Steve Lusk
Alex Amirnovin
Tim Collins
ViaSat Inc.

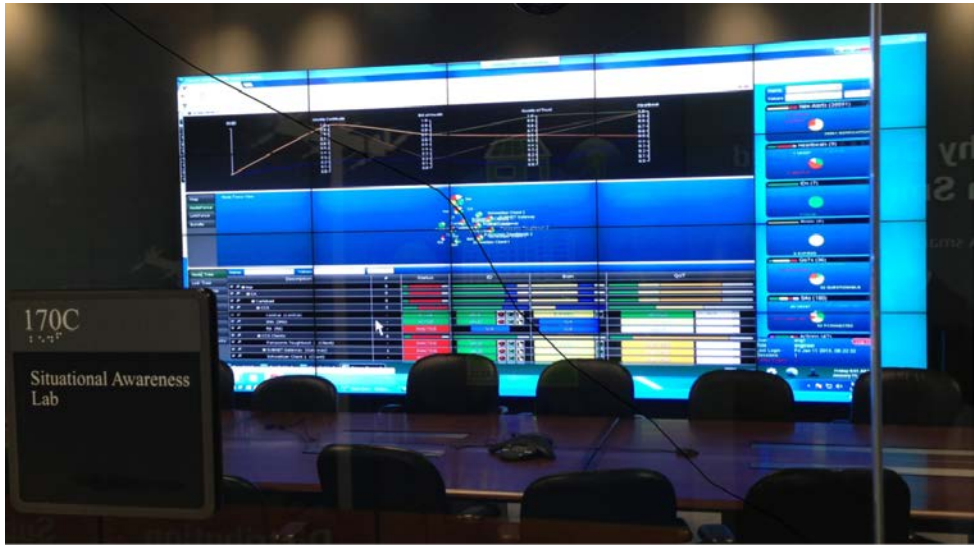
Cyber-intrusion Auto-response and Policy Management System (CAPMS)

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: Cyber-intrusion Auto-response and Policy Management System (CAPMS)

- **Objectives**
  - Integration of advanced algorithms with cybersecurity monitoring to respond autonomously to prevent and/or mitigate cyber intrusion events
  - Demonstrate the possible responses to cyber intrusion events as determined by policy
  - Demonstrate effectiveness of responses due to changes in policy and/or the addition of new events
- **Schedule**
  - Oct 2013 - Sep 2015
  - Key deliverables
    - DOE Kick-off Meeting
    - DOE Program Peer Review
    - System Test Readiness Review
    - Demonstration Readiness Review
    - CAPMS Demonstrations/Reports



- **Total Value of Award:** $6,088,851
- **% Funds expended to date:** 21%
- **Performer:** ViaSat Inc.
- **Partners:** Duke Energy, Southern California Edison

Duke Energy. SOUTHERN CALIFORNIA EDISON An EDISON INTERNATIONAL Company ViaSat

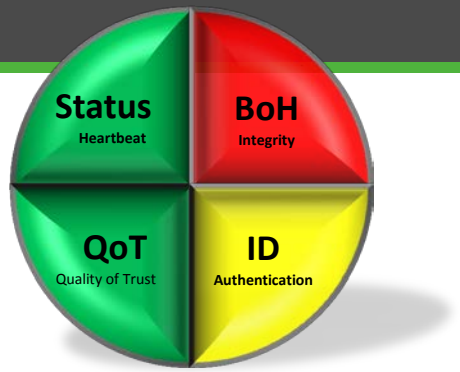
Advancing the State of the Art (SOA)

- **Current "state of the art"**
  - Detection of cyber attacks is daunting given the multitude of information from Cyber, grid and physical security systems
  - Signature-based event correlation is weak at interpreting a coordinated multi-site attack against cyber, physical and grid assets
  - Typical responses to cyber attacks are post mortem at best; many go undetected
- **Feasibility of your approach**
  - Built on ViaSat's existing Trusted Network Platform (TNP) based on open standards to encourage industry adoption
  - Quality-of-Trust (QoT), game theory and causal algorithms provide road map for possible cyber detection and responses
  - Based on two diverse grid architectures from Duke and SCE with real world examples of cyber defense and possible threats

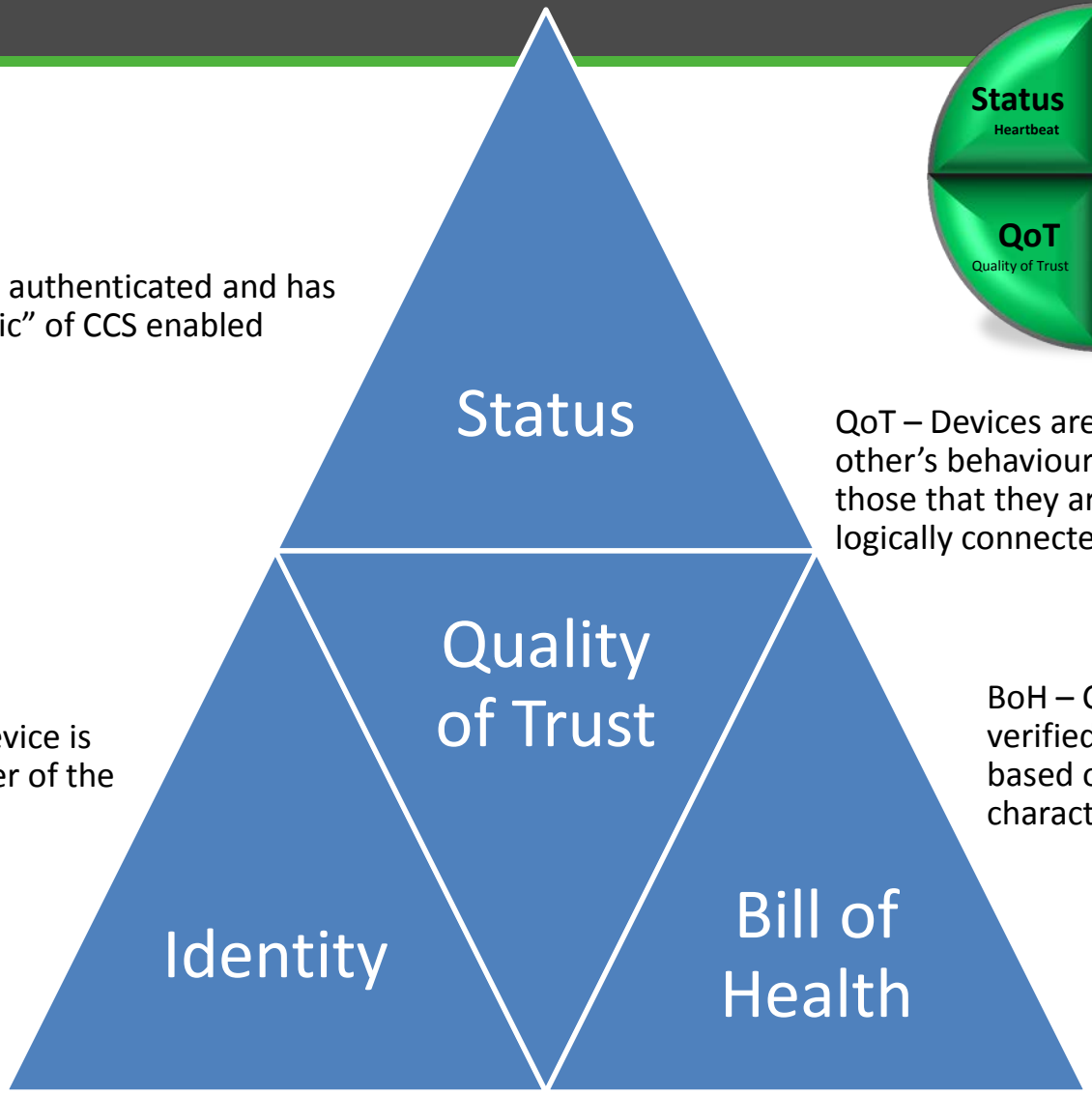
ViaSat Trusted Network Platform Visualization

Security Attributes

Status – Device has been authenticated and has securely joined the “fabric” of CCS enabled devices.



QoT – Devices are monitoring each other’s behaviour and reporting on those that they are physically and/or logically connected to.



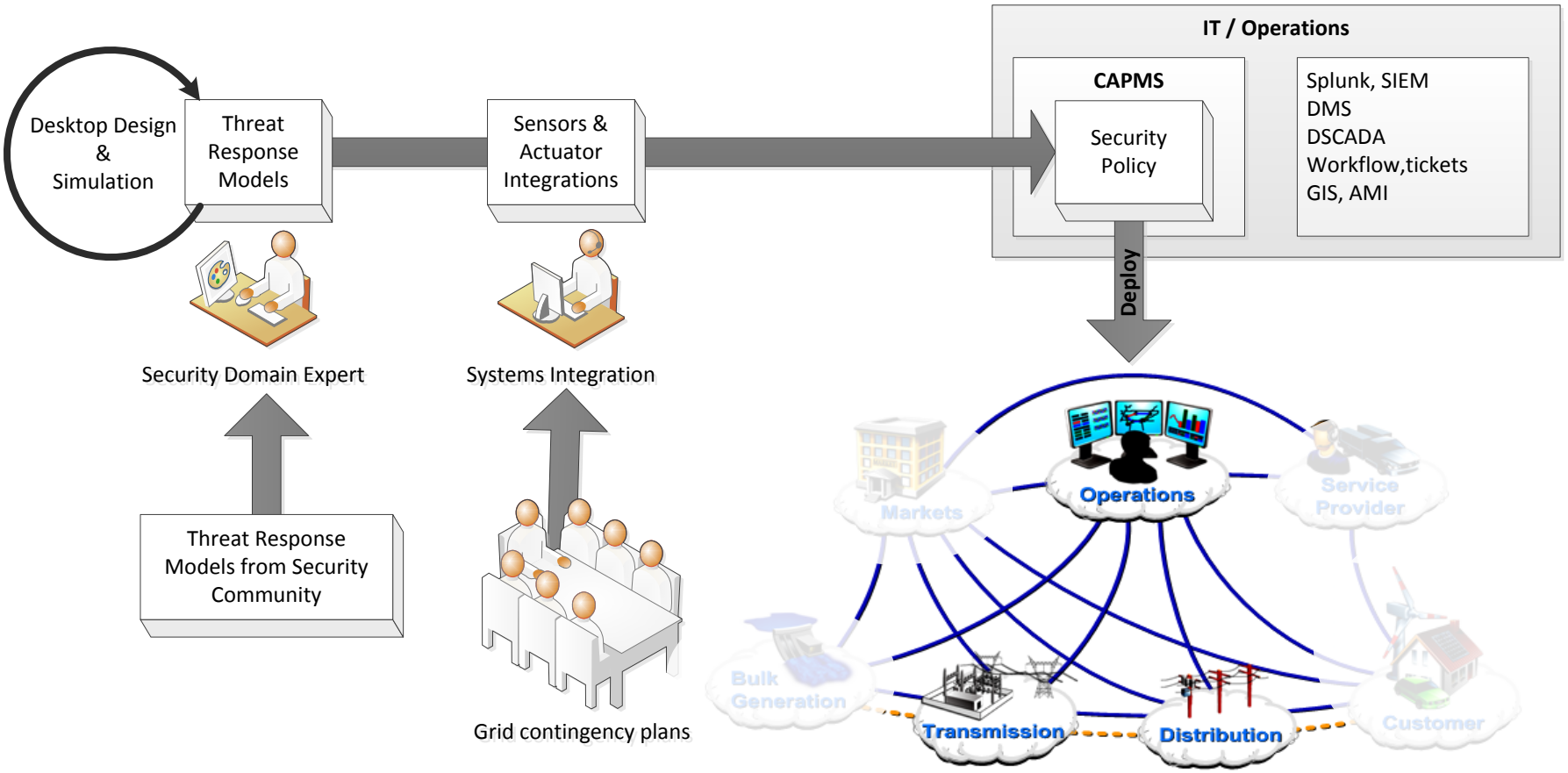
ID – Establishes that a device is an authenticated member of the system.

BoH – CCS central authority has verified a device’s integrity based on a defined list of characteristics/attributes.

Advancing the State of the Art (SOA)

- **Why our approach is better than the SOA**
  - Distributed architecture provides more accurate information regarding an attack
  - Real-time evaluation of the network allows for proactive responses that can prevent and/or mitigate cyber attacks
  - Policy-based responses are tailorable which allow for custom configurations and automated responses specific to each network
- **Why our approach advances the cybersecurity of energy delivery systems**
  - Based on advanced algorithms CAPMS will propose additional cyber sensor monitoring capabilities to improve the energy delivery systems ability to detecting cyber attack
  - Attack models will evolve and can be integrated from a community of security experts and built the industry's collective capabilities over time.
  - Attack models and automated responses are tailorable allowing for further refinement of CAPMS for defending against cyber attacks

Threat Model to Policy Deployment



Challenges to Success

- **Challenge 1**
  - Defining Threat Scenarios and Responses is challenging. It assumes the enemy gets through and takes advantage of network design. Signature based detection is not effective. Profiling is far better but more challenging to define/develop.
  - Mitigation: work closely with Partner utility companies to address the most likely and/or most vulnerable areas of the network for attack
- **Challenge 2**
  - Utility industry has become more dynamic so the landscape is ever changing. CAPMS Demonstrations will just scratch the surface of dynamic policy based systems.
  - Mitigation: provide a reference implementation and sample set of threat scenarios that capture the security priorities of our utility partners and provide a modeling capability for future work
- **Challenge 3**
  - Cyber attacks are becoming more common and immediate defenses are needed. Focusing on the next generation capability while a multitude of short term solutions are being proposed is challenging
  - Mitigation: design CAPMS as a service using open standard interfaces providing the ability to support new cyber sensors and policies as they evolve.

Progress to Date

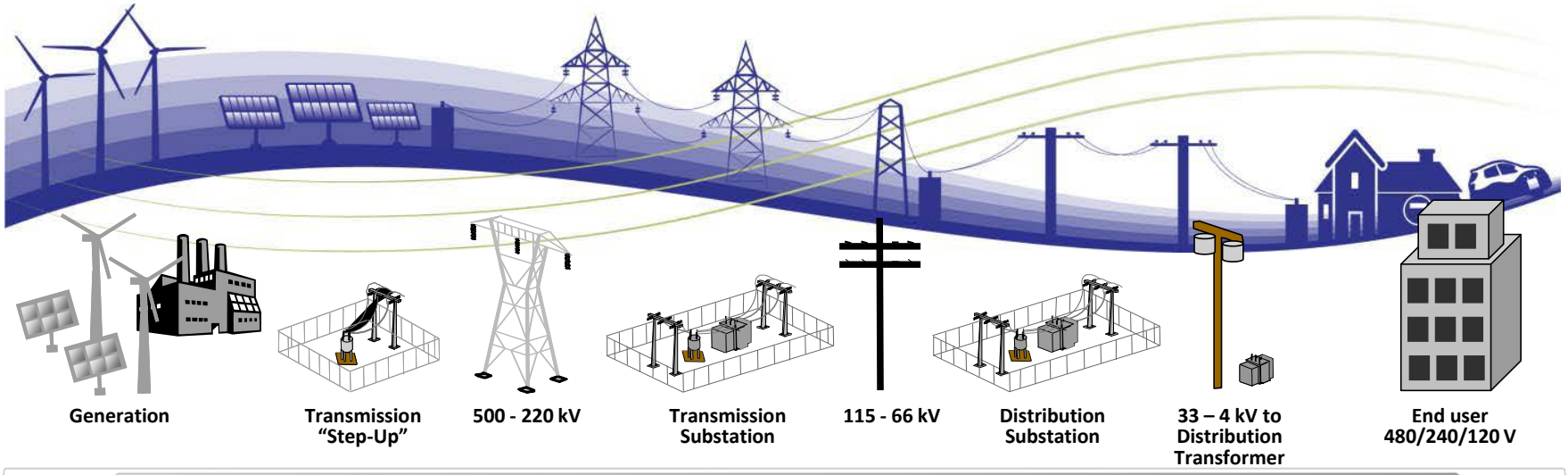
- **CAPMS Demonstration Scenarios**
  - Working with Partner Utilities to expand definition of threat scenarios
    - Duke is a distributed model using sensors on a Comm Node architecture to detect and respond to cyber attacks
    - SCE is a more centralized approach using sensors on Phasor Measurement Units (PMUs)
  - Coordinated effort using existing NESCOR use cases
- **Research & Analysis**
  - *Cyber Sensor and Actuator Study* addressing multiple methods and techniques increasing the number of cyber sensors and actuators
  - *Autonomous Intrusion Response Study* addressing multiple algorithmic approaches to control system auto-response to the increasing number and severity of cyber incidents
  - *QoT Study for CAPMS* includes methods and techniques to enable nuanced responses to new/additional cyber events
  - *CAPMS Causal Algorithms and Use Cases* provides framework for evaluating various algorithms for CAPMS and how they work together

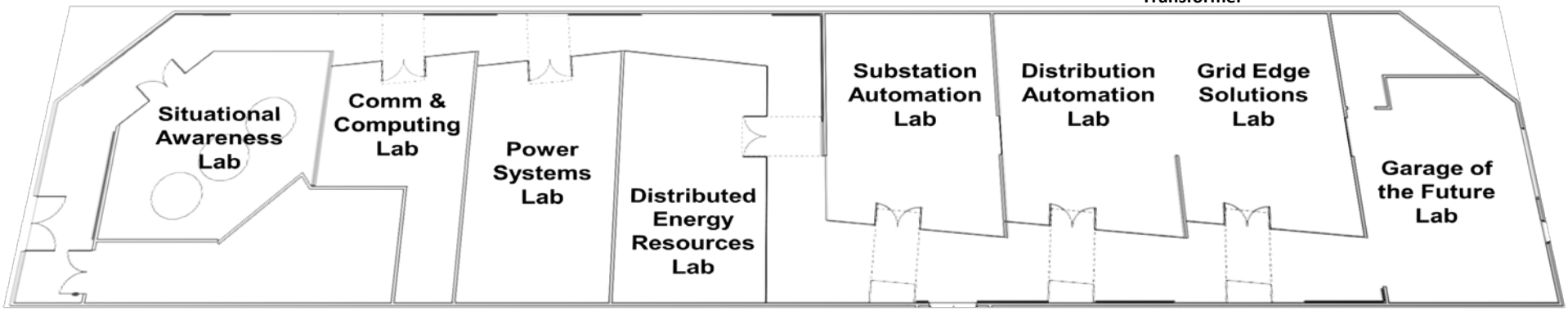
Progress to Date

- **Design / Development**
  - *CAPMS System Specification* provides detailed System definition for CAPMS and defines System Level Requirements
  - *CAPMS Architecture Specification* defines a service oriented architecture for addressing the CAPMS requirements for detecting and responding to cyber security events
  - Integration of *Deep Packet Inspection (DPI)* with TNP to enhance detection of Cyber-intrusions
- **Preparation of labs and demonstration areas**
  - SCE is preparing Westminster test lab for additional hardware to host TNP and real/simulated power utility components
  - Duke is building out the Mount Holly test facility and has purchased TNP servers and related test equipment
  - ViaSat expanded TNP development and test hardware for CAPMS System testing and pre-staging for partner utility facilities

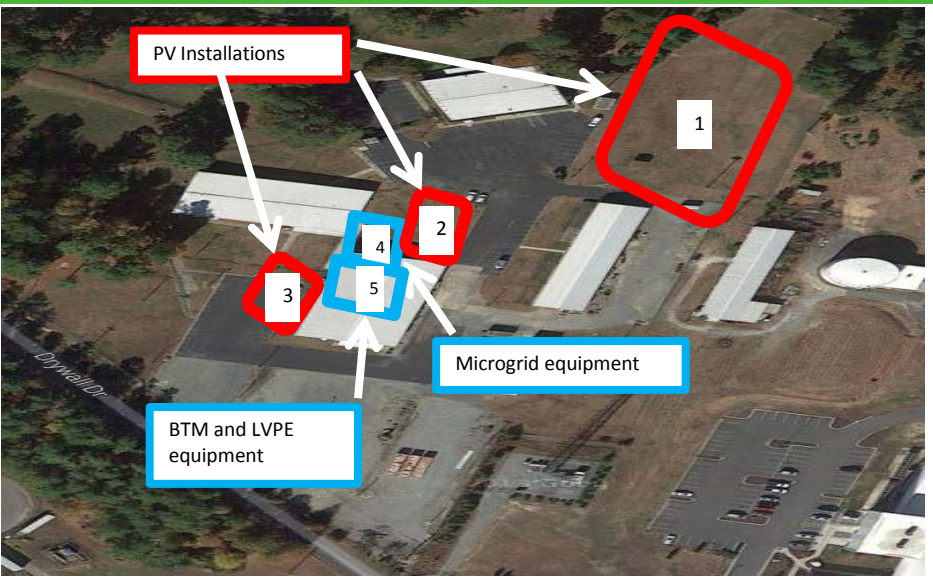
SCE Westminster Facility

- **SCE Smart grid labs provides the ability to simulate Cyber Intrusions and demonstrate the capabilities of the Auto-response and Policy Management features**





Mt. Holly Demonstration Facility



Duke's Mt. Holly MicroGrid

- Brand new microgrid demonstration facility with no rotating mass generation
- Duke's Comm Node and ViaSat's TNP will provide network monitoring, security and visualization
- Threat scenarios center around detection, response, and recovery to Cyber Attacks in a distributed network

Location 1

50-75kW of fixed solar panels with smart inverter utilizing wireless communications

Location 2

10kW of tracking solar panels with smart inverter utilizing wireless communications for solar water heating

Location 3

10kW of roof mounted solar for EV charging

Location 4

Battery storage system, automated switch gear, and new building transformer

Location 5

RTU's, telecom equipment, smart appliances, demand response, smart panel breakers, and low voltage power electronics

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - What category is the targeted end user for the technology or knowledge?
    - Power Utility companies looking to strengthen and automate their cyber incident response capability to lower risk
    - DOE, NESCOR and related organizations looking to expand the definition of sound security practices for the utility industry
  - What are your plans to gain industry acceptance?
    - Duke and SCE demonstration facilities will present real-world examples of cyber-intrusions, auto-responses and policy management services which can be applied to other energy delivery systems
    - Cyber Attacks are ever changing and will continually challenge the industry. CAPMS provides an operational framework for early detection of complex attacks with configurable options to quickly adapt to the latest industry threats.

Next Steps for this Project

- Threat Scenarios
  - Further define/clarify threat scenarios with partner utilities for the demonstration
- Design and Development
  - Update policy management system to support tailorable policy definitions for multiple utility network designs/architectures
  - Implementation of auto-response techniques and algorithms for detecting and responding to cyber-intrusions
  - Implementation (or simulation) of additional cyber sensors deemed critical to detecting cyber attacks
- System Test
  - System testing will fine tune demonstration of threat scenarios
- Demonstration Preparations
  - Demonstration Readiness Review artifacts include: Updated System Test Plan/Procedures; System Test Report; Software Release Note; Updated User's Manual to support CAPMS features (draft)
- CAPMS Demonstrations/Reports
  - Demonstrations will occur at each partner utility's test facility
  - Dates/times of the demonstrations will be arranged with DOE PMO
  - Draft CAPMS Demonstration Test Report will be provided prior to the demonstration
  - Final CAPMS Demonstration Test Report will be provided after the demonstration