# TCIP: Trustworthy Cyber Infrastructure for the Power Grid

**William H. Sanders**
**University of Illinois at Urbana-Champaign**

DOE Office of Electricity Delivery & Energy Reliability

Visualization and Controls Program Peer Review, October 2006

Information Trust
INSTITUTE

# Scale of effort

- $1.5 M per year for 5 years (Total FY06 DOE funding: 125K)
- NSF/CISE, NSF/ENG, DOE, DHS
- 4 universities, 19 senior investigators
  - University of Illinois at Urbana-Champaign (14)
  - Washington State University (3)
  - Cornell University (1)
  - Dartmouth University (1)
- 19 member external advisory board (growing from 14)

# TCIP Vision and Strategy

- Provide the fundamental science and technology to create *an intelligent, adaptive power grid* which
  - survives malicious adversaries
  - provides continuous delivery of power
  - supports dynamically varying trust requirements.

- By:
  - Creating the cyber building blocks and architecture
  - Creating validation technology to quantify the amount of trust provided by proposed approach

# TCIP: Trustworthy Cyber Infrastructure for Power

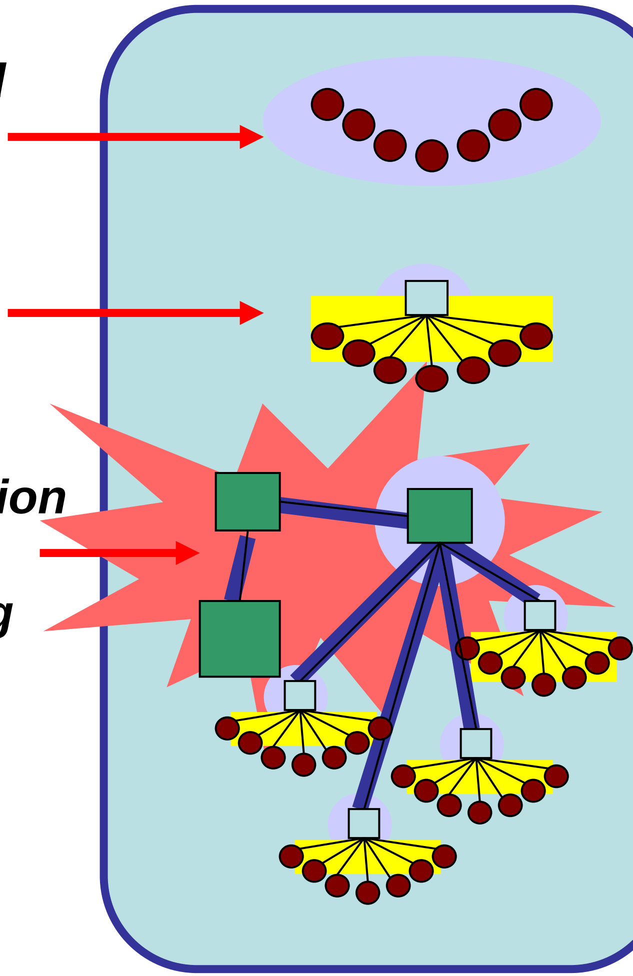
**Address technical challenges motivated by power grid problems in:**

**By developing science and technology in:**

***Ubiquitous exposed infrastructure***

***Real-time data monitoring and control***

***Wide area information coordination and information sharing***



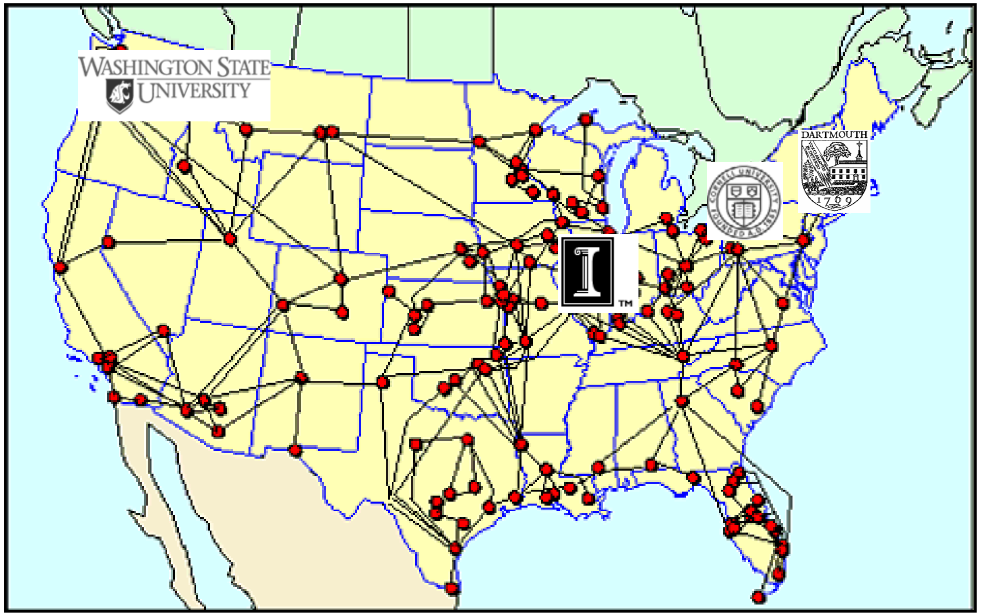
**Trustworthy Devices**

**Communication & Control Protocols**

**Quantitative Evaluation & Validation**

# TCIP Senior Investigators

- Trustworthy Devices
  - Gross, Gunter, Iyer, Kalbarczyk, Sauer, and Smith
- Communication & Control Protocols
  - Bakken, Bose, Courtney, Hauser, Khurana, Nahrstedt, Scaglione, Welch, Wang, Winslett
- Quantitative Evaluation & Validation
  - Campbell, Nicol, Overbye, Sanders, Thomas, Zimmerman



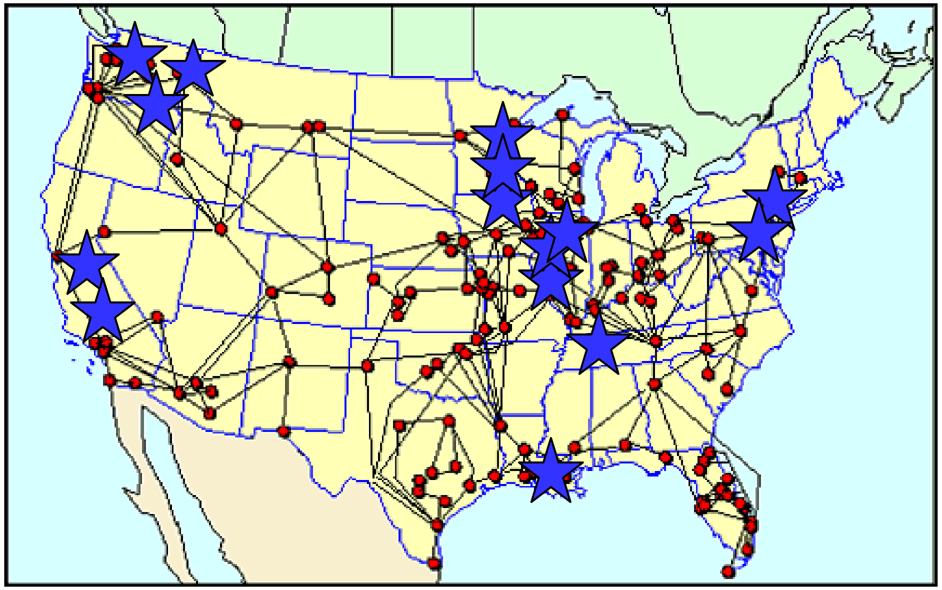

- Partner Institutions
  - Cornell
  - Dartmouth
  - University of Illinois
  - Washington State University

# TCIP Graduate Students

- Stian Abelsen (WSU)
- Musab AlTurki* (UIUC)
- Zahid Anwar* (UIUC)
- Angel Aquino-Lugo (UIUC)
- John Kwang-Hyun Baek (Dartmouth)
- Scott Bai (UIUC)
- Daniel Chen* (UIUC)
- Nihal D'Cunha (Dartmouth)
- Gabriela Jacques da Silva* (UIUC)
- Matt Davis (UIUC)
- Reza Farivar* (UIUC)
- Chris Grier (UIUC)
- Weining Gu (UIUC)
- Steve Hanna* (UIUC)
- Ragib Hasan* (UIUC)
- Joel Helkey (WSU)
- Alex Iliev (Dartmouth)
- Mohammad Khan* (UIUC)
- Shrut Kirti (Cornell)
- Jim Kusznir (WSU)
- Adam Lee* (UIUC)
- Michael LeMay* (UIUC)
- Suvda Myagmar (UIUC)
- Hoang Nguyen (UIUC)
- Thuy Nguyen* (UIUC)
- Hamed Okhravi* (UIUC)
- Karthik Pattabiraman* (UIUC)
- Sundeep Reddy (UIUC)
- Sankalp Singh* (UIUC)
- Evan Sparks (Dartmouth)
- Kim Swenson (WSU)
- Zeb Tate (UIUC)
- Patrick Tsang (Dartmouth)
- Erlend Viddal (WSU)
- Long Wang* (UIUC)
- Erik Yeats (WSU)
- Jianqing Zhang (UIUC)

* Not funded by TCIP, but working on TCIP

# Partnerships – Spanning Stakeholders



## Technology Providers

**ABB** – Industrial manufacturer and supplier
**Siemens** – Industrial manufacturer and supplier
**AREVA** – Major SW vendor for utility EMS systems
**Cisco Systems** – CIP Researchers
**GE Global Research** – Research in communication and computing requirements for US power grid
**Honeywell** – Industrial control system provider and SCADA researcher
**KEMA** - Supports clients concerned with the supply and use of electrical power
**OSII** – Major SW vendor for utilities including SCADA and EMS systems
**PowerWorld Corp** – System analysis and visualization tools
**Schweitzer** – Industrial control system provider
**Starthis** – Automation Middleware
**PNNL** – National Lab doing SCADA research

## Electrical Power Generation & Delivery

**Ameren** – Major traditional utility in Mo. and IL
**Entergy** – Major traditional utility in South
**Exelon** – Major traditional Utility – Midwest & East
**TVA** – Largest public power company

## Regional Management

**CAISO** – Independent system operator for CA
**PJM** – Regional transmission organization (RTO) for 7 states and D.C.
**EPRI** – Electric Power Research Institute

# Broader Impact to other Process Control Systems

- Embedded computing base to enforce trust properties
- Efficient, timely and secure measurement and aggregation mechanisms
- Adaptable performance/security policies for normal, attack, and emergency condition
- Scalable, tunable, inter-domain authorization
- Fundamental principles for security in emergency conditions
- Security metrics, multi-scale abstractions for measurement-based attacks models to emulate real scenarios

# Technical Challenges

1. **Trustworthy Devices**: cybersecurity of low-level devices and their communications.
    - Sheer number of devices to be secured
    - Cost of securing them
    - Performance impacts of security on the devices' functionality
2. **Communication and Control Protocols (1)**: efficient, timely and secure measurement and aggregation mechanisms for edge device data.
    - Challenge: devising and implementing adaptable policies and mechanisms for trading off performance and security during
        - Normal conditions
        - Cyber-attacks
        - Power emergencies

# Technical Challenges

3. **Communication & Control Protocols (2)**:
    - Mechanisms for scalable inter-domain authorization
    - Fundamental principles for security in emergency situations.
    - Approaches
        - Dynamic negotiation under normal, attack and emergency conditions
        - Mechanisms to exploit the trusted computing base.
4. **Quantitative Evaluation & Validation**: validate the TCIP designs and implementations produced in the other areas.
    - create security metrics, multi-scale abstractions and attack models
    - emulation technology to allow quantitative analysis of real power grid scenarios.

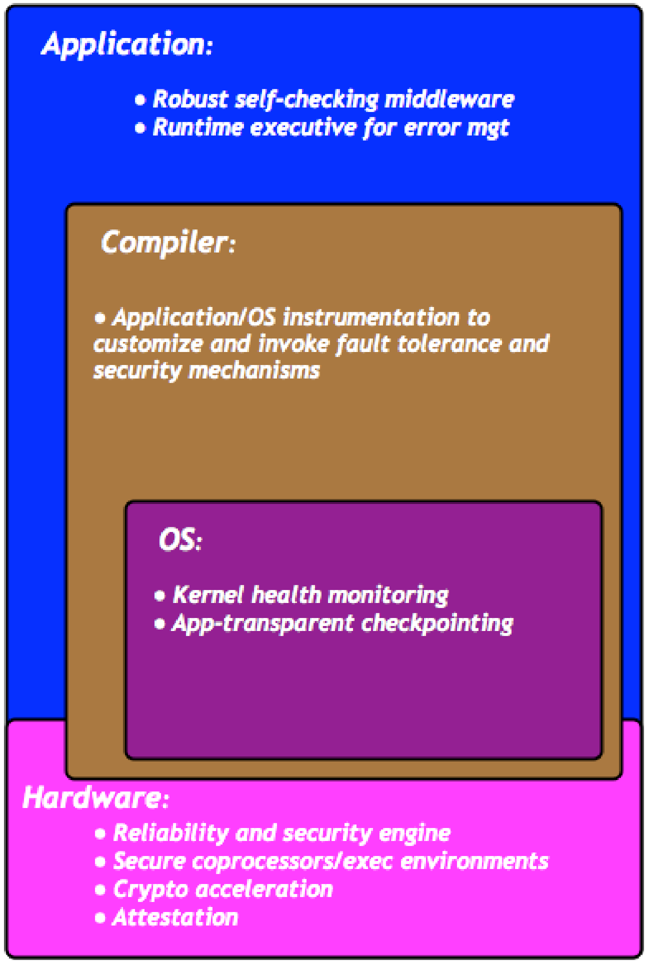
# Challenge: Trustworthy Devices

Vision:
- *Systematically transform the computing base*
- for *holistic application security and reliability*

Main idea:
- Derive *application-centric checks*
- *embed them* in the HW
- *access them* with OS/middleware support
- *validate* them in power-grid cyber infrastructure

Considering:
- Both COTS and new architectures
- *technical challenges* raised by deployment/management


Team Background:
- *Reliability and Security Engine*
- *fast crypto*, with replication
- *IBM 4758* design, validation, apps
- open-source *TCPA/TCG* platform and apps
- Sun *"Center of Excellence";* TCG, OS, PKI



# Technical Accomplishments: Trustworthy Devices

- Developed a secure (and extensible architecture) for intelligent meters with bi-directional communications to the electricity service provider (UI; Gunter)
  - Developing secure architecture for meters used in automated meter reading systems
- Developed hardware mechanisms to enable trustworthy sharing of and computation on private data (Dartmouth; Smith)
  - Created tiny trusted third parties: T3Ps
- Built Integrated HW/SW framework to support reliability and security services (UI; Iyer & Kalbarczyk)
  - Reconfigurable operating system-level kernel module to support OS/application aware security and reliability services
  - Reconfigurable processor-level hardware framework to support security and reliability – Reliability & Security Engine

# Challenge: Control Area Framework

**Requirement:** **Protection of sensitive data, state information,**

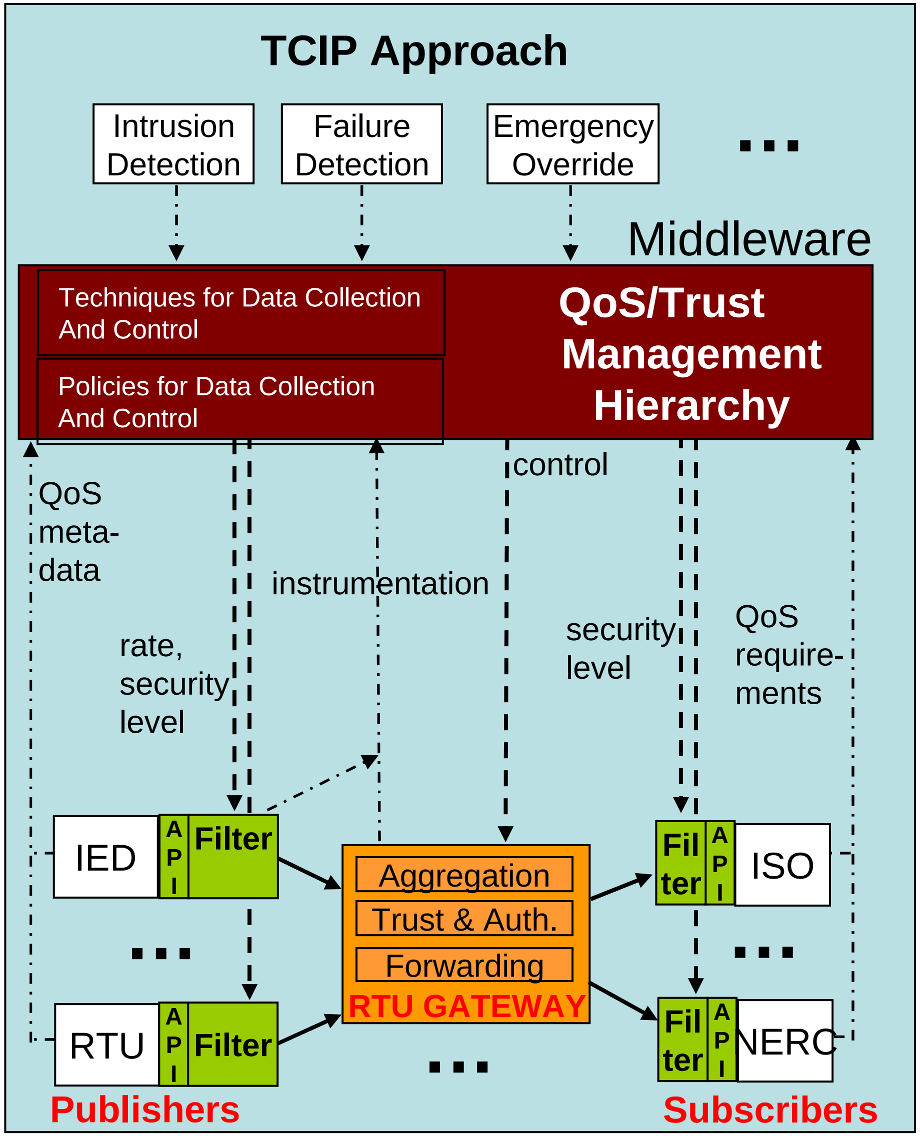
**TCIP Approach:** Develop control area framework TACC for trustworthy data, state collection, sharing and control

**Challenges:**

- *Integrated* secure, reliable, and real-time TACC framework
- *Usable* trust mechanisms in power system context

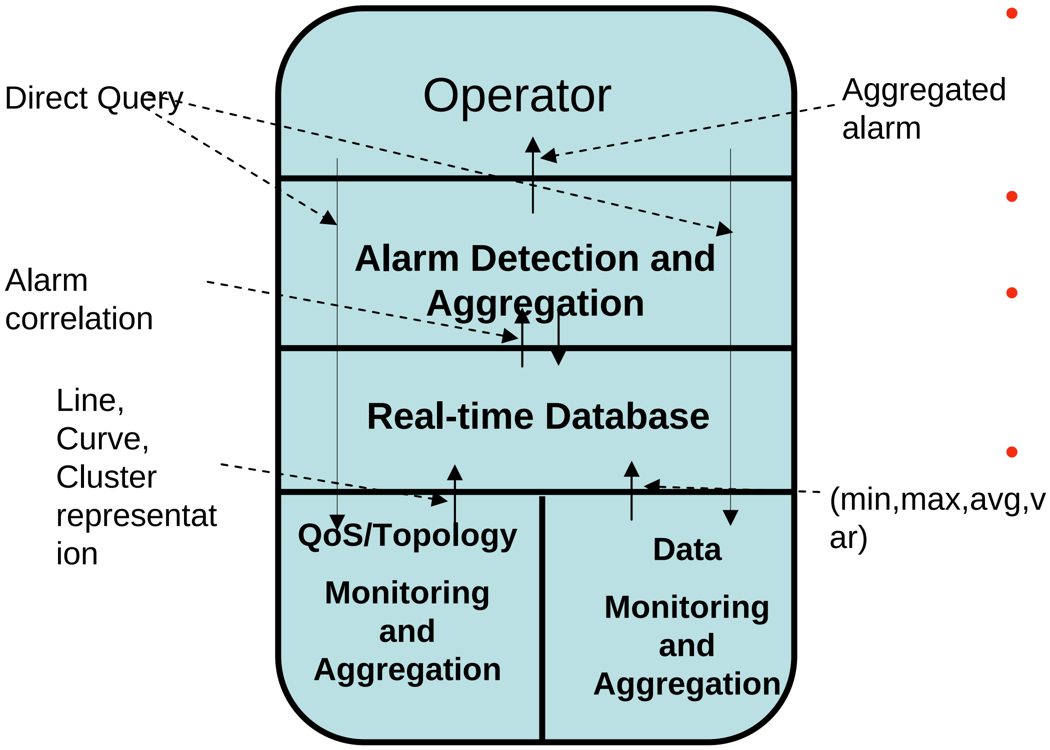
**Issues:**

- *Architectural constructs* to make trust compatible with operational needs
- Detector benefits from *aggregation techniques*
- QoS/trust *policy dependability* due to hierarchy




**Trustworthy Aggregation for Collection and Control (TACC)**

# Challenge: Integrated QoS/Data/Alarm Aggregation Architecture




- **Requirement 1:** Accurate reflection of SCADA system state
- **Goal:** Satisfy Requirement 1, i.e., create *efficient aggregation techniques* for integrity-secure power status data and network state information collection
- **TCIP Approach:** Hierarchical and Appropriate state aggregation
- **SCADA system state:**
  - Bandwidth, delay, network topology
  - Breaker status, voltage, current, phase
- **Aggregation techniques:**
  - **Sampling techniques**:
    - Phase by phase
    - Round-robin
    - Selective/Partial sampling
  - **One dimensional data**
    - (Min, Max, Average, Variance)
  - **Multidimensional data**
    - Computational Geometry techniques
    - AI Learning Techniques
    - Probabilistic Techniques

# Technical Accomplishments: Protocols

- Developing an architecture and set of algorithms to support malfunction detection in SCADA networks caused by software update from vendors, faulty devices, or malicious attacks. (UI; Nahrstedt) Observations to date:
  - Communication delay and change detection delay contribute significantly to the total detection delay, and are not independent.
  - Certain forms of aggregation perform (e.g., quantized aggregation) better than others (e.g., average aggregation) in low bandwidth networks.
- Completed initial prototype of Gridstat; currently extending it with policy and reliability mechanisms as well as designing and implementing new approaches to redundant, bounded-delay routing (WSU; Bakken, Bose, Hauser)
- Completed conceptual design of a framework for dynamic and composable trust (WSU; Bakken, Bose, Hauser)

# Challenge: Integrated Simulation Testbed

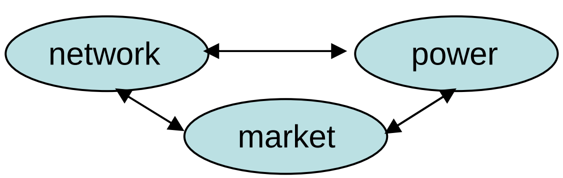
**Goal**: Integrate electrical, market, and communication simulators

**Challenges**:

- Time scales are different
- Data abstractions / formats are different
- Existing simulators lack expression of inter-dependency

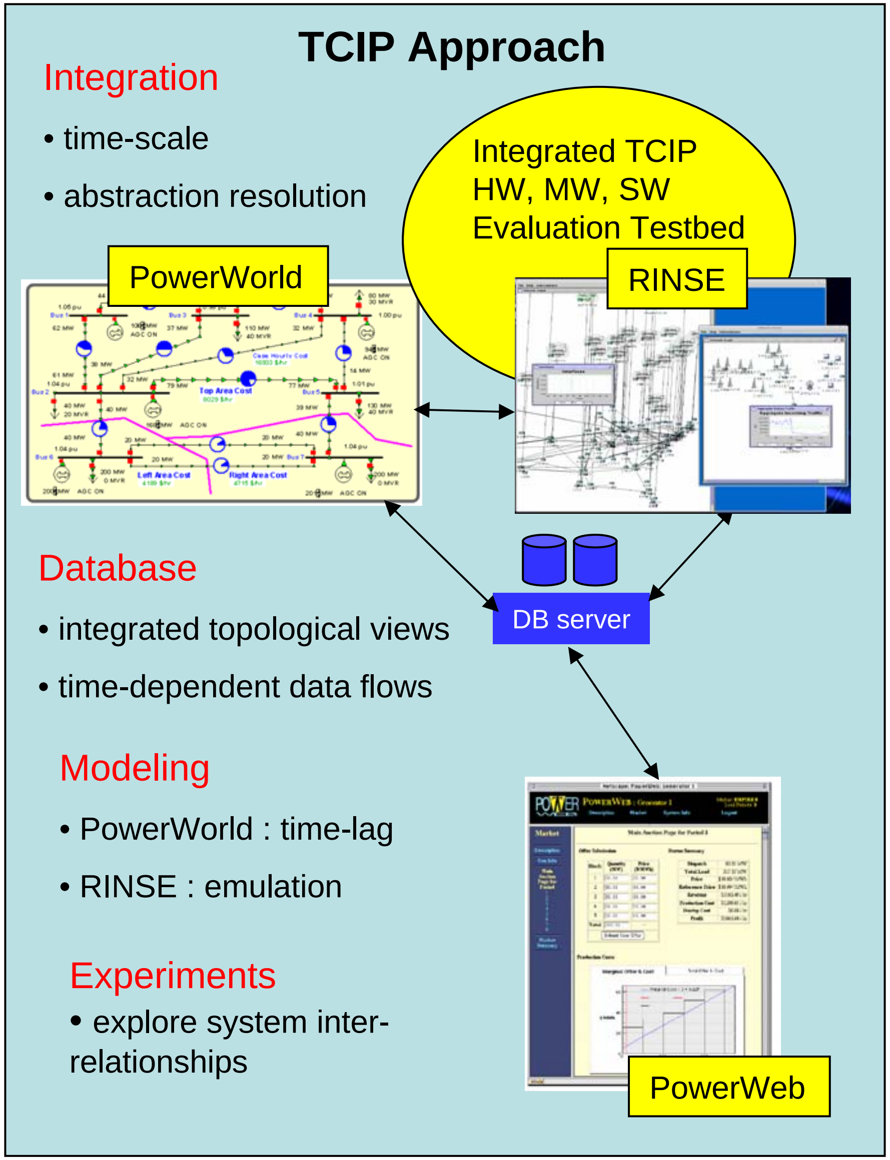
**Issues**:

- Can we make power simulation computations dependent on communication characteristics?
- Can we integrate data from different simulators?
- Capture interdependencies




**Broader contexts**

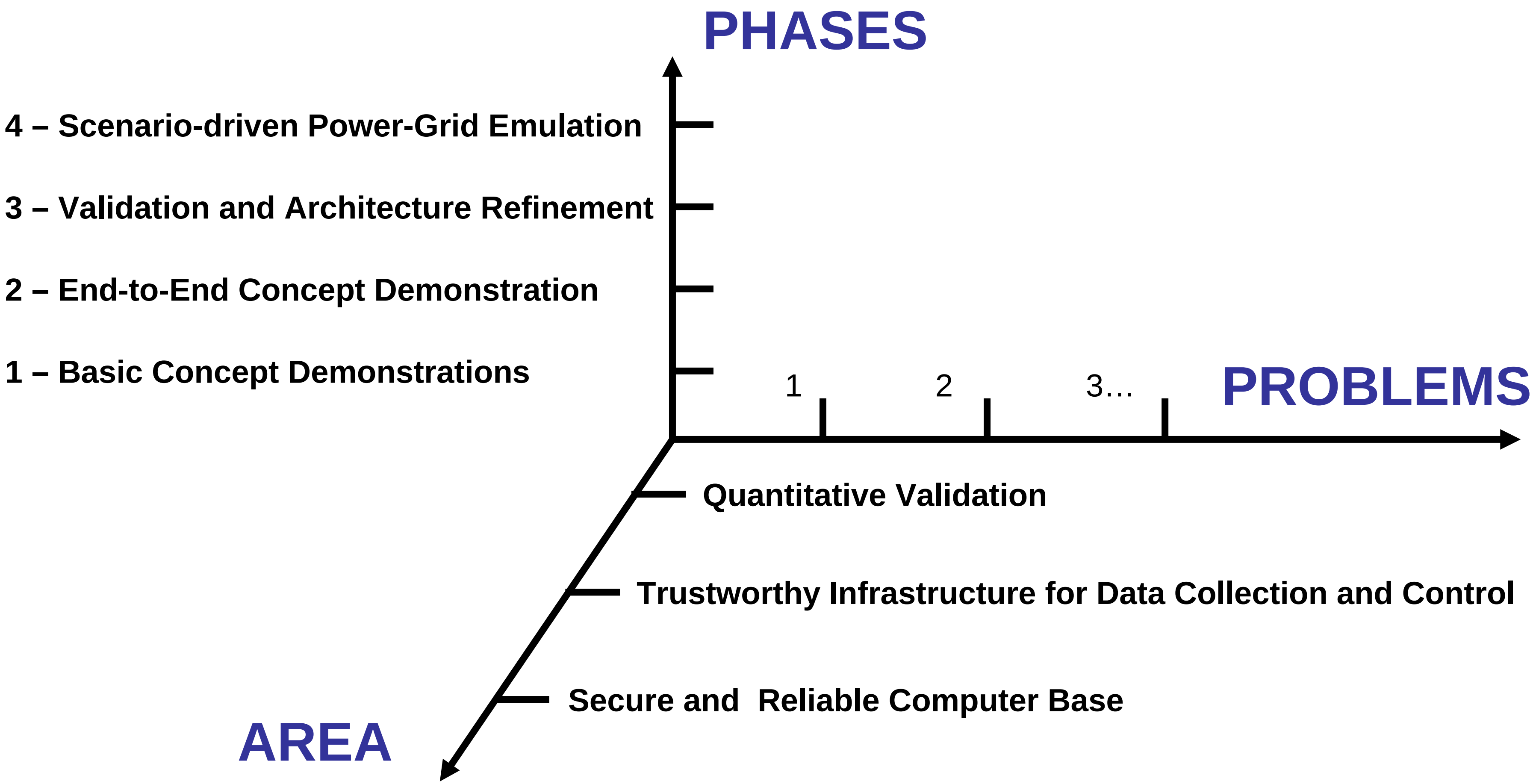
- Integration of general data inter-related simulations



# Technical Accomplishments: Validation

- Integrated Multiple Simulators together:
  - Linked of RINSE with PowerWorld and PowerWeb, using OpenVPN technology for packet capture. (UI; Nicol)
  - Extending the Development of the PowerWeb Test Platform to integrate with the RINSE network simulator (Cornell; Thomas et al.)
- Provided New Simulation Capabilities:
  - Integrated PowerWeb with RINSE, allowing market-based network traffic to be read/manipulated in transit (Cornell)
  - Adapted Gridstat Code to operate in the SSFNet environment, a close relative of RINSE. (WSU)
  - Building software that can be used to model various parts of the power system Currently implementing the 61850 protocol and are beginning to model devices. (UI; Overbye)
  - Greatly reduced the execution cost of simulating large-scale worm attacks, by exploiting the fact that simulated worm payloads are not important, and we can optimize worm traffic passing through the network (UI; Nicol)

# Multi-Axis Integration of Research



# For more information

http://tcip.iti.uiuc.edu

whs@uiuc.edu