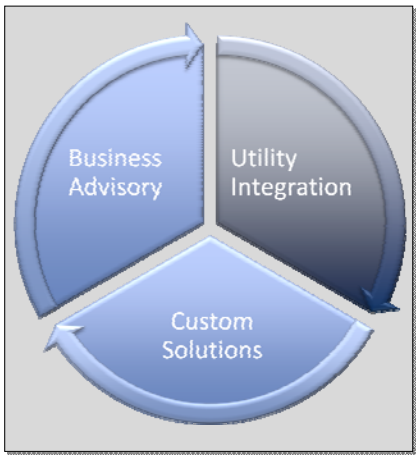
When Should the NERC CIP be Applied to Smart Grid Projects?

Tobias Whitney
The Structure Group
tobias.whitney@thestructuregroup.com
314-422-7050

Introductions - *The Structure Group*

The Structure Group is a leading provider of business advisory, enterprise integration, and custom solutions to energy & utility companies…



Business Advisory

- Single Industry Focus - Energy
- Deep Domain Expertise
- Real-world Experience
- At fore-front of industry issues

Utility Integration

- World-class integration capabilities
- Extensive vendor partnerships
- Functional experts
- Capabilities in:
  - Operations - GMS, DMS, EMS, SCADA
  - ETRM – Allegro, TriplePoint, OpenLink
  - Asset Management – Maximo, Passport
  - Smart Grid – AMI/MDM, DRMS and DA

Custom Solutions

- Houston-based development team
- Custom application development
- Hosting / Maintenance capabilities
- Reusable solutions

Agenda

Overview of Smart Grid Functions

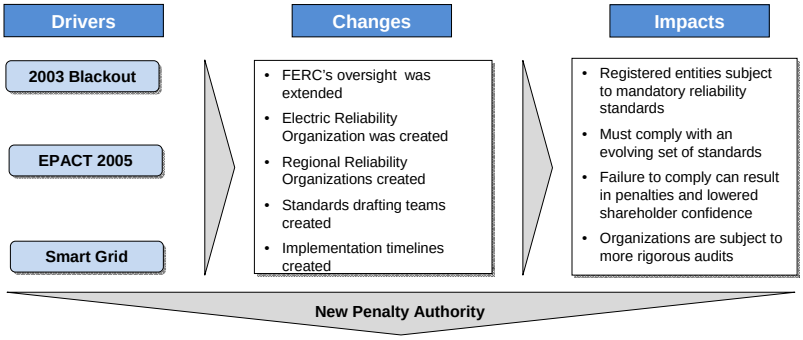
Security Implications and Risks

- Meter to the Premise
- Wide Area Wireless Network
- Distribution Automation & Substation Connectivity
- Control Center Integration
- Website Security

NERC CIP vs. Smart Grid

A New Regulatory Era

Industry Change Drivers



	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

Compliance Challenges
The Compliance Lifecycle

The industry is quickly retooling to meet the demands of FERC/NERC compliance…

The Compliance Lifecycle

Managing Compliance

- ***How do I integrate my program across business units?***
- ***How to I gain visibility into the health of my compliance program?***
- **How do I proactively address compliance issues?**
- ***How do I ensure my processes are repeatable ?***
- **How do I automate my compliance workflow?**
- **How do I measure compliance?**
- **How do I ensure my program stands the test of time?**

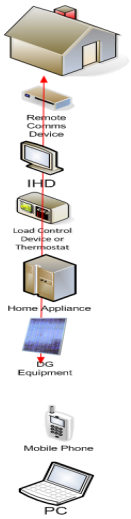
Most started with understanding and assessing compliance. Many **have *proved compliance at a point in time via an audit.* As a result, most appreciate the complexity of managing compliance…**

Smart Grid Overview

Smart Grid will increase the amount of operational and customer data. New, but viable technologies will be used such as:

- Home Area Network and in home devices (home displays and controllable thermostats)
- Smart Meter
- Substation/Distribution Automation
- RF/Wireless Network Communication
- AMI Head End
- Meter Data Mgt System
- Distribution Mgt System

Security has been evaluated for each technology and new operational processes will be introduced



Functional Overview
Customer Solutions

Intelligent Home Displays, Smart Thermostats

- To provide timely and available system data
- To ensure the authenticity of pricing signals to customer initiated load management devices resources

Customer Web Portal

- To validate the authenticity of users accessing the portal
- To provide timely energy consumption and billing data
- To provide users the ability to manage energy profile or change their programmable set points remotely
- To present accurate records of demand response activity

Functional Overview
Operational Solutions

Distribution Automation

- To maintain the integrity of analog values, status changes and sequence of event data generated by field devices such as sectionalizers, load tap changers, distributed IEDS and VAR management
- To maintain the accuracy and non-repudiation of automated feeder sectionalizing and restoration configurations

Remote Disconnect

- To protect customer accounts to ensure billing and payment data is up to date and correct
- To restrict unauthorized command signals and ensure that customer service is maintained
- To provide the customer availability to their respective account(s) within customer payment services

Functional Overview
Reliability Solutions

Demand Response Mgt, Distributed Generation

- **To restrict unauthorized command signals to load management resources**
- **To protect utility assets from unauthorized physical or electronic compromise**
- **To maintain availability of two-way metering data**
- **To transmit authenticated command signals to distributed generation resources**

Outage Management

- **To maintain the accuracy and timeliness of outage information provided by smart meters**
- **To maintain the accuracy and availability of EMS/DMS data provided to outage management**
- **To protect the data stored and presented to GIS related functions**

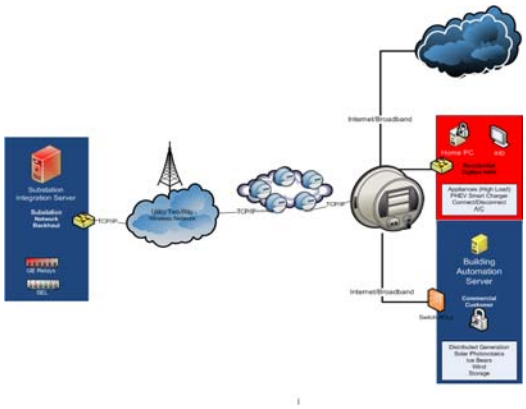
Architecture 1
Utility to Customer Premise

Key Technologies:

- Smart Meter
- Intelligent Home Displays
- Programmable Thermostats
- ZigBee Home Area Network

A security approach addresses the threat as follows:

- Multiple encryption standards will be used to protect customer and utility meter data
- Customer Privacy Requirements will be addressed
- Alarm tampers for physical access to Smart Meters
- Utilize industry standard public key infrastructure to authenticate meter control signals and data such as 256 Bit Elliptic Curve Cryptography



Relevant Standards:
- NIST Special Publication (SP) 800-53, NIST SP 800-82
- AMI-SEC Smart Grid Security Guidelines

Architecture 2

Meter and Distribution Automation Network (AMI Network)

Key Technologies:

- Substation Integration Server
- Intelligent Electronic Devices
- AMI two-way radio towers
- IP enabled relays

A security approach addresses the threat as follows:

- Encryption of all end-point device communication on AMI network. The following technologies will be used to secure the storage and transmission of meter data:
  - 128 bit AES Encryption
  - 256 EC Encryption
  - Digital Signatures
- The physical location of gatekeeper or collector devices will be within a physically secured perimeter or within a utility control location such as a substation
- All devices will possess physical tamper detection and alarm when local access is obtained or when the device has been taken off-line
- Each device will possess intrusion detection/protection security system to identify if malicious activity is taking place within the local area of the device
- The device will be able to perform traffic filtering to limit non-essential communication

Relevant Standards:
- NERC CIP 002-009
- NIST Special Publication (SP) 800-53, NIST SP 800-82
- AMI-SEC Smart Grid Security Guidelines

Architecture 3

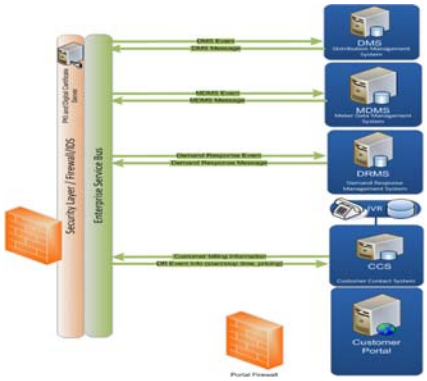
Control Center Integration

Key Technologies:

- Distribution Management System
- Meter Data Management Systems
- Demand Response Management System
- Customer Portal

A security approach addresses:

- Security management consoles should be utilized at head-end equipment to manage the security of meters, collector/gateways and HAN devices. The console should provide a full suite of services to manage:
  - Authentication/Authorization
  - Meter and HAN Registration
  - Intrusion Detection Data
  - Network encryption
  - Data encryption
  - Digital Certificates
  - Network traffic filtering
  - User Administration
  - Auditing and Security Reporting
  - Key Management
- Firewall and intrusion detection systems should be implemented to manage and monitor AMI network interface
- All head-end (AMI network interface) equipment will be deemed critical and will be managed to comply with the NERC Critical Infrastructure Protection Standards



Relevant Standards:
- NERC CIP 002-009
- NIST Special Publication (SP) 800-53, NIST SP 800-82

Architecture 4

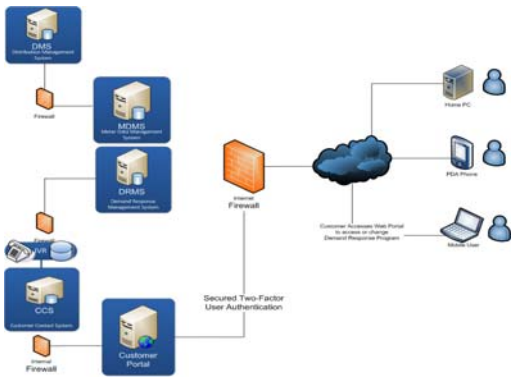
Web Access to Customer Profile Data and Pricing

Key Technologies:

- Web Site
- Customer Portal
- Mobile Technologies
- Demand Response Presentment

A security approach addresses:

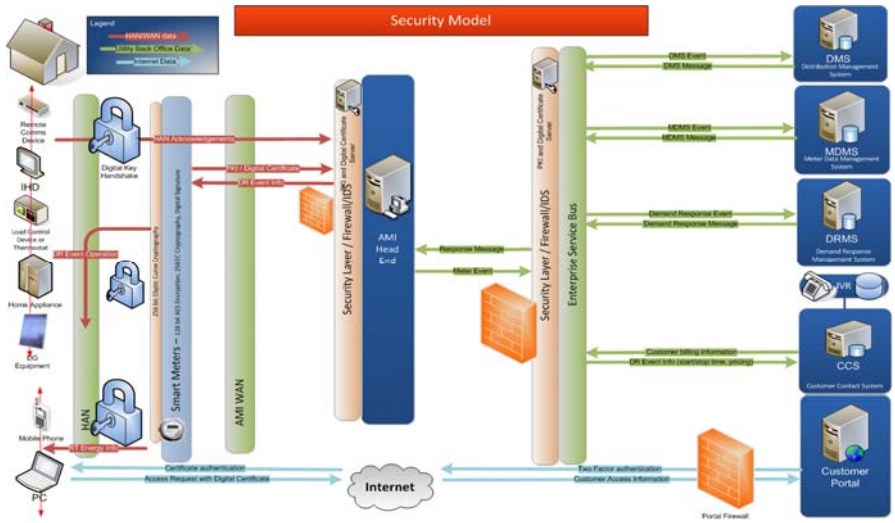
- The infrastructure associated with the web portal will be secured using traditional web applications security standards that will address:
  - Customer privacy requirements
  - Two-factor authentication
  - 3-tiered web application architecture
  - Secured DMZs to limit access between system environments
  - Activity traffic monitoring and firewalls
  - Web site security accreditation



Relevant Standards:

- Sarbanes-Oxley
- Company Security Policy
- COBIT and COSO IT Control Standards

Smart Grid Security Model



Risk-Based Methodology

- NERC Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System
- These Critical Assets are to be identified through the application of a risk-based assessment
- The Risk-Based Methodology should:
  - Define what constitutes “criticality”
  - Clearly communicate how asset lists are developed
  - Identify scoring criteria
  - Provide transparency around how Critical Assets are measured in each category

Risk-Based Methodology

- Assets to consider for Criticality include:
  - Control centers and backup control centers
  - Transmission Substations
  - Generation Resources
  - Systems and Facilities Critical to System Restoration
  - Systems and Facilities Critical to Automatic Load Shedding
  - Special Protection Systems
  - Any Additional Assets that Support Reliable Operation of the Bulk Electric System

Risk-Based Methodology
Sample Illustration

The Guideline Discusses the following Key Grid Components:

- For LSE and DP Registrations:
  - System critical to automatic load shedding supporting the reliability or operability of the BES" as listed in CIP-002-1.
  - "Demand-Side Management (DSM) or Direct Control Load Management (DCLM) that supports the reliability or operability of the BES" which if lost or compromised could create unintended load shedding.
- For GO/GOP Registrations:
  - Under "Essential generation" added generation capacity that is required to serve normal load under normal conditions.
  - Under "Essential for known constraint mitigation" revised thresholds to include:
    - voltage collapse
    - voltage going below the under-voltage load shed points
    - frequency going below the under-frequency load shed points
    - system collapse due to frequency related instability

17

Structure is dedicated to helping our clients address their compliance concerns. For more information on how Structure may be able to help your organization, please contact us:

Structure™

Tobias Whitney
The Structure Group
Tobias.whitney@thestructuregroup.com
314-422-7050