SCE's Phasor Measurement and Grid Stability System

A Discussion of

SCE's General Rate Case Testimony

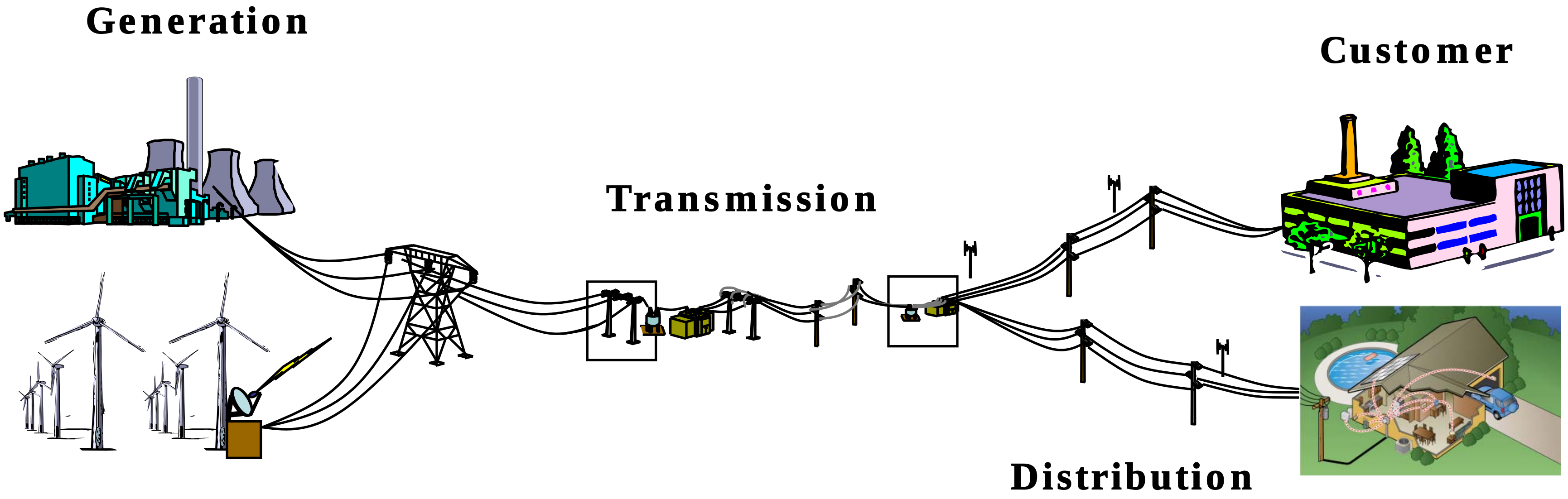
Main Themes of SCE’s Argument

- Managing modern electricity systems is becoming more complex
  - *Operations before and after restructuring*
  - *Market and environmental issues*
- Existing operational tools are inadequate
- Increasing cost and potential for failure
- Synchronized phasor measurement systems basics
- Funding requirements and project management
- Industry and policy support for SPMS

Market and Environmental Realities

- Decreasing capacity margins due to load growth and lack of new transmission infrastructure
- Increasing demand for electricity, reliability and power quality
- Historic difficulty in funding, permitting and siting transmission and distribution facilities
- Certain generating assets are preferable to others

Interoperability from the Generator to the Customer



Generation

Customer

Transmission

Distribution

Existing Operational Tools Are Inadequate

- Operators do not have tools to determine system stress and proximity to instability or potential collapse
  - *Cite the U.S. – Canada Power System outage Task Force Final Report on the August, 14, 2003 Blackout*
- Operators do not have wide area visibility beyond their service territory boundaries
  - *Cite the U.S. – Canada Power System outage Task Force Final Report on the August, 14, 2003 Blackout*

Existing Operational Tools Are Inadequate

- Many entities are collaborating in conducting extensive RD&D into phasor measurement capabilities with positive results
  - *Cite the creation of EIPP and NASPI, DOE- and CEC-funded efforts*
- Deploying base phasor infrastructure and systems may already have a positive NPV for electric service provider customers
  - *Cite the California Energy Commission Phasor Measurement Application Study*

Increasing Cost and Potential for Failure

- The Northeast Blackout impacted over 50 million people, costing about $1 billion per day
  - *Cite FERC Staff Preliminary Assessment of NERC's Proposed Mandatory Reliability Standards*
- Florida blackout causes approximately 3 million people to lose power
- From 1960 to 1996, North America had experienced two system wide outages. From 1996 to 2004, the number has increased to five
  - *Cite SCE General Rate Case*

Additional and Future Benefits

- Operation closer to the margin with exact measurements
- Improvements in power transfer capabilities and contingency response options
- Real-time automation of system reliability and enhancement assets (e.g. SVC and RMR capacitor banks)
- Improved study capabilities for planning and operations

Funding Request and Project Management

- Hardware costs for PDC’s and support equipment - $5 million*
- Software costs, including integration with the energy-management system - $15.5 million*
- Infrastructure upgrades for hardware installations and communications - $9 million
- Other labor costs - $4.5 million*

**Estimates based upon recent EMS project costs*

AMI Security Approach

July 18, 2008

Initial Analysis

- Recognition of the problem
  - *AMI touches every consumer*
  - *AMI is a command and control system*
  - *AMI has millions of nodes*
  - *AMI touches almost every enterprise system*
- Recognition of the state of the industry
  - *Inadequate vendor RFI and RFP response*
  - *No best practices or standards*
  - *TCM confirmed industry delta*

Technology Capability Analysis

AMI Technology Capability Maturity (TCM) Security Framework

Maturity Level	Comprehensive Policy Based Access Controls and Content Labeling	Field Device Attestation and Self Corrective Diagnostics	Virtualized Process and Memory Partitioning	Device integrity monitoring (e.g., software checksum) and reporting	Completely Integrated Security Operations Console	Virtualization for Field Network	Dynamic Key Management (Ad-hoc)	Complete Key Management Services: Generation, Distribution, Negotiation	Secondary Audit and Deterministic Intrusion Detection	Edge Filtering (e.g., Filtering at Premise Gateway)	Cryptographic Extension for Consumer Confidentiality and Authentication	Security Operations Console	Field Tool Authentication	Cross Certified HAN Device Security	AMI Applications integrated with IT Access Controls Systems (e.g., IDM/AD)	Remote Security Upgrades	Cryptographic Confidentiality though Pre-placed Symmetric Keys	Non-Cryptographic Device Confidentiality and Authentication	Local Access Controls	Back-office Integrity Services (e.g., Virus detection)	Firewall based Segmentation of Field and IT assets	Physical Security Measures for Field Assets	Security through Topography and Network Addressing (e.g., NAT)
5	X	X	X	X	X	X	X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X
4				X	X	X	X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X
3								🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟩 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X
2														🟩 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X
1																		🟪 X	🟪 X	🟪 X	🟪 X	🟪 X	🟪 X
0																							🟪 X

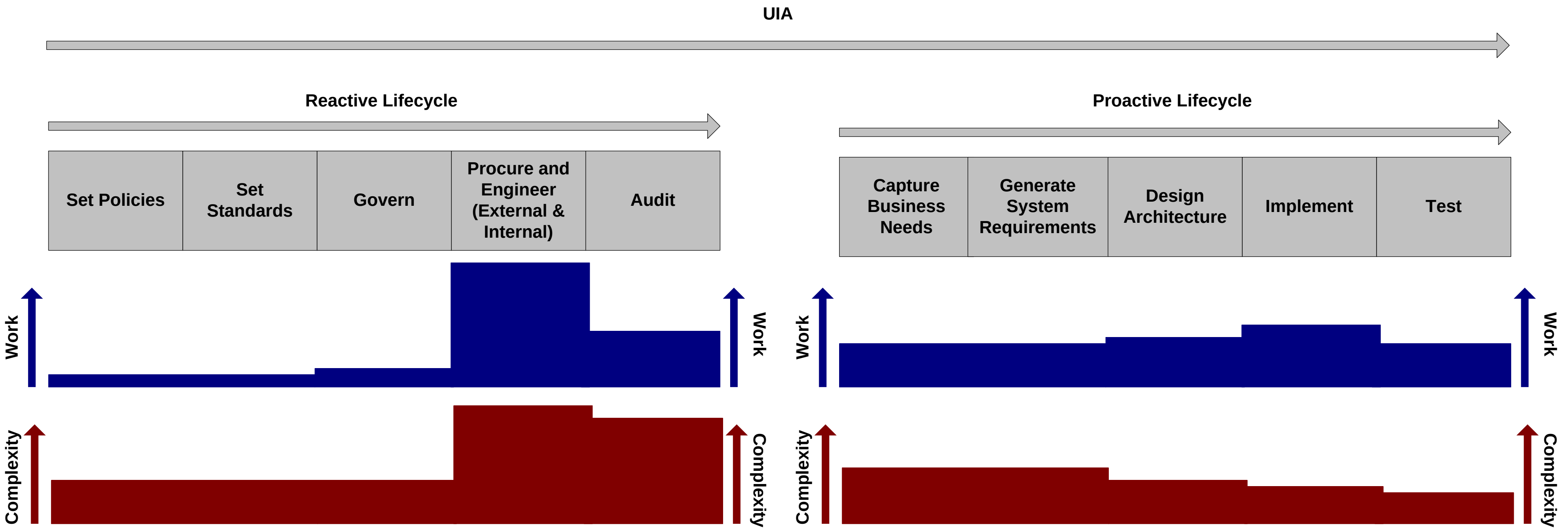
🟪 Release One

🟩 Release Two

Approach

- Frame and Scope the problem
  - *What are we trying to secure?*
  - *What are the constraints?*
  - *What can we reuse?*
  - *What can we borrow from other industries?*
- Approach
  - *Use basic system engineering principles*
    - *Use abstraction for complexity management*
    - *Define requirements*
    - *Decompose requirements and functions*
    - *Allow for performance and constraint tuning*
  - *Tailor for engineering process for security*
    - *Introduce risk driven requirements process*
    - *Introduce concept of robustness*

System Engineering Benefits



UIA

Reactive Lifecycle

Set Policies | Set Standards | Govern | Procure and Engineer (External & Internal) | Audit

Work

Complexity

Proactive Lifecycle

Capture Business Needs | Generate System Requirements | Design Architecture | Implement | Test

Work

Complexity

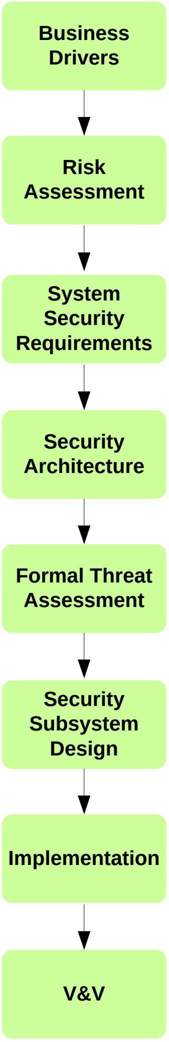
<u>Benefits</u>
- Low staffing requirements during first few lifecycle phases
- Minimal engineering expertise required in early phases (e.g., Policy by management edict)

<u>Risks</u>
- No clear mechanisms for applying technology standards and policies
- Requires a separate audit and assessment phase
- Low confidence in adherence (Comprehensive auditing near impossible)
- Program artifacts are self contained (no reuse)
- Implementations success based on individual contribution

<u>Benefits</u>
- Guarantees business value (all work is aligned to business process automation and business needs
- Strong binding between each lifecycle phase
- Compliance Framework is built-in to the model
- Program implementation risk are reduced significantly
- Program implementers have large body of predecessor work (generates day one value)

<u>Risks</u>
- Engineering expertise required in beginning of lifecycle
- Failures ripple through system

System Security Engineering



Business Drivers

Business Functions (Remote Disconnect, Remote Meter Read)
Regulatory Requirements

Risk Assessment

HAN compromise leads to a compromise of the backhaul network
Creating a DOS at the Collection Engine
Malicious use of an AMI asset by an insider

System Security Requirements

Shall supply a mechanisms which assures the confidentiality of the meter's data while in transit
Shall supply a mechanisms which assures the integrity of the meter's data while in transit

Security Architecture

Defines and Indentify security functions
Organizes security functions

Formal Threat Assessment

Indentify Assets
Define Asset Vulnerabilities
Indentify Threats
Map threats to system domains and assets

Security Subsystem Design

Key Management Subsystem Design
Segmentation and Filtering Subsystem Design
User Access Controls Subsystem Design
Audit Subsystem Design

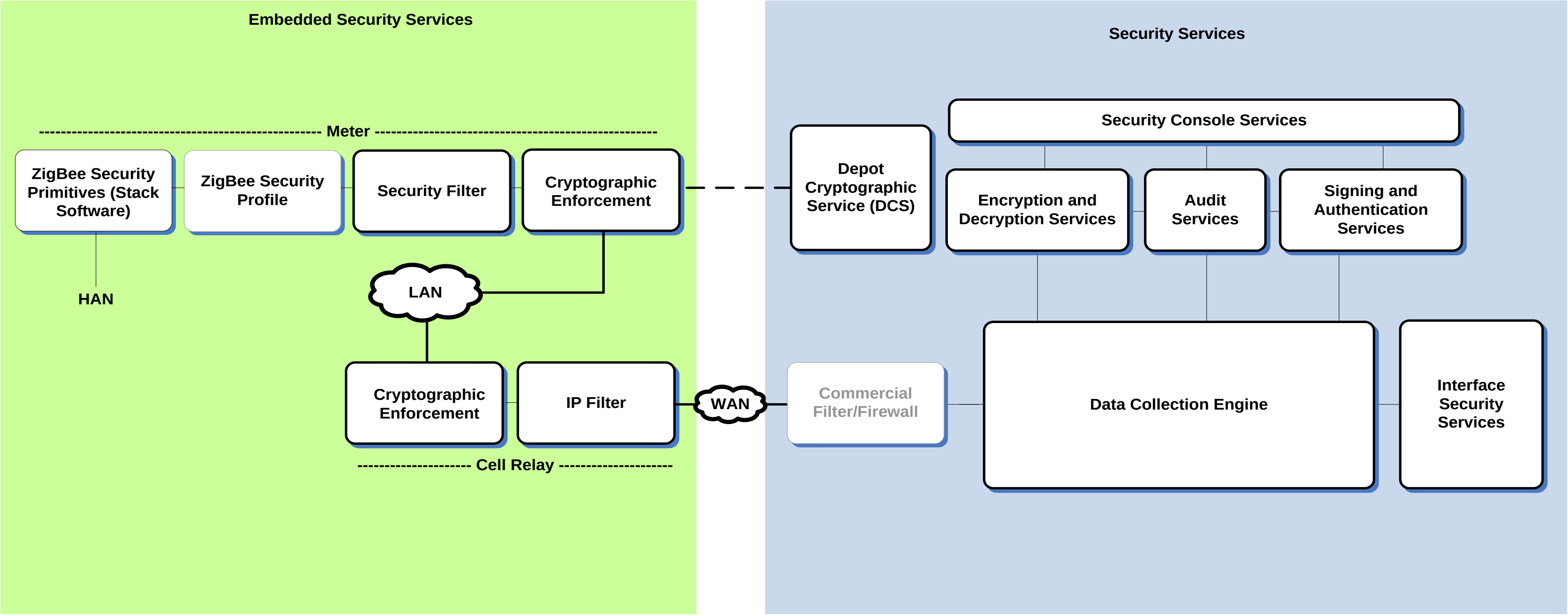
Implementation

Procurement
Development
Configuration

V&V

Validate Requirements
Define Qualification Provisions
Test Procedures
Testing (Internal, Third Party)

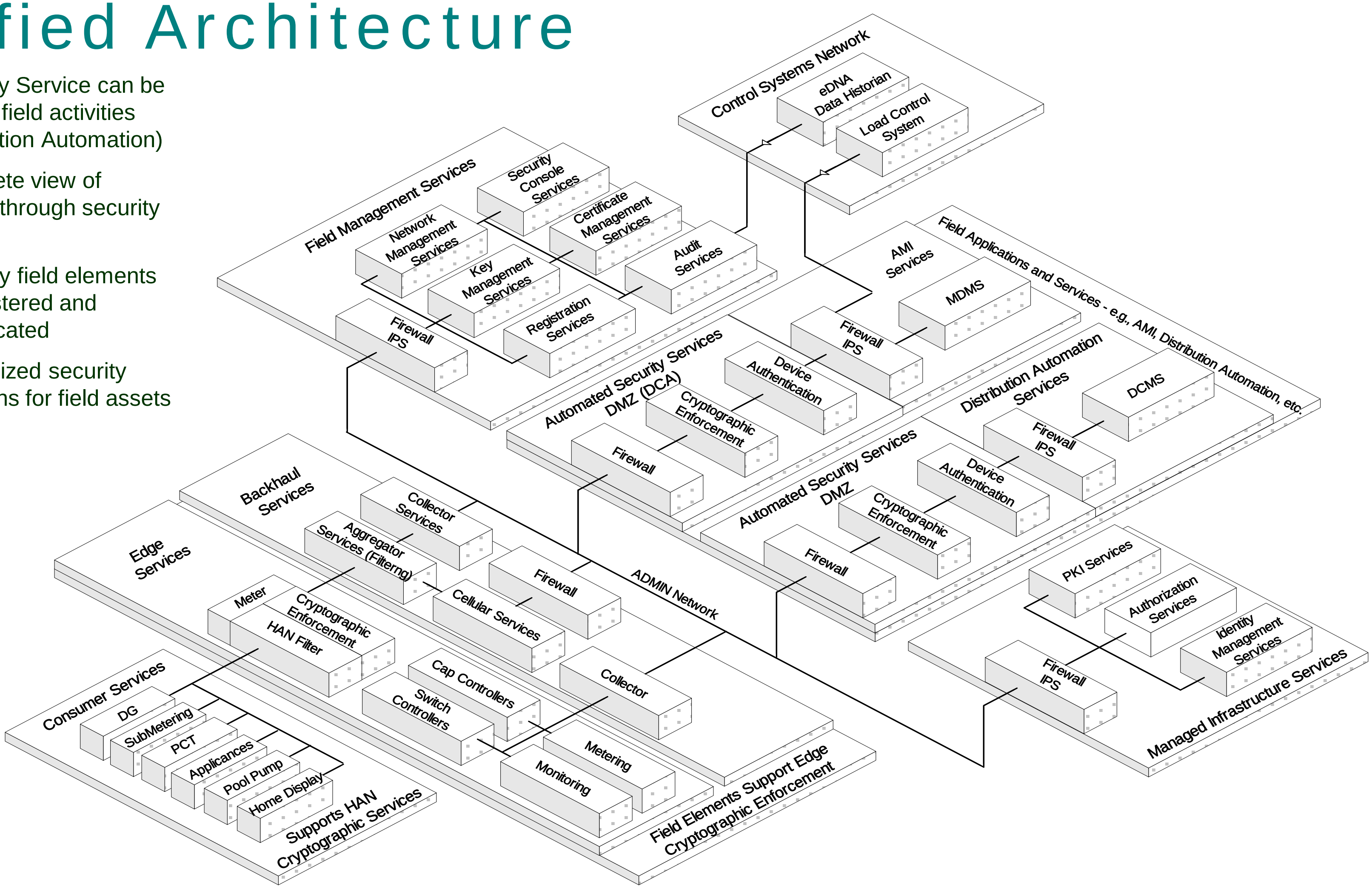
System Security Architecture



Embedded Security Services
Security Services
Meter
ZigBee Security Primitives (Stack Software)
ZigBee Security Profile
Security Filter
Cryptographic Enforcement
HAN
LAN
Cryptographic Enforcement
IP Filter
Cell Relay
WAN
Commercial Filter/Firewall
Depot Cryptographic Service (DCS)
Security Console Services
Encryption and Decryption Services
Audit Services
Signing and Authentication Services
Data Collection Engine
Interface Security Services

Unified Architecture

- Security Service can be used for field activities (Distribution Automation)
- Complete view of network through security console
- All utility field elements are registered and authenticated
- Centralized security operations for field assets


Control Systems Network
eDNA Data Historian
Load Control System
Field Management Services
Security Console Services
Network Management Services
Certificate Management Services
Key Management Services
Audit Services
Registration Services
Firewall IPS
AMI Services
MDMS
Field Applications and Services - e.g., AMI, Distribution Automation, etc.
Firewall IPS
Automated Security Services DMZ (DCA)
Device Authentication
Cryptographic Enforcement
Firewall
Distribution Automation Services
DCMS
Firewall IPS
Automated Security Services DMZ
Device Authentication
Cryptographic Enforcement
Firewall
Backhaul Services
Collector Services
Aggregator Services (Filterng)
Firewall
Cellular Services
ADMIN Network
Edge Services
Meter
Cryptographic Enforcement
HAN Filter
Cap Controllers
Switch Controllers
Collector
Metering
Monitoring
Field Elements Support Edge Cryptographic Enforcement
PKI Services
Authorization Services
Identity Management Services
Firewall IPS
Managed Infrastructure Services
Consumer Services
DG
SubMetering
PCT
Applicances
Pool Pump
Home Display
Supports HAN Cryptographic Services

Back-up slides and drawings

Rate Case presentation

2008 NASPI Task Team Deliverables

- Research Information Task Team database documenting all RD&D activities and publications
- Business Management Task Team white paper on arguments supporting phasor deployment in funding proceedings

SCE Prior to Industry Restructuring

- For nearly a century, SCE planned and operated its system as a vertically-integrated electric utility
- Integrated planning (generation, transmission and distribution) provided for future capacity margin and safe, reliable power delivery
- Integrated operations provided ample means to act quickly and decisively to mitigate system events and economically maintain assets

SCE After Industry Restructuring

- SCE no longer operates a majority of the interconnected generation resources
- Disintegrated planning places decision-making in the hands of many market participants with differing goals and objectives
- Various market participants make operating decisions, based upon entity specific needs

Phasor Measurement System Basics

- SPMS's function by continuously collecting measurements on voltage, current, frequency and phase angle from many points on a system
- Measurements are time-stamped with GPS or other precise time information
- Data is compiled and stored in a computer system for continuous analysis and future study
- Information is displayed for system operators for decision-making

Documents and Entities Supporting the Integration of Phasor Technologies

- Energy Independence and Security Act of 2007
- Energy Policy Act of 2005
- The U.S. Department of Energy (DOE)
- Federal Energy Regulatory Commission (FERC)
- National Electric Reliability Council (NERC)
- California Independent System Operator (CAISO)
- California Energy Commission (CEC)
- Western Electricity Coordinating Council (WECC)
- NASPI and EIPP

Back-up slides and drawings

Security Presentation

Accomplishments

- **Capabilities**
  - ***Patent (AMI Security Methods)***
  - ***System authenticates and manage 30+ million nodes***
  - ***All cryptographic methods are compliant with NIST***
  - ***Security methods are very fast***
  - ***Meters and aggregators have programmable filters***
  - ***System supports a set rich audit services***
- **Industry Leadership**
  - ***Lead several ZigBee Alliance related security activities***
  - ***Working with several academic institutions on next generation security methodologies (e.g., University of Illinois, CalTech, CMU)***
  - ***Designed security for CEC's title-24 Programmable Communicating Thermostats***
  - ***Lead and present at several industry events (e.g., DoE, CEC)***
  - ***Lead several standards activities (IETF, ANSI, IEEE, IEC, UCA)***

Documentation Requirements

AMI Security Documentation

	Field Assets			Data Center Assets		
AMI Security Domains	Home Area Network	Meter	Communications	AMI Network Automated (DCA)	AMI Network Managed (DCA)	AMI Operations (MDMS + Enterprise)
Product Development	OpenHAN (requirements)					
	External Security Engagements (e.g., AMI-SEC artifacts)					
	Internal SCE AMI Security (architecture, requirements, whitepaper, etc.)					
	AMI Security Patent					
	Meter/Communication Vendor Integration (IRS)					
	ZigBee Alliance Security WG Engagement Documentation (architecture, profile, cluster)					
						eMeter Security Integration (IRS)
				Internal SCE Security Workshop		
	Knowledge Domain: Computer Security (COMPUSEC)			Knowledge Domain: Information Technology Security (ITSEC)		
	Knowledge Domain: Communications Security (COMSEC)					
Operations and Support	3rd Party Integration (logistics, registration, certification)					
	Testing and Validation (internal, IV&V)					
	User Training (admin, field tech, etc.)					
	Security Operations (usage, policies and procedures)					
	Compliance (e.g., NERC)					