SOUTHERN CALIFORNIA EDISON®

An *EDISON INTERNATIONAL*® Company

SANS SCADA Summit 2010

Technology, Innovation, and Security

March 29, 2010

www.sce.com/smartgrid

From Concept to Reality – SCE's secure implementation of AMI program, SmartConnect

Initial Analysis

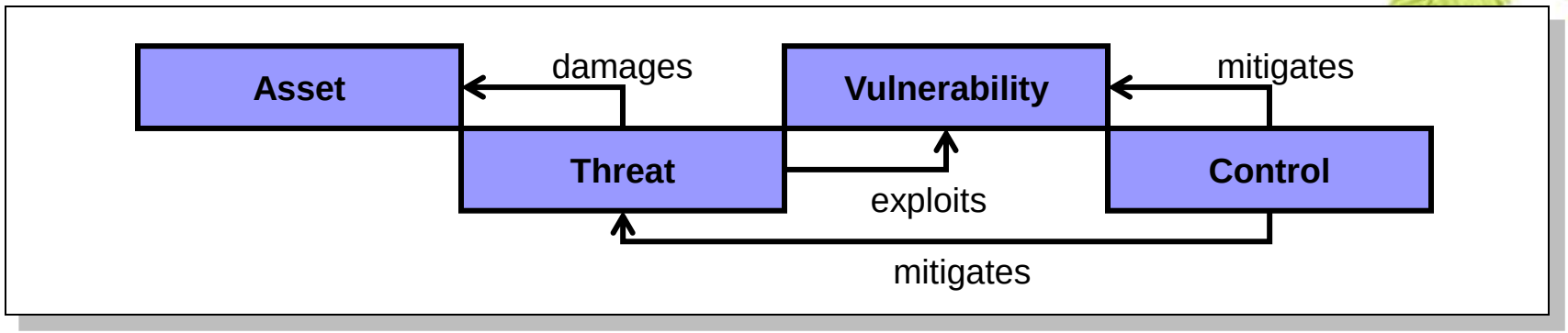
- Recognition of the problem
  - AMI touches every consumer
  - AMI is a command and control system
  - AMI has millions of nodes
  - AMI touches almost every enterprise system

- Recognition of the state of the industry
  - Inadequate vendor RFI and RFP response
  - No best practices or standards
  - TCM confirmed industry delta

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 the engineering process for security
    - Introduce risk driven requirements process
    - Introduce concept of robustness
- Use Open Innovation practices and through public/private standards efforts to ensure a robust, open security solution

Risks and Threats



- SCE uses a rigorous process to identify and catalogue all threats and risks in the system (based on Department of Defense, Common Criteria)
- Threat analysis based on formulaic process (Identify Asset, Threat, Vulnerability, Control)
- Analysis shows the high level risks in the system (examples):
  - Home area Network compromise leads to a compromise of the backhaul network
  - Creating a Denial of Service at the Collection Engine
  - Malicious use of an AMI Device by an insider
  - Hijacking or spoofing a highly trusted device, such as the cryptographic server or network management system

Technology Capability Analysis

It's important to articulate the level of security necessary to vendors

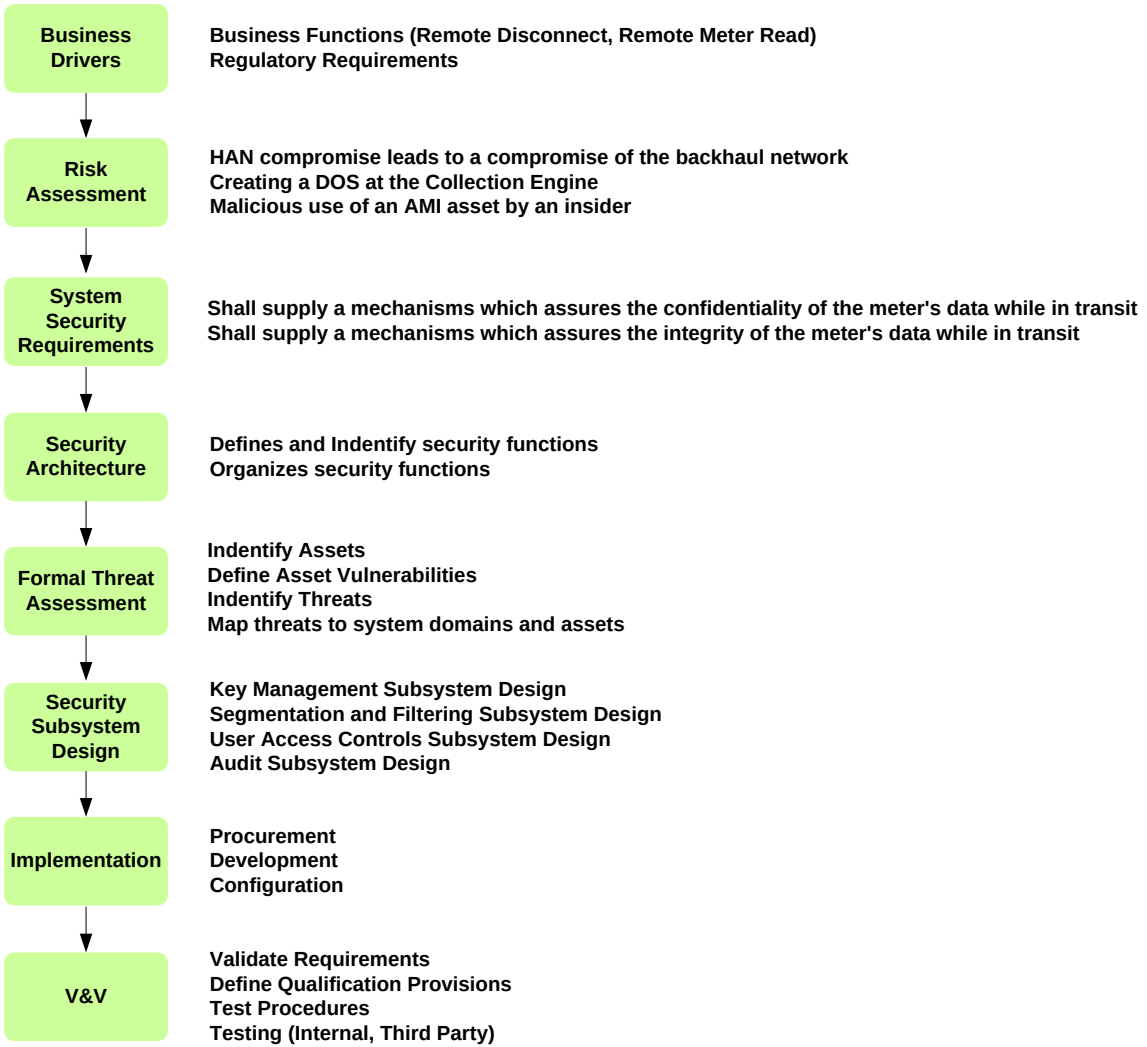
AMI Technology Capability Maturity (TCM) Security Framework

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	X
0																							X

Release One

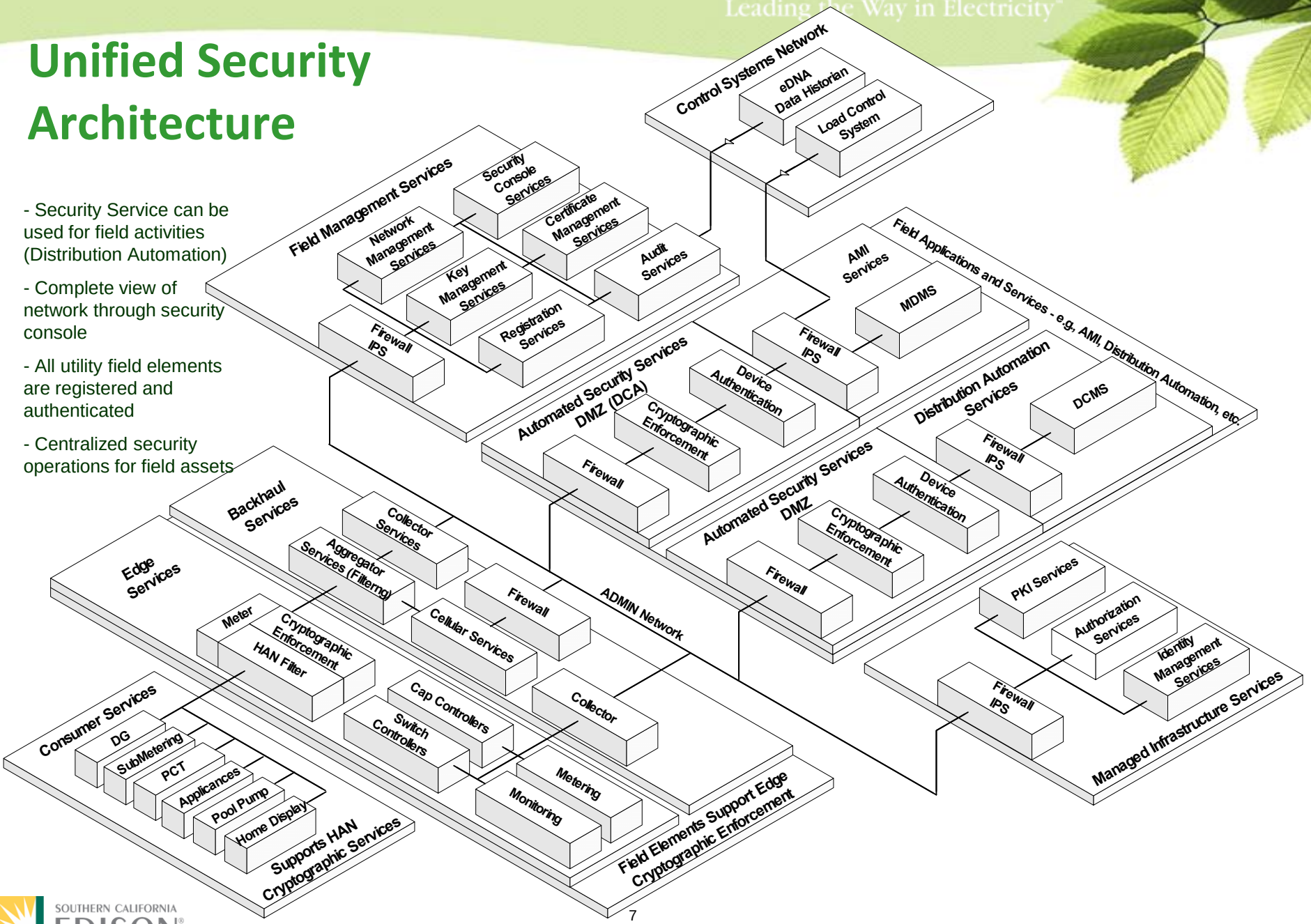
Release Two

System Security Engineering



Unified Security 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



Accomplishments

- System authenticates and manages 30+ million nodes
- All cryptographic methods are compliant with NIST
- Security methods are very fast
- Meters and aggregators have programmable filters
- System supports a rich set of audit services

Moving Forward

- Support, participation, and leadership in standards efforts
- Wide Area Situational Awareness
- Next generation smart grid architecture