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

December 7-9, 2016

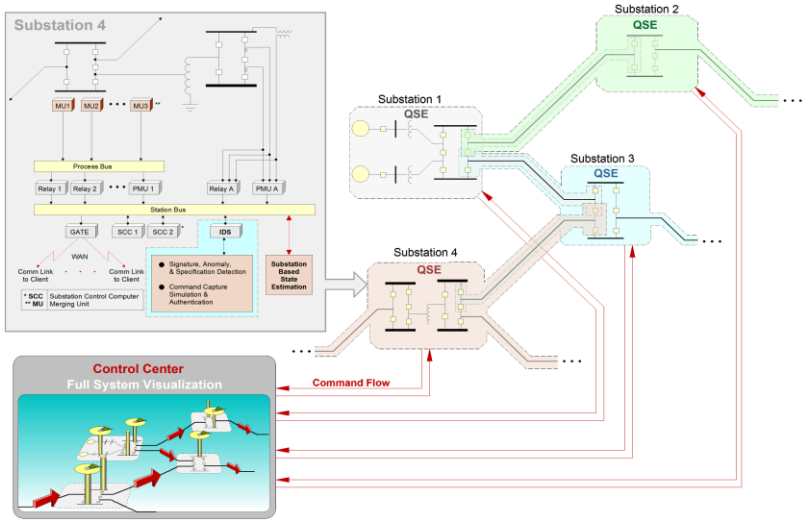
Summary: CYMSA

Objective

- Detect adversarial manipulation of smart grid components in real-time operational environments with distributed modeling & network security monitoring solutions.

Schedule

- POP: June 2013 – May 2017
- Key deliverables:
  - The software has been testing in a laboratory environment and is ready for field demonstration – August 2016
  - Field demonstration activities have begun. First demonstration will take place 12/9/2016
- Result: improved cyber situational awareness real-time technology & tools.



Performer:	**Georgia Tech Research Institute**
Partners:	**Georgia Tech, OISF, Southern Company, Burbank Water & Power, and Virgin Islands Water & Power Authority**
Federal Cost:	**$3,283,063**
Cost Share:	**$1,649,500**
Total Value of Award:	**$ 4,932,567**
Funds Expended to Date:	**% 73**

Advancing the State of the Art (SOA)

- **Distributed Situational Awareness**
  - Continuously updated system model (PB-CPcoM)
  - Security determination through real-time context
- **Cyber Physical Co-Simulation**
  - Joint simulation of the power & communications layers
  - Dynamic system simulation for cyber-security evaluation
- **Cybersecurity Sensing**
  - Model-based discrimination between syntax & semantics

Challenges to Success

Technology Adoption

- Planned demonstrations intended to convey value proposition
- Significant demonstration planning underway, if not completed
- Field demonstrations scheduled

Operational Deployment

- Operational environment significantly different
- Simplified installation desirable

Historical Performance

- Cost-share partner advocacy & buy-in
- Communicate to vendors (market discovery)

Progress to Date

- R&D components successfully integrated & tested
  - Primary use-case is malicious or mistaken control identification
- Laboratory demonstration complete
  - System tested for cost-share partner on substation hardware
  - System performance within latency constraints
- Letters of commitment for demonstration received
- Significant demonstration planning underway, if not complete
- Cost-share goals for R&D phase met
- Industry advisory board established and engaged

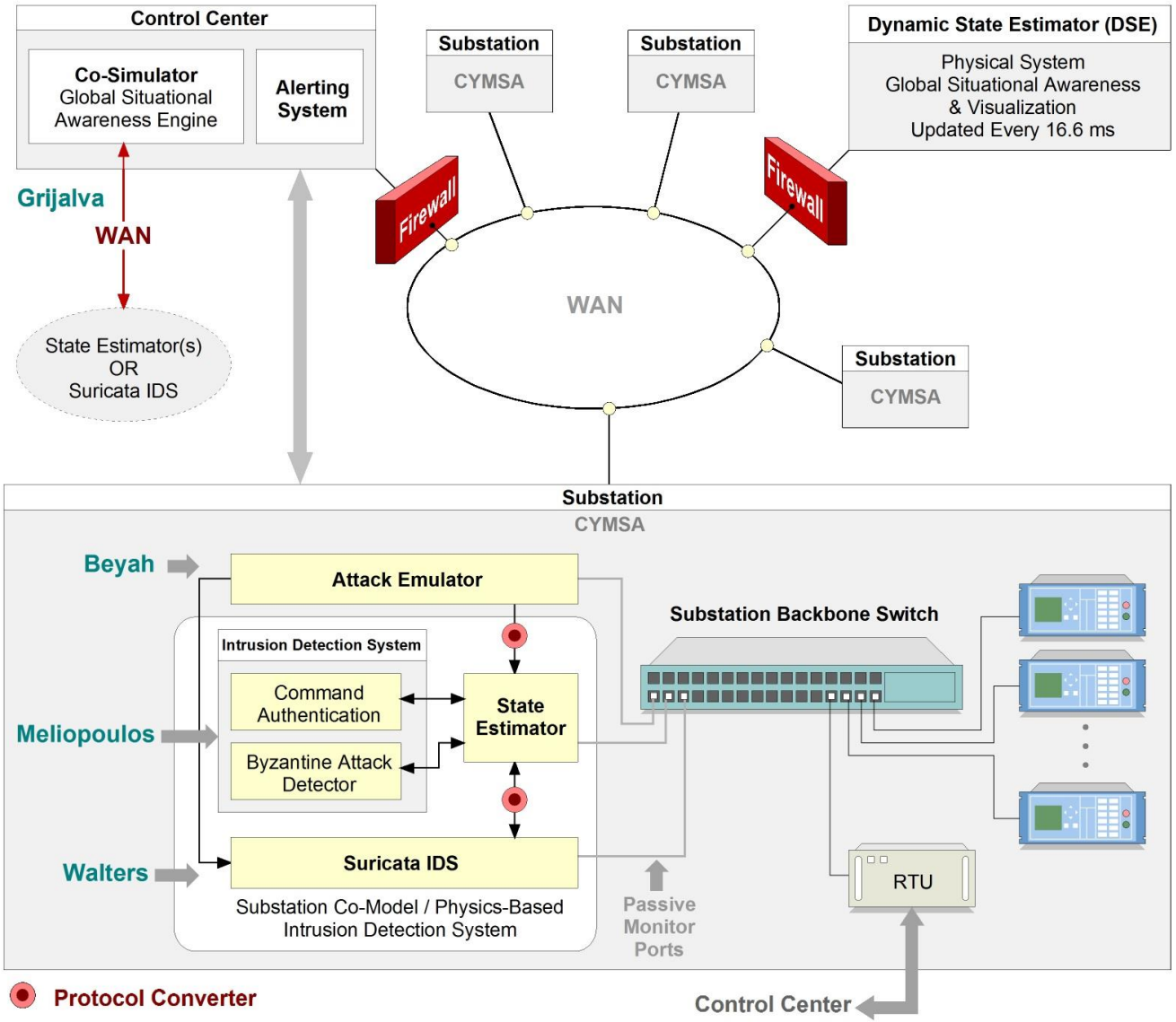
Collaboration/Technology Transfer

- CYMSA consumers likely utility companies and vendors
  - System insight & security operationally useful
  - Managed security services through vendors potentially
  - OEM would support hardware deployment
- Industry acceptance planning = demonstration
  - Three field demonstrations planned to validate technology
- Demonstration scenarios
  - Real-time data acquisition & models
  - Modern infrastructures and equipment
  - Offline control for demonstration safety in live setting
  - CYMSA's threat model to be tested

Next Steps for this Project

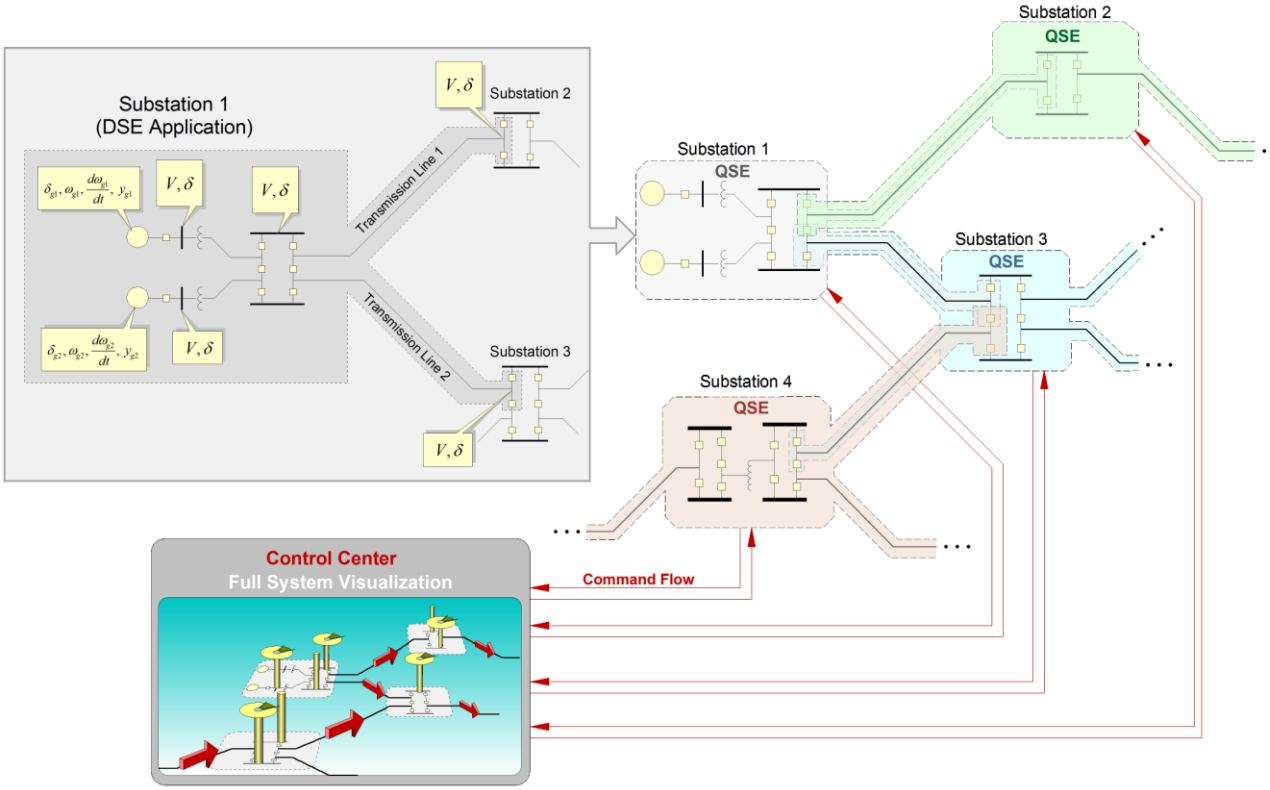
- *CYMSA has entered demonstration phase*
  - Some R&D work remains, but not the main focus
- Project will focus primarily on all aspects of demonstration
  - Field demonstration
  - Use-case validation – some possibility to explore other malicious scenarios
    - Bad data injection is academically of interest
  - Open source contributions where possible
- Lessons learned & market information capture

System Communications Architecture



Substation Based State Estimator – Control Center State Estimator

Requires at least one GPS-synchronized IED at each substation.
System is represented with a set of differential equations (DE).
The Dynamic State Estimator fits the streaming data to the dynamic model (DE) of the substation.
The substation state estimate is transmitted to the control center where the system state is synthesized.
Demonstration projects exist at (USVI-WAPA, SoCo, NYPA and PG&E).
Distributed Dynamic State Estimator executes once each cycle (16 milli-seconds).



The Estimator is Defined in Terms of:

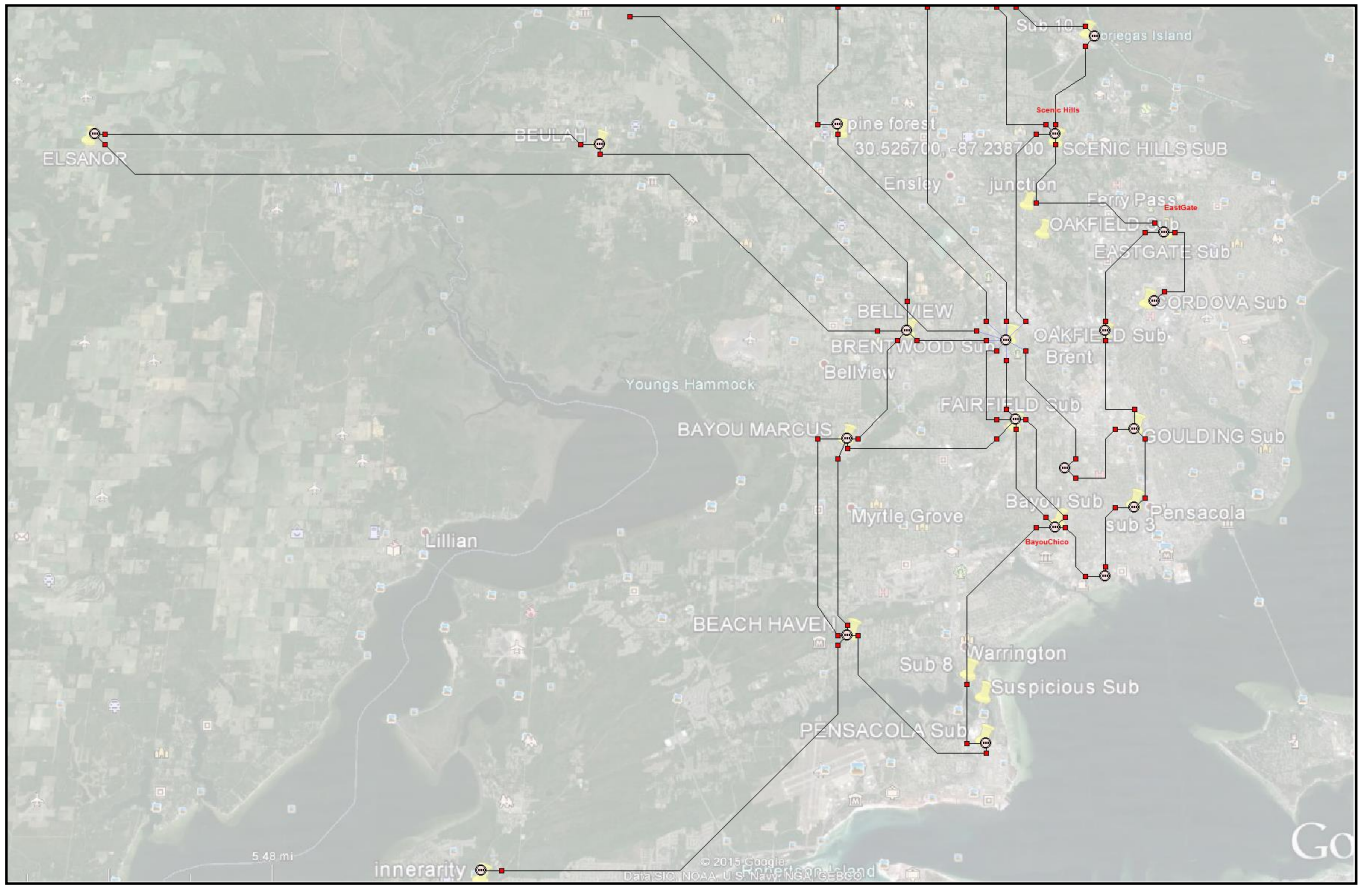
- Model (power + instrumentation)
- State
- Measurement set
- Estimation method

Operates on the PB-PCcoM

- ***Object orientation***
- ***Observability***
- ***Redundancy***

Physically Based Integrated Cyber-Physical System co-Model (PB-CPcoM)

The physical power system is modeled in terms of its physical construction (3-phase breaker-oriented); 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.

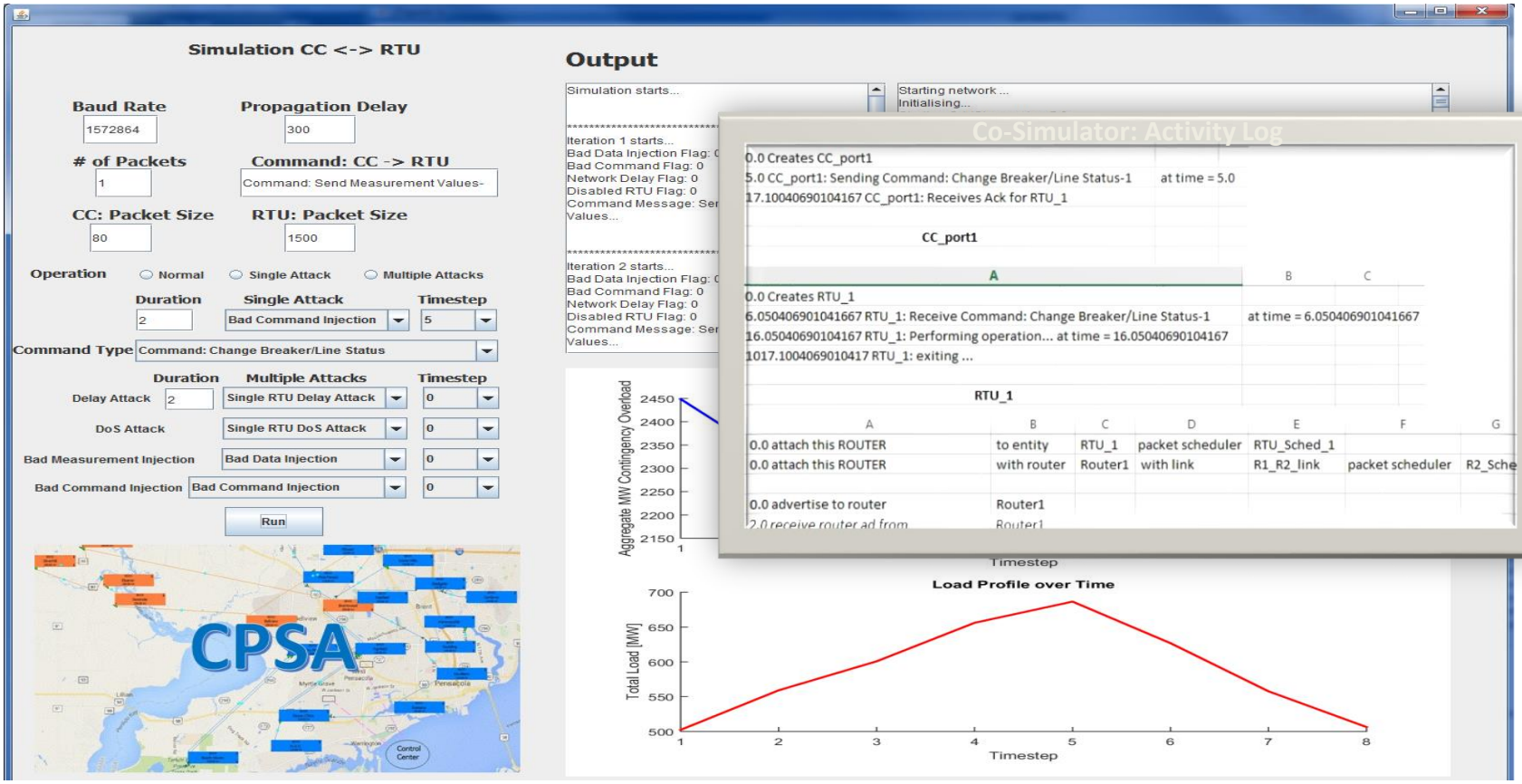


The integrated model enables co-simulation and evaluation of the complex interactions between the two systems.

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

Co-Simulator

- Synchronized integration of GridSim and JADE (Java)/Matlab/PowerWorld
- Ability to model communication network topology with varying baud rates, propagation delays, and packet sizes for SCADA systems.



POWER AND CYBER LAYER VISUALIZATION