Grid-Interop™

The Growing Need for Cyber Security in Smart Grid Networks

#GridInterop

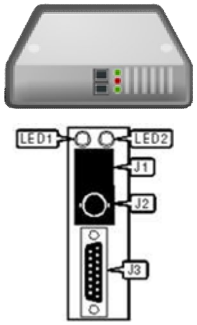
Grid-Interop 2011

Advanced Distribution Systems

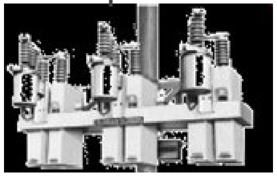
New Security & Operations Needs

Wireless Substation Computers

SCADA Bridges/Converters



Automated Switched Cap Banks



Automated Sectionalizers & Switches

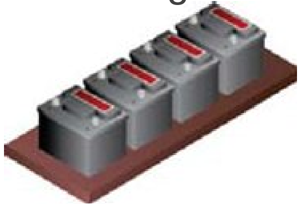
Smart Transformers (Regulators, Sensors, Meters)

FIELD AREA NETWORKS

Wind Generation

PV Generation

Community Storage



Wireless Line Sensors & Feeder Metering

EV Charge Management

Direct Load Control

- **Distributed Intelligence**
- **Advanced Communications**
- **Remote Operations**
- **Security Monitoring, Protection, Controls**

Emerging Field Area Networks

Challenges to Address

- Traditional SCADA supplemented by highly distributed and numerous sensors and controls
  - Tightly integrated, high density embedded field hardware
- Wireless communications are predominate solution
- Multiple wireless technologies with different network topologies and deployment strategies
  - Proprietary Private Networks (open 900 MHz and licensed bands)
  - Cellular Data
  - “Industrial” WiFi Solutions
  - WiMax
- Typical network penetration and vulnerability assessment & intrusion detection tools are not applicable
- Utilities have limited visibility into field area networks. Needs include:
  - Situational Awareness
  - Diagnostics
  - Network Performance Management
  - Intrusion Detection
  - Modeling Tools
  - Network Optimization

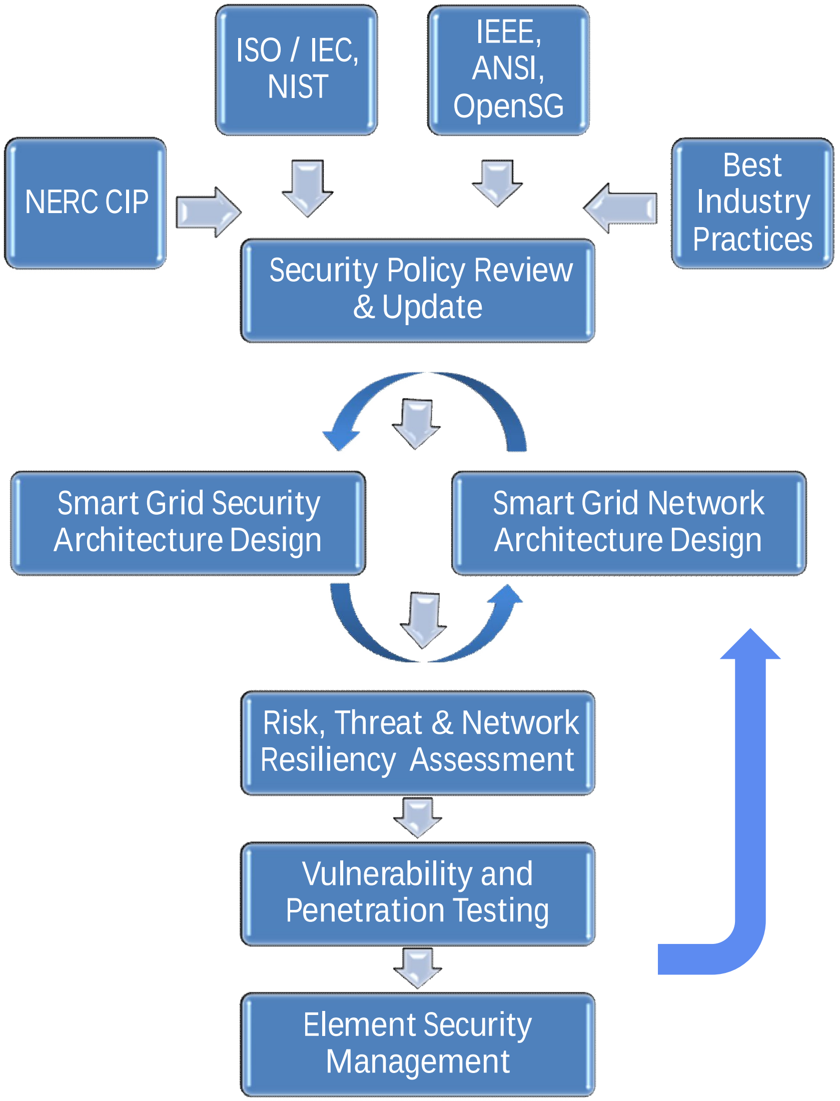
Example Security Concerns

- Disabling power in a local area or at a specific address
- Forging or altering data for consumption and generation metering
- Preserving the privacy of customer data
- Maliciously degrading power quality
- Making unauthorized changes to circuit connections
- Creating large fluctuations in power load
- Losing complete control of utility equipment
- Denial of service (e.g., making automatic restoration equipment ineffective/unresponsive)
- Maliciously influencing utility operations through compromised equipment or sensor data
- Maliciously manipulating electric vehicle charging
- Damaging utility infrastructure
- Compromising an interconnected energy services company (e.g., AMI, DR, IPP)
- Protecting supply chain from cyber security threats

A Smart Grid Security Model

Building In Smart Grid Security

- Smart Grid is an opportunity to plan top-down security approach
- Technology Introduction Process
  - Need to factor in vendor security architecture (current & future)
- Business factors, availability of standards, and technology maturity will also alter the approach
- Supply Chain Management



ISO / IEC, NIST

IEEE, ANSI, OpenSG

NERC CIP

Best Industry Practices

Security Policy Review & Update

Smart Grid Security Architecture Design

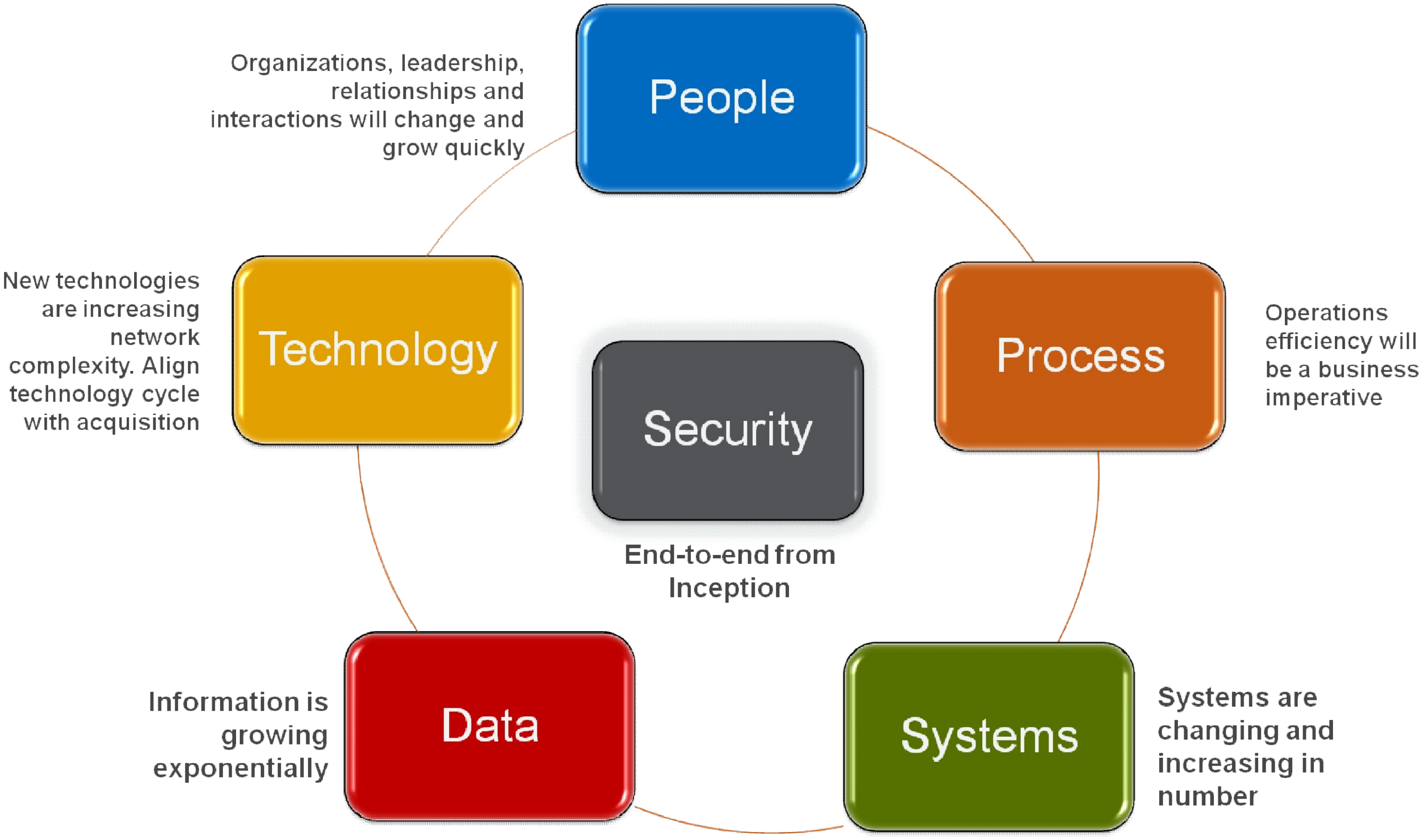
Smart Grid Network Architecture Design

Risk, Threat & Network Resiliency Assessment

Vulnerability and Penetration Testing

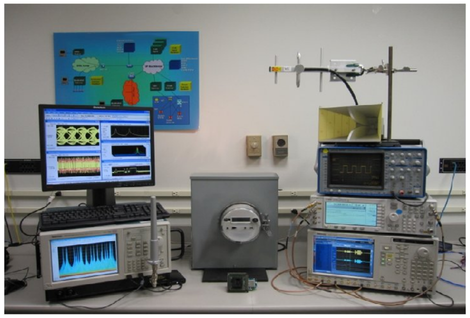
Element Security Management

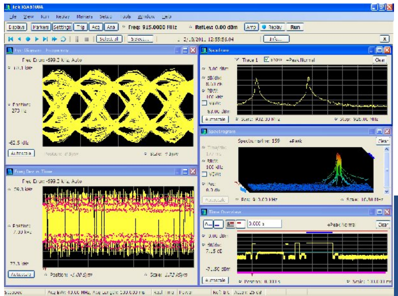
Take a Holistic Approach to Security


Organizations, leadership, relationships and interactions will change and grow quickly
People
Operations efficiency will be a business imperative
Process
New technologies are increasing network complexity. Align technology cycle with acquisition
Technology
Security
End-to-end from Inception
Information is growing exponentially
Data
Systems
Systems are changing and increasing in number

Field Area Network Security Solutions Needed

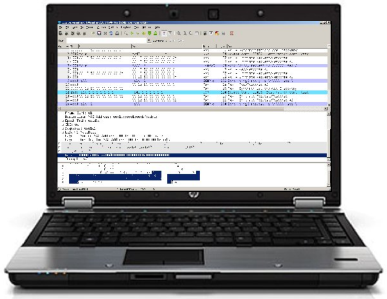
- FAN Protocol Analysis Tool:
    - Probe-based traffic monitoring and analysis tool
    - Visibility into FAN traffic flows, packet exchanges among nodes
    - Multi-Channel Packet capture & decoding
    - Packet Dissectors to permit decomposition of captured traffic through several protocol layers
    - WiFi capability
    - Support IPv4, IPv6 and other proprietary and standards-based protocols
- Benefits:
    - Monitor and inspect packet contents (security exchanges)
    - Assess network health
    - Diagnostic tool for Field Technicians & remote maintenance





Field Area Network Security Solutions Needed

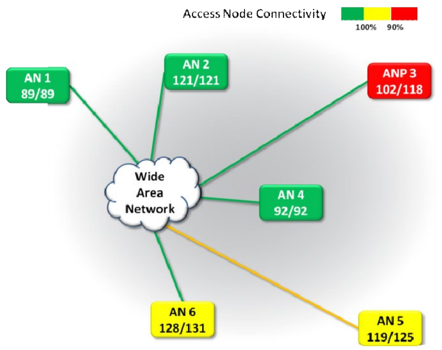
- FAN Wireless Intrusion Detection System:
  - Scalable, probe-based system
  - Distributed intrusion detection intelligence and centralized storage
  - Rule-based intrusion detection engine
    - Flexible triggers, rules, signatures to detect anomalies and potential malicious events
  - Real-time traffic collection and network health monitoring
  - Real-time and post-capture intrusion detection analysis
  - Diagnostic tool, (e.g., inject traffic through alternative network means)

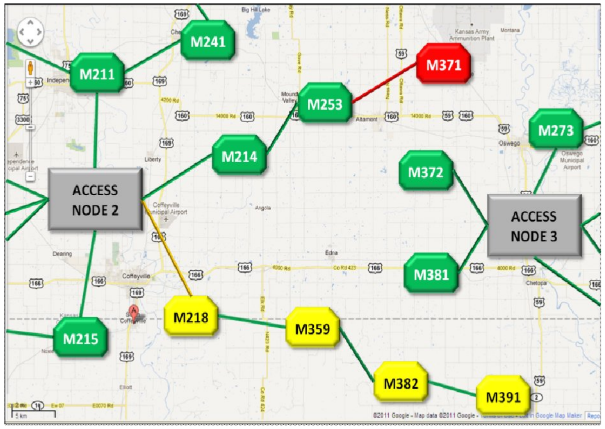


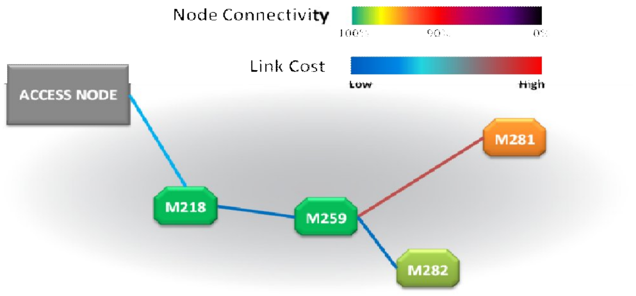
- Benefits:
  - Extend existing IDS capabilities into FAN – monitor FAN for malicious activities or policy violations
  - Operate independent of FAN components

Field Area Network Security Solutions Needed
Visibility into the FAN and its uses

- Operations
  - Current view of network topology and routing
  - Network performance (packet errors, latency, node utilization)
  - Security Operations
  - Mitigating supply chain threat
- Diagnostics
  - Diagnosing problems with new technology
  - Communication system faults
  - Comparison of current network with baseline & historical snapshots
- Engineering
  - Dynamic routing performance
  - Understanding Traffic Patterns
  - Design vs. as-implemented comparison
  - RF performance analysis
  - Planning/Traffic Scheduling
  - Enforcing vendor SLAs







In Conclusion

State of Security in the Smart Grid

- Utilities are being asked to emerge from a “culture of compliance” to a new “culture of cyber responsibility”
  - Compliance with NERC CIP does not mean your network is secure – it is a bare minimum requirement for many
  - Many utilities struggling with OT security as both a science and an art (OT network isolation disappearing)
- Mitigation of Supply Chain Threats for Cyber Security is only now being recognized
- Smart Grid Security is not a one time event – it will evolve with the Smart Grid over the next decade, initially with an internal focus and eventually with an external focus
- Largely due to urgency in stimulus funds, many utilities deployed without the time to define a Smart Grid security architecture, update security policies, deploy new security capabilities
- FAN Situational Awareness is growing need and concern
  - FAN Protocol Analysis tools
  - Extending Intrusion Detection Systems into FAN environments
  - FAN Visibility tools