Seth Walters
Dr. Sakis Meliopoulos
Dr. Santiago Grijalva
Dr. Raheem Beyah
Georgia Tech

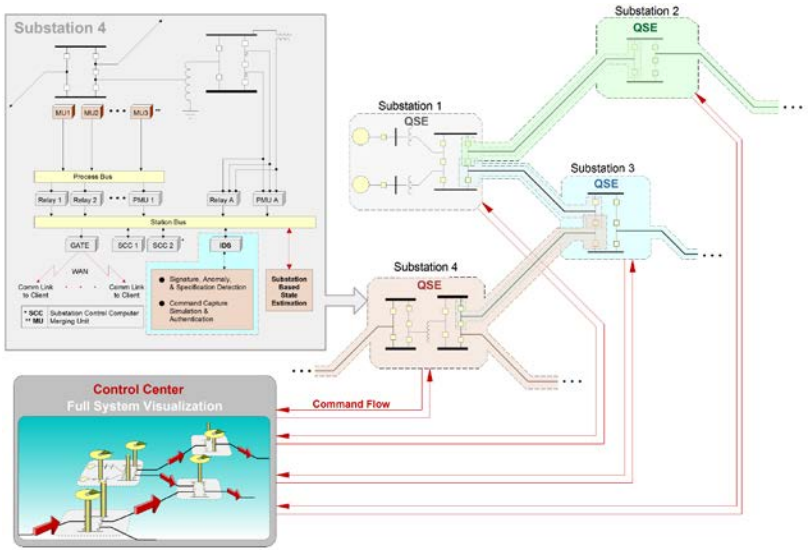
Cyber-Physical Modeling & Simulation for Situational Awareness (CYMSA)

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: CYMSA

- **Objective**
  - Detect adversarial manipulation of smart grid cyber components in a real-time operational environment with distributed modeling & simulation context and security sensors
- **Schedule**
  - POP: June 2014 – May 2017
  - Key deliverables:
    - M&S, Rules / Sensors: Jan 2016
    - Laboratory testing: Apr 2016
    - Demonstration: Oct 2016; Feb. & May. 2017
  - Result: Improved SA technology & tools



- **Total Value of Award:** 4.93M
- **% Funds expended to date:** <1%
- **Performer:** Georgia Institute of Technology
- **Partners:** OISF, Southern Co., VIWAPA, & BWAP

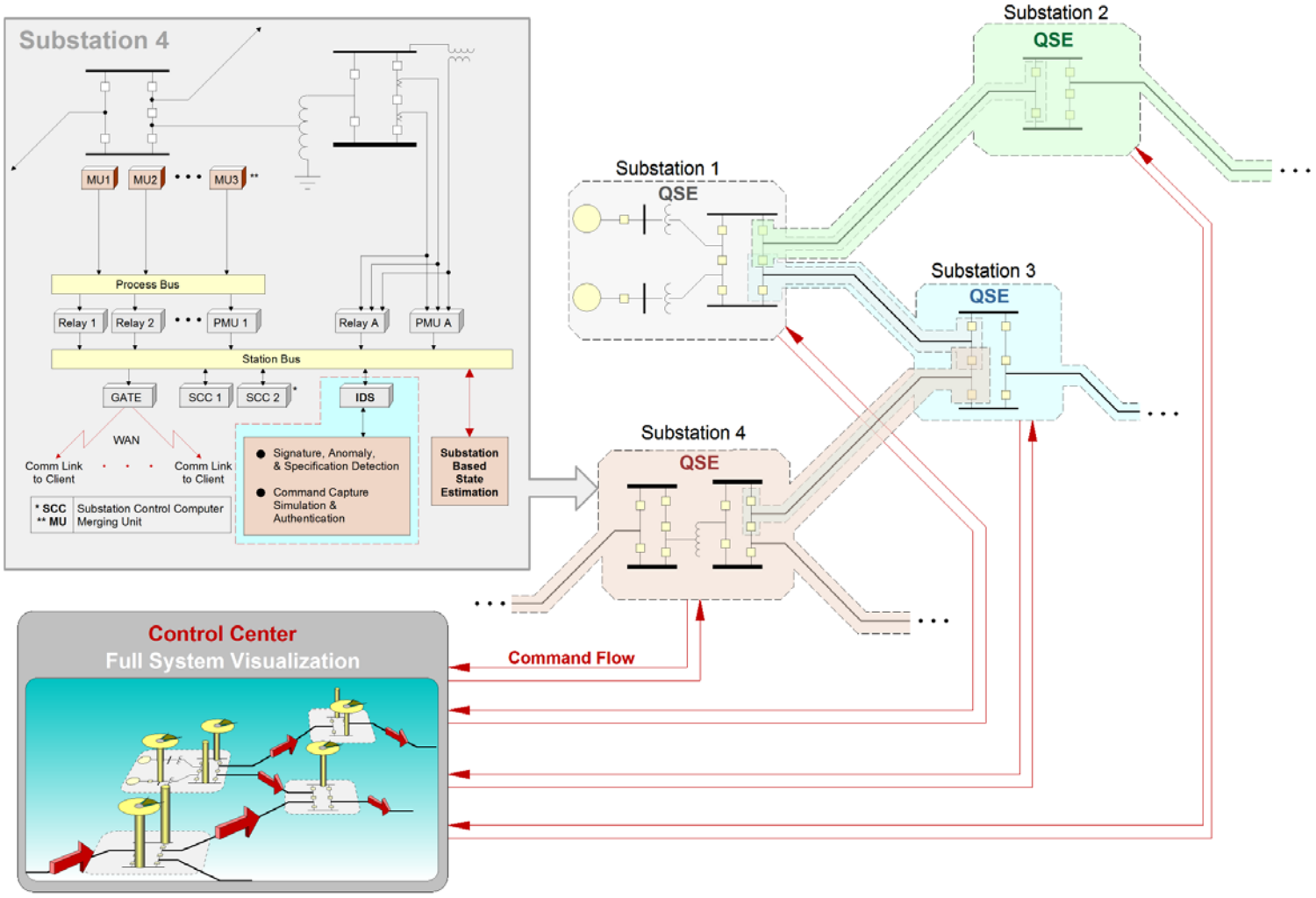
Advancing the State of the Art (SOA)

- **Distributed Situational Awareness**
  - Security sensors with context
  - Evolving context through system models
  - Context is evaluative basis for sensors
  - *Real time context is a need*
- **Cybersecurity at system level decision making**
  - Integrated Physical and Cyber model
  - Model & simulation based
  - Real time
- **Cybersecurity at substation level automation**
  - As above

Advancing the State of the Art (SOA)

- **Potent IDS technology possible**
  - Dynamically assess threat & safety
- **IDS as system probes**
  - Cyber layer safety in terms of network truth
  - Advanced warning of system instability
- **IDS as cybersecurity sensors**
  - Detect evolving threats through model discrepancies
  - Semantics vice syntax for threat assessment

Schematic Approach



Distributed Cyber Security monitoring approach:

Substation Level (shown)

Control Center (not shown)

Challenges to Success

- **Technical Challenges**
  - Optimal cybersecurity architectures for smart grid
  - Real-time modeling & simulation
  - IDS / cybersecurity sensors
    - Rule-generation & conflict resolution
    - Rule expiration optimization & thrashing mitigation
    - Deep-packet inspection for smart grid protocols
- **Acceptance Challenges**
  - Demonstrate applicability to improved safety
  - Demonstrate transparency on grid networks
  - Demonstration with “live” grid assets

Progress to Date

- **Kickoff meeting held (25 July 2014)**
- **Preliminary Team Meetings**
- **Project Staffing**
- **Ramp up with systems & software**

Collaboration/Technology Transfer

- **Targeted CYMSA users**
  - Asset owners (utility operators)
  - Vendors
- **Industry Acceptance**
  - Design for demonstration
  - Demonstration reporting (“lessons learned”)
- **Planned Demonstrations**
  - Disconnected substation (Southern Co.)
  - Island power grid (VIWAPA)
  - Metropolitan power grid (BWAP)

CYMSA Upcoming Milestones

- **Commercialization**
  - Technology to Market Plan conceptualized
  - IAB formation complete
- **Research Maturity**
  - Modeling & simulation technologies
    - Cyber-physical co-simulation
    - Distributed State Estimation (no latency SA)
  - Distributed context protocols
  - Security sensor (IDS/IPS) upgrades

History of State Estimation

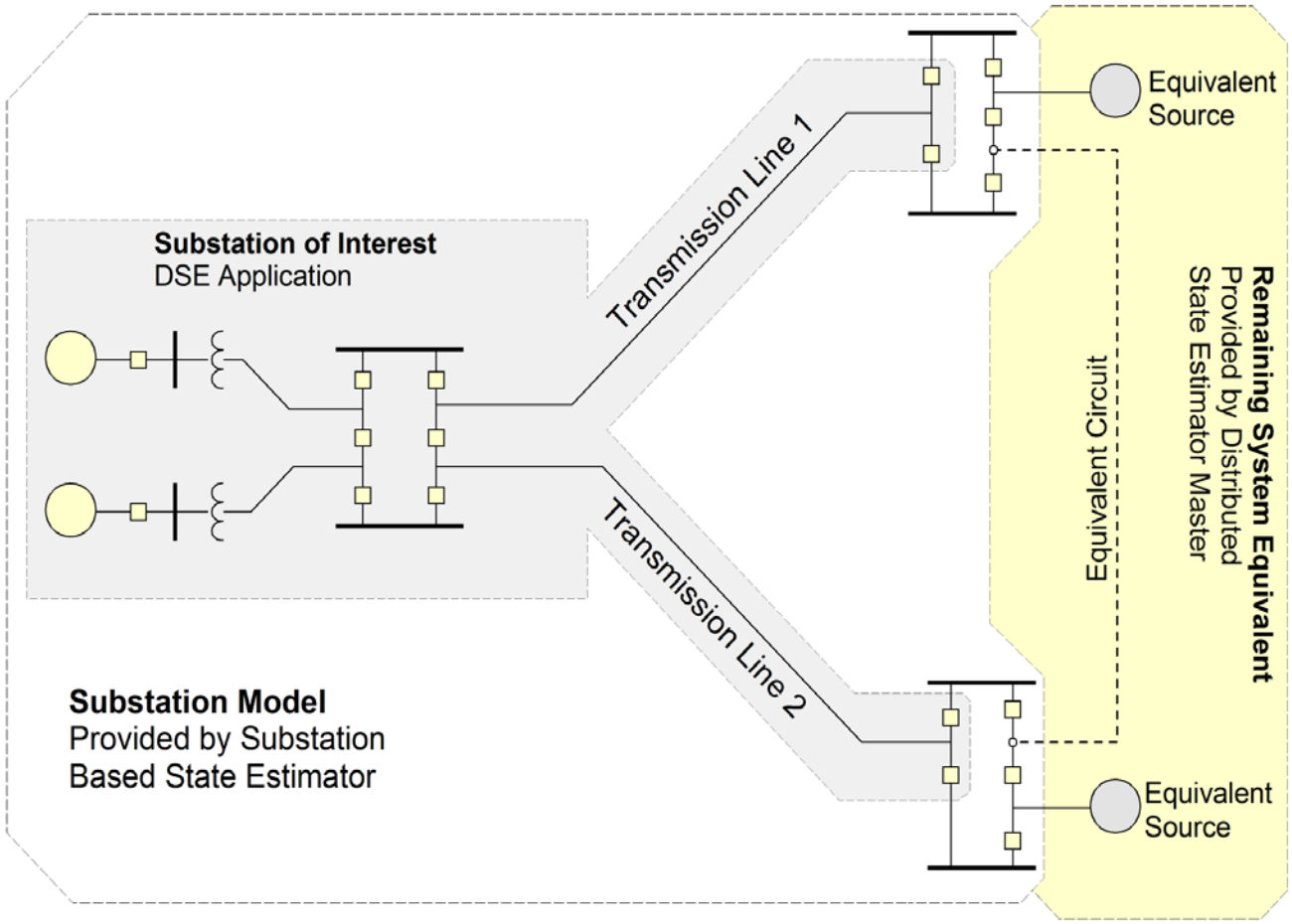
Legacy State Estimation: (a) developed in the late 60s after the 1965 blackout, (b) estimates positive sequence voltage phasors at transmission buses, (c) model needed is only transmission circuits, (d) it is centralized – needs all measurements at a central location – long latencies in the order of minutes.

Three Phase Linear Estimator (1993): uses three phase model and three phase phasor measurements (GPS synchronized measurements). Solution is direct but requires data in a central location.

Substation Based State Estimation (2007): Described next

Substation Based State Estimator

Uses substation data only (no communication latencies) and extracts the model of the substation and the circuits connected to the substation – see figure shaded area



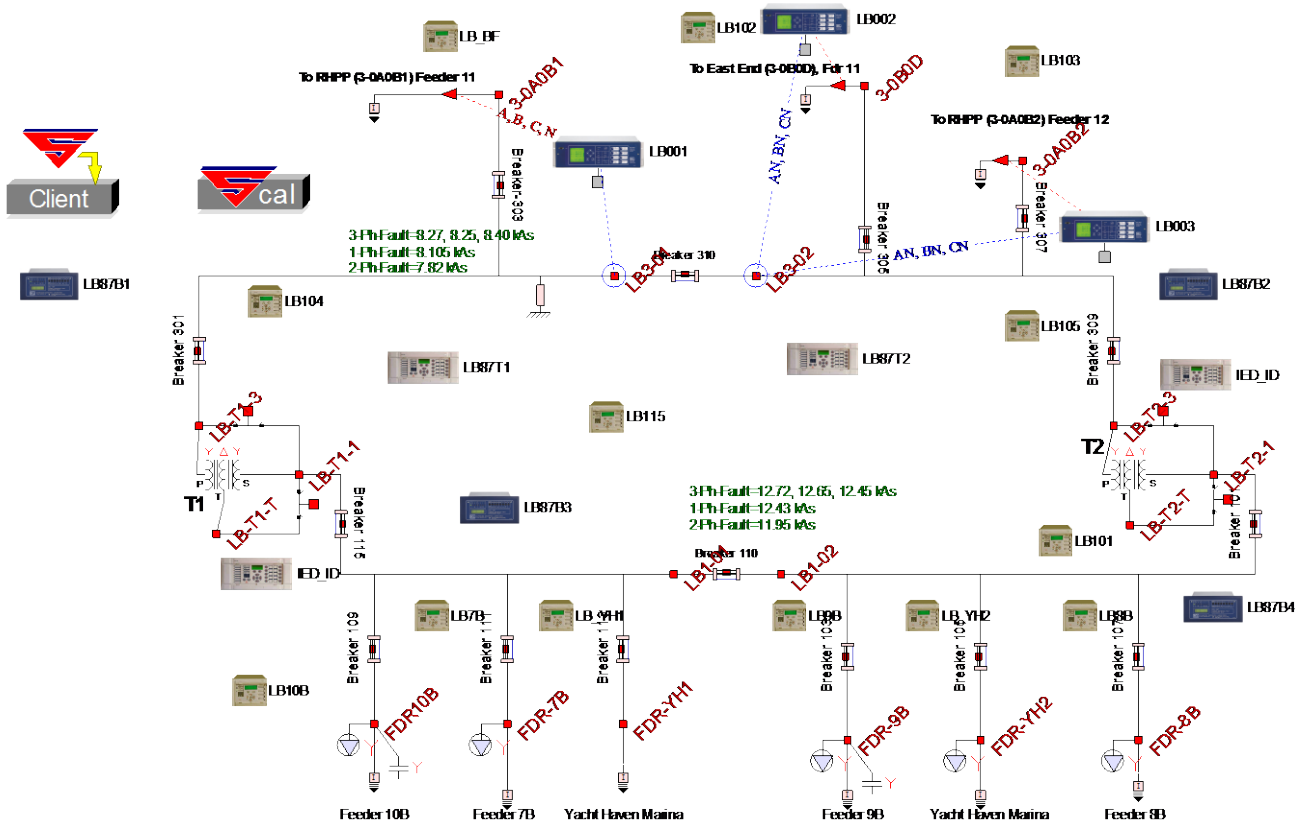
Enables construction of local model in real time without latencies – neighboring state estimator can provide the equivalent of the rest of the system.

The substation model and equivalent is used to perform faster than real time simulation starting from the present operating condition.

The results are used to authenticate or block commands

Physically Based Integrated Physical and Cyber System Model

The physical power system (a sub station is shown) is modeled in terms of its physical construction; the cyber system consisting of relays, instrumentation, communications and human interfaces is integrated with the physical system. Any changes in the physical system propagate to the cyber system and any command at the cyber layer is transmitted to the physical system. (Figure shows the physical and cyber components of an actual substation)



The integrated model enables co-simulation and evaluation of the complex interactions between the two systems.

Most importantly enables the context based authentication or blockage of commands via the cyber system in a seamless and timely manner. Time response of the authentication process is an extremely important issue.