuration
  • Event and Fault File Collection

• Support For Legacy and Future IED’s
  • Reducing Costs for IED Replacement
QUESTIONS
Thank You

Danke

Merci

Gracias

Спасибо

Obrigado

감사합니다

谢谢

ありがとうございます