NAVIGANT
RESEARCH

Smart Grid Communications Security

What are utilities really doing?

21 October 2013

Bob Lockhart
Research Director

Introduction

Navigant Research provides in-depth analysis of global clean technology markets.

The team's research methodology combines supply-side industry analysis, end-user primary research and demand assessment, and deep examination of technology trends to provide a comprehensive view of the Smart Energy ecosystem.

Sector Focus:

Smart Energy
Smart Utilities
Smart Transportation
Smart Industry
Smart Buildings

Research Services:

Research Reports

Subscription Advisory Services

Consulting & Custom Research

- Go-To-Market Strategy
- Custom Market Analysis
- Market Sizing & Forecasts
- Primary Research
- Technology Evaluation
- Commercial Due Diligence
- Competitive Benchmarking
- Strategic Advisory Sessions

Research Services

SMART ENERGY

- Solar Energy
- Wind Energy
- Emerging Renewables
- Biofuels
- Biopower
- Energy Storage
- Advanced Batteries
- Fuel Cells
- Distributed Generation
- Microgrids

SMART UTILITIES

- Smart Meters
- Transmission Systems
- Distribution Optimization
- Home Energy Management
- Utility Data Analytics
- Utility Communication Networks
- Smart Grid Technologies
- Smart Grid Global Analysis
- Utility Innovations

SMART INDUSTRY

- Demand Response
- Smart Cities
- Industrial Innovations

SMART TRANSPORTATION

- Electric Vehicles
- Light Electric Vehicles
- Natural Gas Vehicles
- Commercial Vehicle Innovations
- Advanced Transportation Technologies

SMART BUILDINGS

- Building Energy Management
- Building Automation Systems
- Energy Efficient Lighting
- Smart Building Technologies
- Green Buildings

NAVIGANT RESEARCH

Quick Background

NAVIGANT
RESEARCH

Where are Utilities Coming From?

- Grid Optimization
- Customer Engagement
- Financial Performance
- Example: Data Analytics KPIs
  - Increased Revenue
  - Decreased Headcount
- Business people make business decisions (funding)

Enterprise Security v Control Security

Enterprise Network

- Confidentiality
- Integrity
- Availability
- Infrastructure data enough

Control Network

- Safety
- Reliability
- Integrity
- Need application data

What is the #1 Cyber Security problem? Asked 33 People, Got 26 Answers

- Too much embedded Linux (3x)
- Legacy protocols (2x)
- Defenseless legacy assets (another 50 years)
- Explosion of endpoints (2x)
- Explosion of data
- Adding too much IT to Distribution Grids
- No cyber security standards – indecisive
- Data integrity for control devices
- Lack of consensus (really?)

What is Installed?
Lots of Good Stuff…

- Ruggedized devices
- Two-factor authentication
- ICS-Aware Network Security
- Logical network partitioning
- Bump-in-the-wire
- Control network isolation – including data diodes
- Application Whitelisting & Antivirus
- Embedded Device Encryption
- Data Encryption – at rest / in motion

And the result?

Current State of Security

NAVIGANT
RESEARCH

Nothing forces a utility to be secure

- Most utilities budget to what is legally required
- NERC CIP is not a security standard
  - Bright line >= 100kV (MV/LV out of scope)
  - "NERC Compliance Officer" jobs can require *Juris Doctor*
  - Utilities uninstall IP… non-routable protocols outside CIP scope
- NISTIR 7628 Series very good but not enforceable
- Security is off the hype cycle – but still barely implemented
- "We haven't had an OMG moment yet"
- Still a hero culture

It ain't easy

- One meter can have 4 unique key pairs
  - Encryption works but key management is a challenge
  - DR Event right after key rotation… !
- Substation on a pole – UK
- Event correlation at substations
- AMI/DA Integration… pick a layer, any layer
  - Physical layer
  - Back-end data-only integration
- All technologies can be attacked
  - “No one should feel comfort because of their chosen physical layer”

There are barriers to success

- Many solutions rely upon unlicensed spectra
  - FCC on Progeny: Tough noogies
- AMI vendor assessed 20 deployments of its system
  - *None* had encryption enabled on the meters.
- Many serial devices in control networks
  - They are *still* being purchased today – service life in decades
  - Cannot deploy security on-board
  - Bump-in-the-wire… be careful about added latency
- Most attacks are against the supply side, not endpoints
  - Security “researchers” stopped attacking meters 3 years ago

This is progress?

- Mobile Workforce Applications add new attack vectors
- Some utilities use VPN as their backup SCADA comms
- Many AMI systems use a public network
  - 1M GPRS meters in Holland… war driving?
- Siloed solutions increase linkages, and thus attack vectors
  - EMS, OMS, MWF, GIS, …
- Firmware backdoors – where are the processors made?
- “No OMG moments yet so everything must be fine”

A few important things to do

- Consensus: IP will rule
  - Other protocols become a liability – handcuffs / limited options
  - But how is IP deployed… ???
- Application level security is critical
  - Unlike IT – do not just look at infrastructure layers
  - Do not allow illogical or malicious commands
  - Requires specific Operational knowledge (not a firewall)
- NIST SP800-82 is wonderful
- Processes and deployments, not only technology
- Architecture is key (Neil…)

Contact Us

MAIN OFFICE
1320 Pearl Street, Suite 300
Boulder, CO 80302

+1.303.997.7609

WORLDWIDE OFFICES

United States:	Boulder, Colorado Washington, D.C.
Europe:	London, United Kingdom
Asia Pacific:	Seoul, South Korea

General information: research-info@navigant.com

Me: bob.lockhart@navigant.com

NAVIGANT RESEARCH