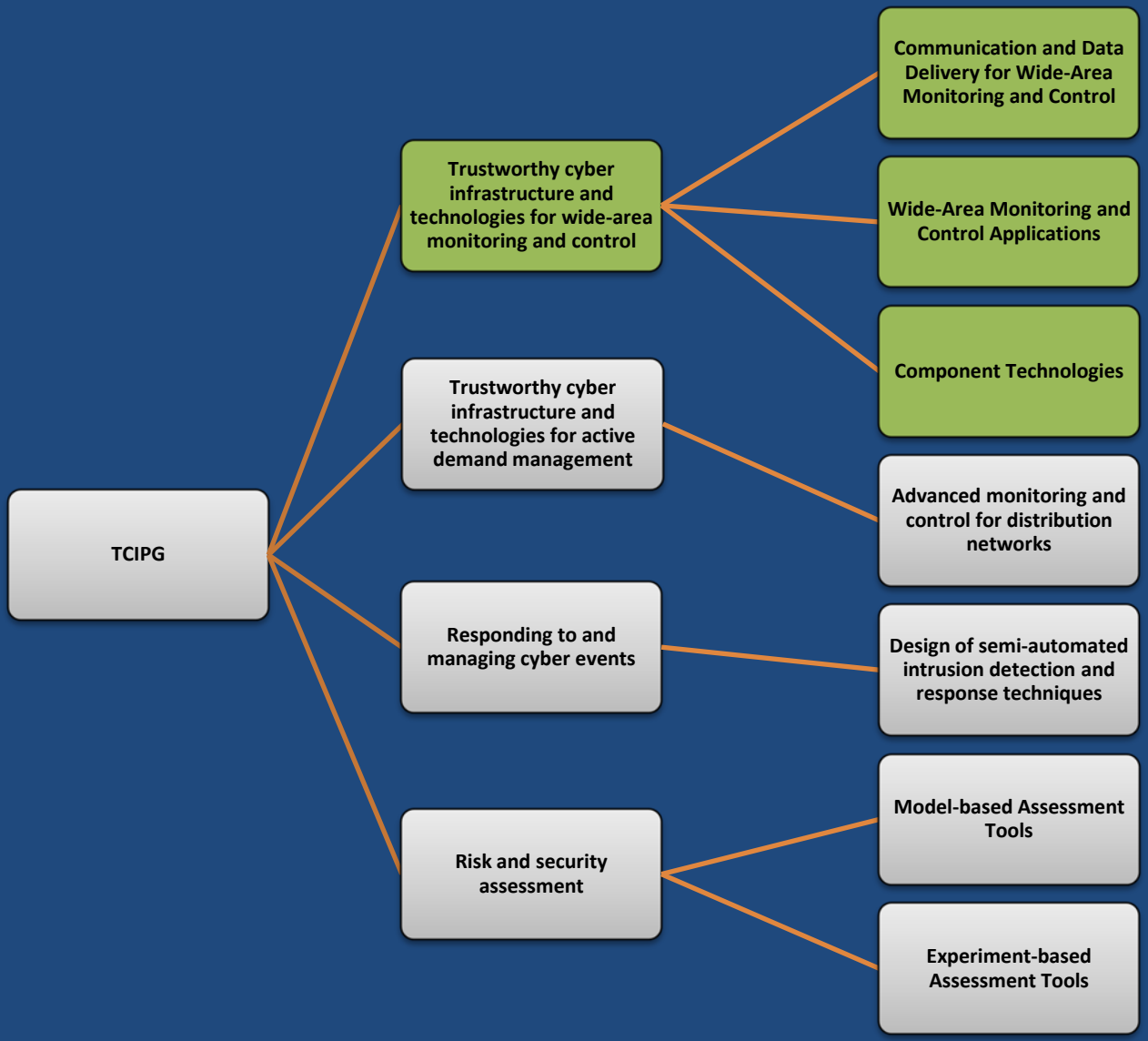
Trustworthy cyber infrastructure and technologies for wide-area monitoring and control

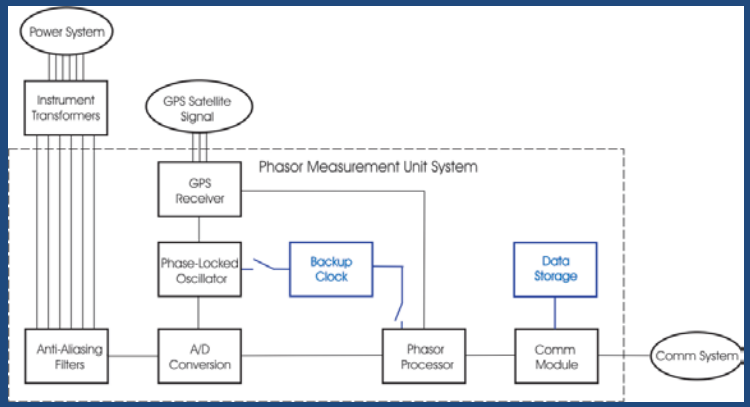
Carl Hauser

TCIPG Cluster Arrangement



Cluster Overview

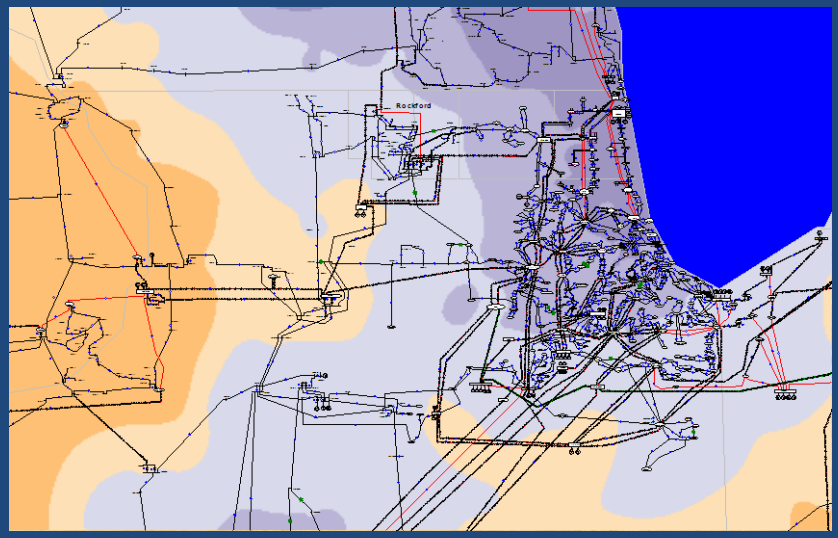
- Smart Grid vision for the wide area (primarily transmission) is:
  - Vastly more sensing at high, synchronous rates (example: PMUs)
  - New applications that use these data to improve
    - Reliability
    - Efficiency
    - Ability to integrate renewables



- Achieving the vision requires secure and reliable communications between sensors, control devices, and monitoring and control applications all owned and operated by the many entities that make up the grid

Cluster Problem Areas

- Smart grid technologies bring new vulnerabilities along with benefits
  - Need improvements in security of wide-area communication technologies
  - Need ways to understand and mitigate the impacts of vulnerabilities

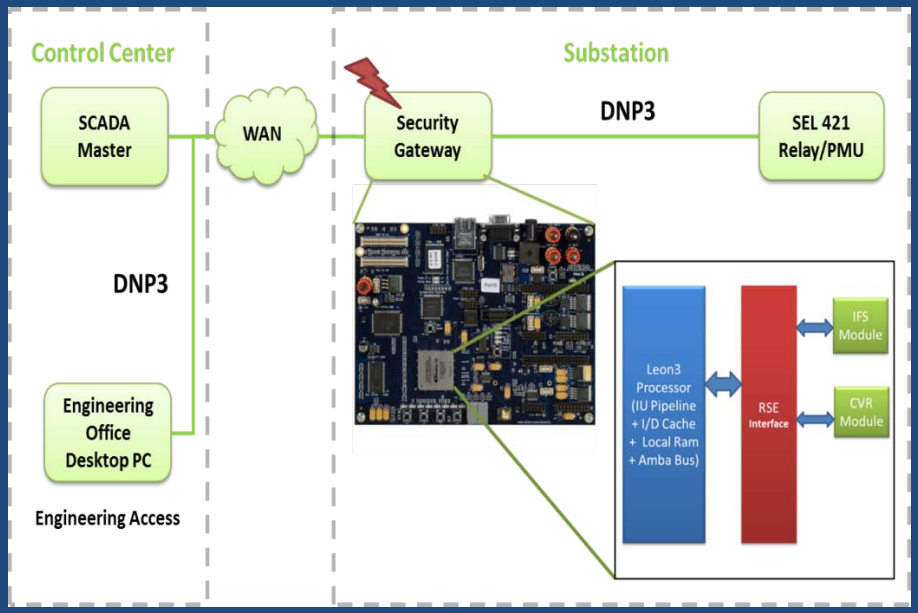


- What data delivery infrastructure design will provide the *integrity*, *confidentiality, availability*, and *real-time performance* needed for wide-area smart grid operations?

Cluster Problem Areas, cont'd

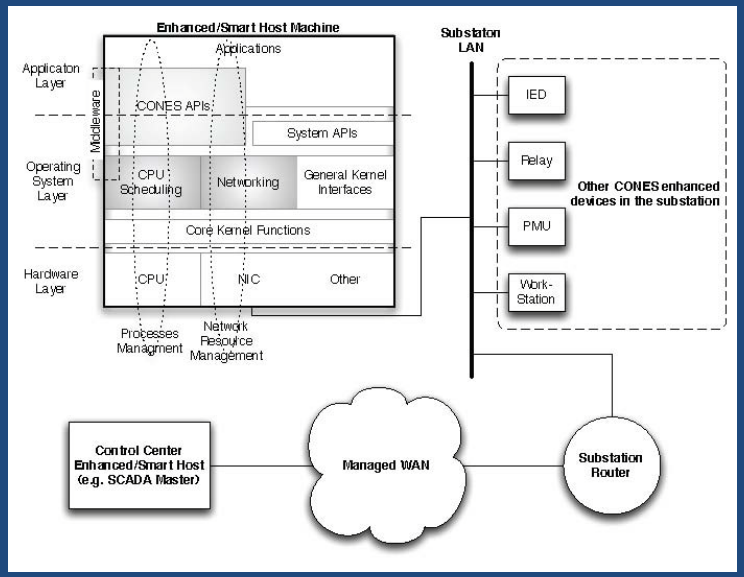
- What is the relationship between security (or lack of security) of communications for wide-area monitoring and control and the power-system's behavior?

- What kinds of hardware and software components will provide a better foundation on which to build the wide-area monitoring and control infrastructure?



Cluster Objectives

- Architect, design, implement, and test prototype trustworthy data delivery infrastructures
  - Drawing on deep understanding of existing power grid protocols
  - Projecting future communication needs
- Develop novel wide-area monitoring and control applications to
  - Further identify communication requirements
  - Understand the effect of communication disruption on power grid operations
- Develop component technologies that:
  - Are robust against attack
  - Enhance application performance



Cluster Activities (with more details in posters)

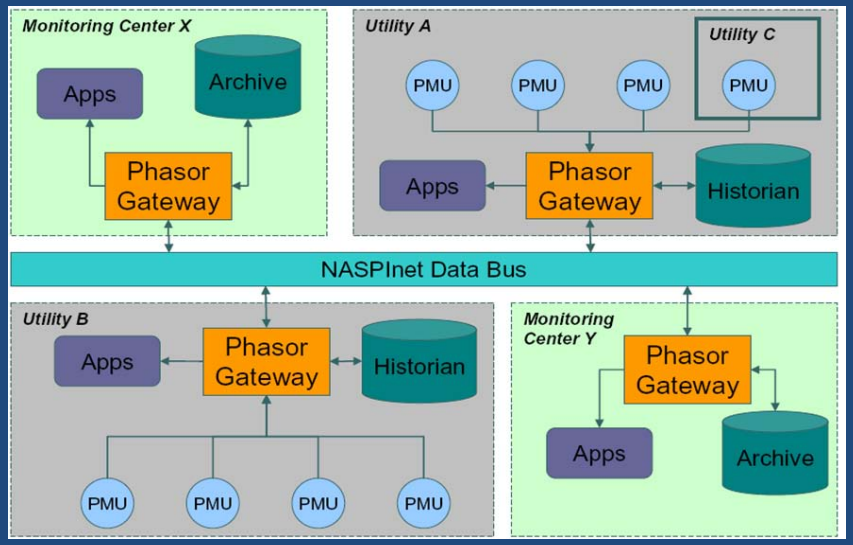
- Ongoing
  - CONES: Converged networks for SCADA
  - GridStat middleware communication framework: management security and trust
  - PMU integration into power flow software
  - GridStat middleware communication framework: application requirements
  - Lossless compression of synchrophasor measurement unit archives
  - Real-time streaming data processing engine for embedded systems
  - Decentralized sensor networking models and primitives for Smart Grid – part 2: state-aware distributed database systems

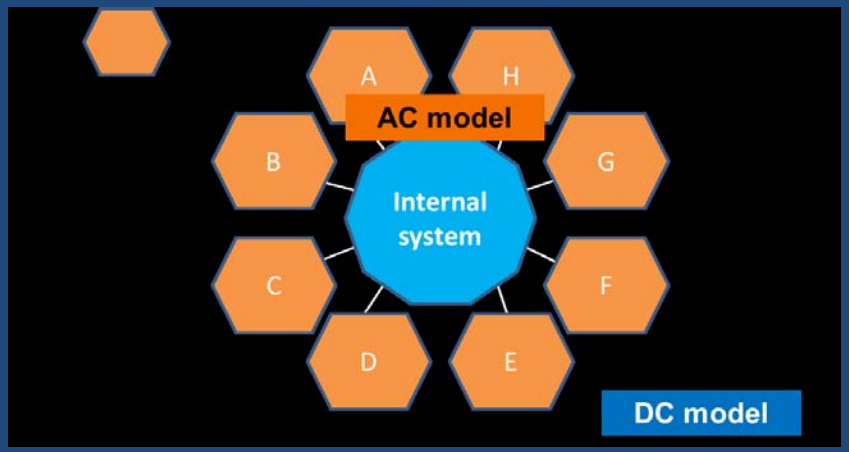
Cluster Activities, cont'd

- New start
  - PMU data quality
- Completed
  - Decentralized sensor networking models and primitives for Smart Grid – part 1: metrics of grid vulnerability to cascading failures
  - Cooperative congestion control in power grid communication networks
  - Secure wide-area data and communication networks for PMU-based power system applications

Cluster Accomplishments and Impacts

- Cluster activities collaborate with: Entergy, PNNL, SEL, GPA, TVA, NASPI, National Instruments, EPRI, PowerWorld, Altera, PowerTech
- Transferred wide-area data delivery and security knowledge to Entergy synchrophasor deployment and NASPInet
- Developed a new power flow algorithm using PMU input data improves solution speed without sacrificing accuracy in areas of interest; it can be used for fast steady-state and transient analysis as well

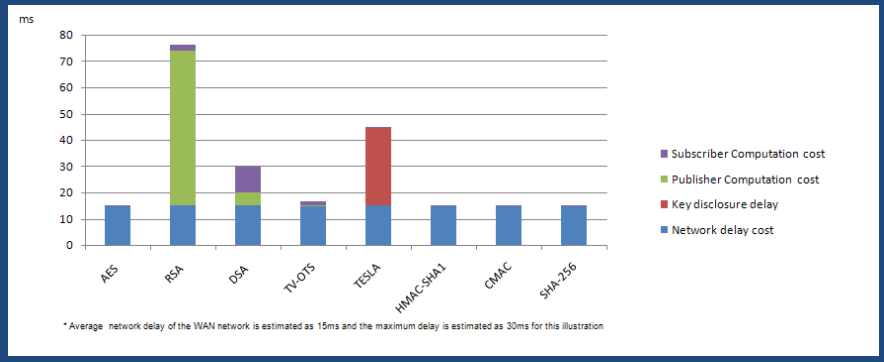


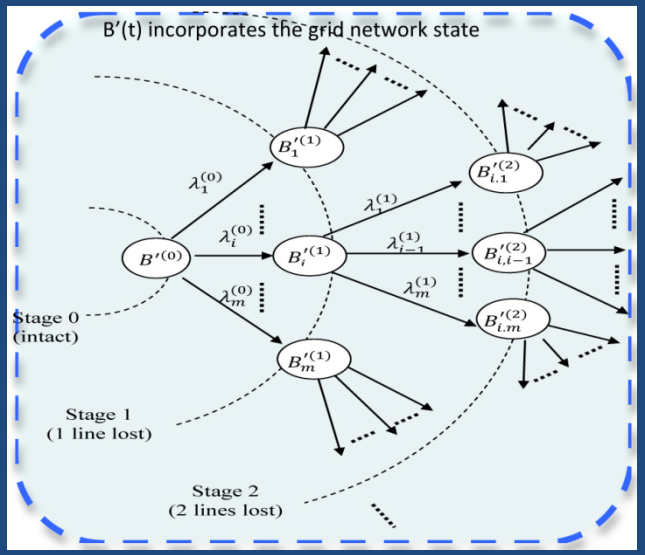


Cluster Accomplishments and Impact, cont'd

- Completed implementation and evaluation of multi-cast authentication protocols in GridStat, demonstrating general infeasibility of public-key based methods and promise of time-synchronized methods

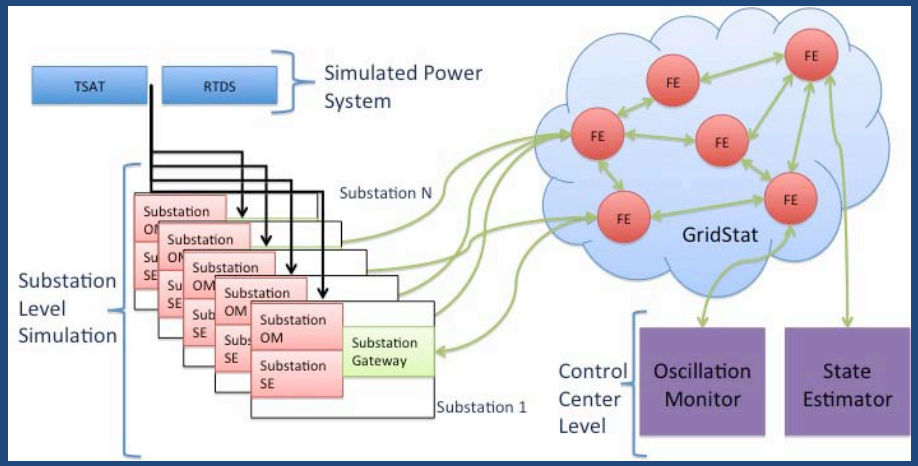
- Completed simulation package for analyzing vulnerability of grid in particular states to cascading failures

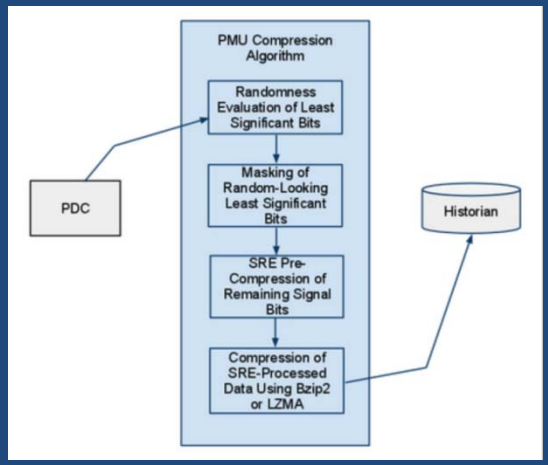




Cluster Accomplishments and Impact, cont'd

- Integrated GridStat data delivery framework with real-time power simulator and actual Smart Grid apps in creating GridSim, a virtual Smart Grid, for DOE
- Created a new PMU data compression algorithm that reduces the size of PMU archives by a factor of 20
- The IFS module achieved low performance overhead (3-4%) and 100% coverage for insider attacks while running common security applications such as SSH, WuFTP and NullHTTP on Linux





Cluster Activities Directions for Coming Year

- CONES: create emulations based on traffic analysis of networks in the field; implement CONES modules on lightweight, embedded devices
- GS Management Security and Trust: create computation models and algorithms for incorporating trust in power grid control decisions; implement inter-organizational authentication of devices
- PMU Integration: use of PMU values directly to improve situational awareness
- GS Applications: graph-theory-based vulnerability indices
- PMU compression: further validation and incorporation into an operational PMU archive
- Sensor networking models and primitives: study of performance of queries in the state-aware distributed database, specifically those related to identifying developing cascading failures and stopping them
- RSE: evaluate the ability of the RSE to resist power-grid attack scenarios, using the TCIPG testbed
- PMU Data Quality: Characterize the error, availability, and reliability of field measurements and phasor measurement devices; identify sensitivity of consuming applications to measurement errors.

Questions and Discussion