Encore Networks

Bridging the Gap between Technologies

by

Matt Girard, Sr. Director of Market Development
Learning Objectives

- Discover about the resources that are available for bridging the gap between older legacy technologies and modern IP based network technology
- Select and implement secure solutions for critical assets
- Options to simplify NERC-CIP requirements
- Leveraging legacy equipment – while migrating to an IP environment
- Reducing operating costs for improved ROI
Bridging the Technology Gap

- **Challenges**
  - Increased Network Costs
  - NERC Compliance, Audits forthcoming
  - Legacy Network Technology, leased lines
  - Retaining legacy RTU and Metering Technology, Serial
  - Common Source Network Management

- **Network Interface Choices**
  - Terrestrial
  - Wireless, Radio and Cellular
  - Satellite

- **Industry Solutions**
  - Implementing IP technology, keeping legacy equipment
  - Reducing operation costs
  - Near Term ROI
Challenges Faced in Telecommunications Infrastructure
Planning Technology

- Cost Containment - Technology best suited for Asset transport
  - Core Grid Management
  - Substation/Metering - AMR

- Sort term vs. Long term requirements
  - Securing Data – to meet NERC-CIP standards
  - IP Enabled technology - Converging solutions
    - Real-time Information access
  - Substation Automation
    - AMR, reduced costs

- Building for the future, retaining the past
  - Leveraging deployed legacy equipment (RTUs & Meters)
  - Migration path for AMR/AMI / SmartGrid

- State by State mandates for AMI; Stimulus package
  - Riding AMI as a backbone
    - Distribution/Switching
Increased Network Costs

- Rising costs for Dial and DDS - Multi-drop circuits (monthly)
- Increased T1 circuit costs; when-where available
  - Reliability
- LMR frequencies becoming scarce
  - Some Un-licensed frequencies controlled by Homeland Security
- Loss of traditional analog circuits
- Push to IP and Fiber
  - Integration of all services
  - Forced upgrades - conversion costs are impacting budgets
  - Service effecting timelines mandated
Leased Line Network Replacement

- **Cost Containment** - The average utility company has 100’s of leased lines with increased carrying costs
  - The majority of carriers are migrating from analog circuits and have switched to an IP infrastructure.
  - The new IP infrastructure allows redundant paths and high throughput for increased application support.

- Frame Relay and MPLS are being used more frequently due to ‘non-IP’ based network connections (Non-Routable protocols)

- Cellular data technology plans offer varying prices to better fit polled applications
  - In most cases Utilities have cellular phone plans that can be leveraged to drastically reduce monthly operating costs

- VSAT solutions have a wide range of bandwidth offerings to fit all applications from fail-over to primary communication paths
## NERC-CIP Cyber Security

<table>
<thead>
<tr>
<th>Standards</th>
<th>Summary</th>
<th>Purpose</th>
<th>Typical Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NERC-CIP-003</td>
<td>Security Management Controls</td>
<td>Management and Control to protect Critical Assets</td>
<td>Encrypted In-Band Management</td>
</tr>
<tr>
<td>NERC-CIP-005</td>
<td>Electronic Security Perimeter(s)</td>
<td>Identify and Protection of the Electronic Security Perimeter for all Critical Assets including access points</td>
<td>Encrypt All Data</td>
</tr>
<tr>
<td>NERC-CIP-007</td>
<td>Systems Security Management</td>
<td>Establish, Implement and Document Technical Procedural controls that enforce access authentication to all Assets within the Electronic Security Perimeter</td>
<td>Multi-level password protection at all control levels, encryption and secure out-of-band management</td>
</tr>
<tr>
<td>NERC-CIP-009</td>
<td>Recovery Plans for Critical Assets</td>
<td>Establish and Implement Business Continuity and Disaster Recovery techniques and practices</td>
<td>Fail-over, backup solutions and Mobile-quick deploy solutions</td>
</tr>
</tbody>
</table>

**Note:** All NERC CIP Standards 002-009 are Subject to Audit and Enforceable beginning July 1, 2009
NERC Compliance - Securing the Environment

- VPN based Security through Encryption; AES-256 or 3DES
- Multi-level password, event logging and SYSLOG.
- Remote Management via SNMP
  - Device management and alarming
- Disaster recovery through redundant data paths
  - Cellular & VSAT offer diverse wireless data paths
  - Auto-Failover and Recovery between data centers
  - Quick Deploy and Fly-away systems
- Mobile Asset Management; GPS Based Geo-Fencing
Critical Asset - Legacy Support

- Leveraging Existing Network Devices
  - RTUs
  - Meters

- Retaining the serial interface
  - Harboring assets to reduce cost of compliance

- Serial Protocol support - Terminal Server
  - Encapsulation
  - Spoofing - Conversion
    - Latency - Polled protocols
  - Common Serial Protocols in Utilities
    - DNP, CDC, Conitel, Modbus, PGNE, Async-terminal server, Frame
Network Management - Operational Support

- Migration to on-line and on-demand platform
- Simple to use interface
  - Common readily available with technicians
  - Simplified training
- Easy deployment
  - Tracking installations in large scale rollouts
- Broadcast Alarms - Failures
  - Centralized management
- System Awareness
  - Load management
  - Smart distribution
- Security
- Redundancy – Automatic Fail-over
Terrestrial Networking

- Solutions typically found in the Utility
  - Fiber SONET Rings – high-speed - OC3 / 48
  - T1/Frame Relay/MPLS - mid-level speed
  - Dial/DDS/Multi-drop-slow speed

- Typical Utility will have many forms deployed

- No limit to applications, just bandwidth to support requirements

- Can lead to lengthy lead times for installation
  - Mass deployments can be difficult to manage

- Susceptible to localized damage; backhoe failure, etc
  - Lengthy repair cycle
Cellular and LMR Data Networking

- **Cellular Networking - Reliable broadband option**
  - Similar to a standard terrestrial network connection
    - With High-Speed EV-DO & HSDPA transmission rates are over 1Mbps
  - Easily deployed - No antenna pointing, ballast, etc
  - IP Based network
    - Evolving and growing infrastructure
    - Need to convert serial-legacy applications to IP
    - Need to add encryption for secure networking (NERC Compliance)

- **LMR (Land Mobile Radio)**
  - Used widely throughout Utilities for mobile-comm and metering
  - 700MHz; 800-900MHz
    - Licensed and unlicensed
VSAT Networking

- Excellent broadband option, consistent performer, available everywhere

- Domestically there are Four key providers of Satellite Services
  - HNS, Spacenet, iDirect and ViaSat

- Frequency bands typically found in the USA are Ku, Ka and C
  - Ku band commonly used for the past 20 years
    - Blanket licensing is based on total EIRP
  - Ka operates at higher frequencies utilizing spot beams, can be load sensitive
  - C band requires more power and larger antenna
    - Requires individual site licensing and management, subject to interference

- VSAT networks are IP based
  - Need to address serial and legacy devices to interface to VSAT
  - All VSAT providers have some internal TCP acceleration (PEP)
    - IPSec could affect applications performance
IP Routing and Non-Routable Protocols

**Routable Protocols (IP)**

- **Router Information Protocol (RIP)**
  - Point to Point IP routing
- **Open Shortest Path First (OSPF)**
  - Alt path routing w/in IP for Mesh
- **Border Gateway Protocol (BGP)**
  - Updated routing tables are ‘learned’
  - Stability concerns with routing table
- **Virtual Private Network (VPN)**
  - Secured Data 3DES or AES
  - Security through multiple layers including authentication keys, passwords
- **Secure Shell (SSH)**
  - Security through digital signature

**Non-Routable Protocol**

- **Frame Relay**
  - Point to point circuits
- **Multiprotocol Label Switching (MPLS)**
  - Point to point IP based circuits
- **DataConnect**
  - Cellular Private IP circuits
- **Drawback - auto-failover to meet NERC CIP-009**
Industry Solutions
Multi-purpose Communications Infrastructure
Existing Utility - Multi-com Path

Remote Sites
Meter or RTU

Radio

TELCO

Leased Lines

Modem Bank

Host FEP

Headquarters
Requirements - Hardened Routers

Core Product Check List

- **10/100 Ethernet ports**
  - 2 Independent ports
  - LAN Switch

- **Serial to IP - Conversion**
  - 2 to 6 Independent Serial ports
  - Protocol support w/Spoofing

- **Integrated Cellular Modem**
  - For Failover or Out-of-Band Management

- **VPN w/AES 256 Support (Multiple tunnels)**

- **AC or DC (12/24/48/130vdc) input supply**
  - Redundant supplies

- **Temperature Hardened**
  - -40° to +85° C

Other Features

- **Universal Expansion Slot:**
  - 56/64 kbps DSU port, Frame Relay
  - Single T1/E1 CSU/DSU
  - Fiber interface
  - DMZ Ethernet port

- **Routing Functions**
  - QoS (Quality of Service)
  - CoS (Cost of Service)

- **GPS for Critical Asset Management**

- **Communication Path Diversity**

- **Host and Central Site Solutions**
  - Migration plan for Legacy to IP
  - Automatic fail-over between data centers
  - Able to accept many network interfaces
Bridged Technology Conversion

Satellite Service Provider Hub
- Redundant Baseband Equipment
  - Satellite Hub
  - Firewall

Customer HQ
- VSR-1200
- Host-DVR
- Server
- RDU
- FEP

SLE Tunnel(s)
- IPsec-Tunnel(s)
- SLE VPN

Supv Control
- Serial
- VSAT Only

T1/MPLS
- T1 or MPLS with VSAT Failover
- Integrated T1/modem
- Serial
- VSAT and Cell Cost based Routing

IP (Internet)
- IPSec-VPN (AES)
- IPSec-VPN (AES)
- IPSec-VPN (AES)
Redundant Host - Multiple Tunnels

Customer HQ

Backup Data Center

Server

IPSec Tunnel(s)

Host-DVR

Server

Serial FEP

IP (Internet)

Serial

Integrated T1/Modem

T1 or MPLS with VSAT Failover

Serial

Integrated T1/Modem

VSAT and Cell Cost based Routing

Serial

Integrated T1/Modem

T1 or MPLS with VSAT Failover

Serial

Integrated T1/Modem

VSAT and Cell Cost based Routing
Summary

- Cost containment
- Networking Technologies
  - Terrestrial
  - Wireless/Cellular/VSAT
- NERC-CIP Standards
  - 003, 005, 007 and 009
- Solutions that include existing resources
  - Keeping legacy devices
  - Adding encryption, redundancy, reliability
- Common sourced management
FAQ

- **How to contain networking costs?**
  - When transitioning current analog terrestrial service to high-speed IP service, costs of devices and lower MRC circuit costs have a typical ROI of 7-14 months.

- **How do I apply various Network Technologies?**
  - Some service providers offer integrated – converged solutions with all networks solutions under one roof. Based upon site demographics, the best solution may include multiple network technologies.

- **How can I keep my critical asset (RTU or Meter) and meet NERC standards plus migrate to newer IP technologies?**
  - By obtaining a product that spoofs the existing serial protocol to IP and securing the data with VPN you can have improved ROI by avoiding RTU or meter upgrades.

- **How can I best manage my critical assets?**
  - Through the use of in-band or out-of-band access methods you can safely and securely manage devices from your central office and potentially avoid a dispatch further improving the ROI margins.
About Encore Networks

- Encore Networks manufactures environmentally hardened routers (BANDIT™) designed for harsh network environments.

- BANDIT™ routers ensure reliable, secure, high throughput SCADA data directly to terrestrial, cellular or VSAT networks.

- Encore Networks supports many legacy serial protocols and routing standards for secure, worry-free IP networking.

- Active Member of the following:
  - Utilities Telecom Council {www.UTC.org}
    - Associate Member and webinar presenter
  - Virtual Private Network Consortium {www.VPNC.org}
    - A ‘trusted’ VPN solution
  - ZigBee Alliance {www.zigbee.org}

- Presenter, Matt Girard, Sr. Director of Market Development
  - {mgirard@encorenetworks.com}; (703)318-4360
<table>
<thead>
<tr>
<th>NERC CIP Category</th>
<th>CIP Codes</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access and Passwords</td>
<td>CIP-004-1, CIP-005-1</td>
<td>- Individual user accounts and passwords</td>
</tr>
<tr>
<td></td>
<td>CIP-007-1</td>
<td>- Required strong passwords, expiring passwords, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Digital security packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Strong Two-factor authentication – IKE Support</td>
</tr>
<tr>
<td>Access Control Management</td>
<td>CIP-003-1, CIP-005-1</td>
<td>- Centralized administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Individual administration accounts and passwords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Comprehensive reports: lists of users, assets, access points, etc.</td>
</tr>
<tr>
<td>Electronic Security Perimeter</td>
<td>CIP-005-1, CIP-007-1</td>
<td>- Secure Access Points</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Access denied by default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Technical Control Methods (2-factor authentication, etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Electronic access monitoring and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Appropriate use banners</td>
</tr>
<tr>
<td>Network / Routing Security</td>
<td>CIP-005-1, CIP-007-1</td>
<td>- Enable/Disable Ethernet Ports / Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Firewall / VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IP Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 802.1x Port Security / 802.1Q VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Intrusion Detection System/Denial of Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- AES256 or 3DES Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Selective Layer Encryption (SLE) for VSAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Programmable changing of Security Keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SNMP guarantee traps</td>
</tr>
<tr>
<td>Dial-up Security</td>
<td>CIP-005-1</td>
<td>- Secure dial-up modem access control, monitoring and logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VPN Cellular access for failover</td>
</tr>
<tr>
<td>Logs, Reports and Audit Resources</td>
<td>CIP-003-1, CIP-004-1</td>
<td>- Comprehensive reports</td>
</tr>
<tr>
<td></td>
<td>CIP-005-1, CIP-007-1</td>
<td>- Detailed access logs with user, port and connection information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- User, Administrator and Asset and Access Point lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NERC CIP Auto Audit report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cyber incident reports</td>
</tr>
<tr>
<td>Employee termination / User rights revocation</td>
<td>CIP-004</td>
<td>- Account / security credential expiration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Administrator initiated user rights revocation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Suspended user accounts</td>
</tr>
<tr>
<td>Alerts and Notifications</td>
<td>CIP-005, CIP-007</td>
<td>- Configurable system alert email messages (SNMP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Unauthorized access attempt notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- System lockout / system error notification</td>
</tr>
<tr>
<td>Security Patch Management</td>
<td>CIP-007</td>
<td>- Published Security Patch scrubs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remote upgrades and auto-update</td>
</tr>
<tr>
<td>Malicious Software Prevention</td>
<td>CIP-007-1</td>
<td>- Encrypted operating system</td>
</tr>
<tr>
<td>System Recovery</td>
<td>CIP-009</td>
<td>- Multi-master, multicast support for Serial SCADA applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Resilient networking w. Cellular technologies primary/backup, with VRRP support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Two code &amp; configuration regions</td>
</tr>
</tbody>
</table>