TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

tcipg.org

Research Activity Fact Sheets

November 2011

University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Table of Contents – Activities Listed by Research Cluster Page No.

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Overview of the TCIPG Center

tcipg.org

What TCIPG Does, Why It's Needed

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure, which in turn depends on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. These risks may come from cyber hackers who gain access to control networks or create denial of service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors. Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, the University of California at Davis, and Washington State University are together addressing the challenge of how to protect the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, resilient, and safe. TCIPG is funded by the U.S. Department of Energy and the U.S. Department of Homeland Security.

TCIPG Research Clusters:

- Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
- Trustworthy cyber infrastructure and technologies for active demand management
- Responding to and managing cyber events
- Risk and security assessment

TCIPG Cross-Cutting Efforts:

- Education
- Testbed and evaluation methodologies
- Industry interactions and technology transition

How It Works

In the cluster on Trustworthy Cyber Infrastructure and Technologies for Wide-Area Monitoring and Control, TCIPG researchers are working on security, key management, quality of service, data management, data compression, application robustness, and network robustness applied to PMU networks, PMU data, state estimation, transmission topology, and power line communications.

The cluster on Trustworthy Cyber Infrastructure and Technologies for Active Demand Management focuses on improving overall power system performance. As the power grid transitions to a system with larger amounts of less-dispatchable renewable generation, control that previously resided on the generation side will need to be transitioned to the load. The impacts of load control for both real and reactive power are being considered.

The cluster is pursuing research in three main areas. First is the determination of how the real and reactive power load should be modified to accomplish control, including use of nonintrusive methods for determining the load composition (and hence its potential controllability) while also providing the potential for privacy protection. Second is the determination of the best means for enabling the monitoring and bidirectional communication needed to accomplish that control, with a specific focus on electric vehicles. Finally, the cluster is also working on AMI intrusion detection to maintain a secure control system.

The cluster on Responding to and Managing Cyber Events focuses on cyber attacks, particularly tools and technologies for responding to and managing cyber attacks. Most recently, TCIPG research in this area has focused on design of semi-automated intrusion detection and response techniques. More specifically, the researchers are developing a Recovery and Response Engine that makes use of game theory techniques to provide optimal responses to cyber attacks.

The cluster on Risk and Security Assessment has been working on extending TCIPG's current testbed for experimental evaluation of attacks and monitoring strategies; designing and setting up an example substation network using actual substation equipment; and extending and releasing a suite of software solutions that includes tools designed for formal program analysis (SymPLAID), dynamic runtime process patching (Katana), interactive packet manipulation (Scapy), firewall rule validation (NetAPT), intrusion detection on embedded systems (Autoscopy Jr.), and highly scalable network simulation (S3FNet), among others.

TCIPG has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.

Where It Stands

Impact is being made at all levels in the project. Together, TCIPG innovations provide clear directions toward a next-generation IT infrastructure for the power grid that is resilient, timely, and secure, supporting the continuous functioning of the nation's electric power infrastructure.

Industry Interaction Board

The involvement of industry and other partners in the TCIPG project is vital to its success, and is facilitated by an Industry Interaction Board (IIB). For more information, see the TCIPG website at tcipg.org, or contact the TCIPG leaders listed below.

Leadership

- **Director:** William H. Sanders (whs@illinois.edu)
- **Industry Partnerships & Technology Transfer:** Peter W. Sauer (psauer@illinois.edu)
- **Managing Director:** Al Valdes (avaldes@illinois.edu)
- **Site Coordinators:** Carl Hauser (hauser@eecs.wsu.edu), Anna Scaglione (ascaglione@ucdavis.edu), Sean W. Smith (sws@cs.dartmouth.edu), and Robert J. Thomas (rjt1@cornell.edu)

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Research Cluster

Trustworthy Cyber Infrastructure and Technologies for Wide-Area Monitoring and Control

Trustworthy Cyber Infrastructure and Technologies for Wide-Area Monitoring and Control Page No.

Cluster Lead: Carl Hauser ..... hauser@eecs.wsu.edu

CONES – Converged Networks for SCADA

Overview and Problem Statement

The CONES project is a TCIPG activity exploring many aspects of network convergence as they apply to power grid cyber networks. Many currently deployed cyber-communications systems in the electric sector consist of multiple communication networks and devices to carry out communications. That is an expensive and inefficient approach, but trying to achieve convergence simply by replacing those channels with a single high-bandwidth connection would also create problems. Those problems include the inability to segregate channels, guarantee timings, and enforce network entry limitations. CONES attempts to address those problems using as much off-the-shelf hardware and software as possible, augmenting them with specialized components when necessary. This project has already been successful in identifying and solving several of the problems in this space, and is actively transferring the knowledge gained to various industry partners. At the same time, CONES research is continuing to explore and refine more convergence techniques.

Research Objectives

- Enable network convergence for control system applications (e.g., SCADA, monitoring, engineering).
- Explore and understand networking needs for existing and future electric sector communication networks.
- Provide solutions to problems not currently addressed.
- Identify best practices and off-the-shelf technologies for convergence in the electric sector.
- **Smart Grid Application Area:** Communications technology.

Technical Description and Solution Approach

- Work with research, government, and industry partners to identify current needs in communications networks, and examine trends in equipment requirements to identify future networking requirements.
- Compare the gathered requirements and data on modern communication networks, identifying solutions or partial solutions for use in the electric sector. This step will also identify areas in which new solutions are needed in order to meet the requirements fully.
- Create solutions, based on minimal customization of off-the-shelf components, that will meet the identified needs of the electric sector. This process includes not only building technology, but also vetting it with current equipment manufacturers' compliance issues and technical issues previously unknown to the researchers.

Results and Benefits

- Soft-real-time process and network scheduling in Linux kernel: this gives devices the ability to report even under duress.
- Identification of a realistic traffic profile in electric sector communications networks, for future research.
- Identified many security concerns for electric sector communications, particularly if they are converged.
- Created many software tools useful to the wider TCIPG research mission.
- **Partnerships and External Interactions:** Entergy, PNNL, GPA, TVA, NASPI.
- **Technology Readiness Level:** Lessons learned and techniques already being transferred; software results currently in use in other research.

Researchers

- Erich Heine, eheine@illinois.edu
- Tim Yardley, yardley@illinois.edu
- Klara Nahrstedt, klara@cs.uiuc.edu

Industry Collaboration

- Grid Protection Alliance

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Cooperative Congestion Control in Power Grid Communication Networks

Overview and Problem Statement

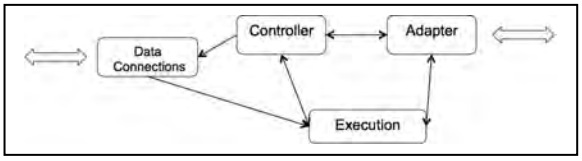
- Real-time guarantees (end-end latency deadlines and critical data loss rate) of PMU flows can be violated when transient congestion occurs in the NASPInet.
- Congestion of traffic in the power grid communication network (NASPInet) can be caused by:
  - Variable compression of the PMU data or other sensory data.
  - Increased sending rate of real-time (RT) PMU flows due to unexpected critical events/observations in their sensory space.
  - Changing demands by control centers due to extended power grid state analysis, causing changes in traffic shapes of RT flows.

Research Objectives

- Provide a Cooperative Congestion Control framework to be used in the NASPInet.
- Protect the real-time guarantees of the PMU flows during transient instability periods.
- Utilize the cooperative nature of the nodes in the NASPInet and the flows that originate from the same substation.
- **Smart Grid Application Area:** Wide Area Monitoring and Control

Technical Description and Solution Approach

- Cooperative Congestion Control (CCC) Framework
  - Multiple service class queuing,
  - Cooperative real-time flow scheduling and BW reassignment, and
  - Cooperative coordination and back pressure approaches among neighboring nodes to counter the transient congestion state.
- CCC framework includes:
  - Overlay router/ phasor gateway design
  - Congestion notification protocol

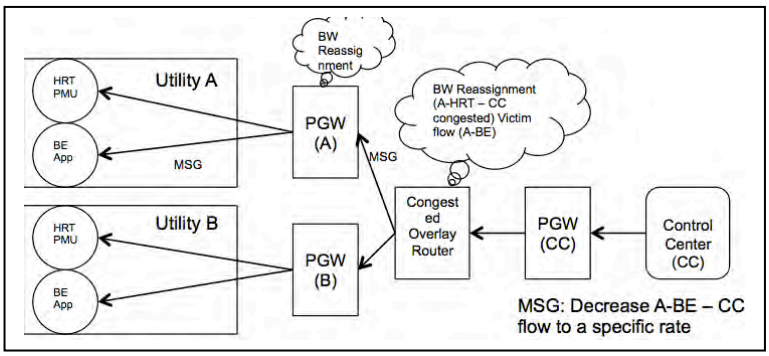


Router Components

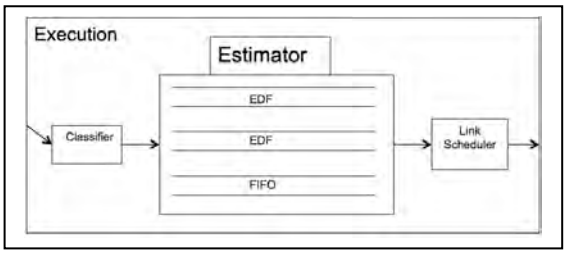
Adapter unit:

The adapter is the primary component where the BW reassignment algorithm and cooperative coordination protocol reside. Its main responsibilities include:

a. Maintaining the link sharing queue hierarchy and updating statistics periodically,
b. Adapting to any transient congestion occurrence by bandwidth reassignment, and
c. Communicating with the adapters of neighboring nodes, notifying them about the new rate (BW) assignments.



Congestion Notification Protocol

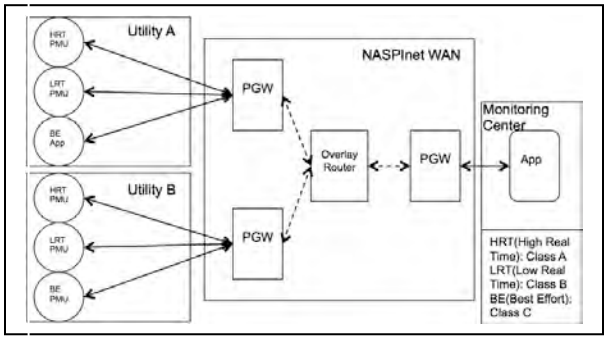


Execution Component

Results and Benefits

- **Technology Readiness Level:** Modules available for deployment

  - At t = 0, all flows start with an initial frequency of 20 Hz.
  - At t = 40 sec, the Utility A's HRT PMU sensor increases its frequency to 40 Hz.
  - Later, at t = 60 sec, Utility B's HRT PMU sensor increases its frequency to 40 Hz.
  - At t = 80 sec, Utility A's HRT PMU and Utility B's HRT PMU increase their frequencies to 50 Hz.
  - Finally, at t = 90 sec, Utility A's HRT PMU and B-HRT PMU increase their frequencies to 60 Hz.



Evaluation Scenario

Flow	0 – 40	40 – 60	60 – 80	80 – 90	90 – 100
A-HRT	0%,0%	50%,4%	50%,0%	40%,1.8%	33%,0%
A-LRT	0%,0%	0%,0%	0%,0%	0%,1%	0%,0%
B-HRT	0%,0%	0%,0%	50%,3%	40%,1%	33%,0%
B-LRT	0%,0%	0%,0%	0%,0%	0%,1%	0%,0%

% of deadline missed packets (flow vs. time interval in sec) without and with CCC framework

Our CCC framework made it possible to achieve real-time guarantees of the PMU flows during the transient instability period (between 40th and 100th sec).

Researchers

- Naveen Cherukuri, naveen.cherukuri@oracle.com
- Klara Nahrstedt, klara@cs.illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Decentralized Sensor Networking Models and Primitives for Smart Grid
Part I: Metrics of Grid Vulnerability to Cascading Failures
Part II: State-Aware Distributed Database Systems

tcipg.org

Overview and Problem Statement

Enhanced measuring/monitoring systems can improve grid security and resilience. This project is focused on data use and data management for Smart Grid applications.

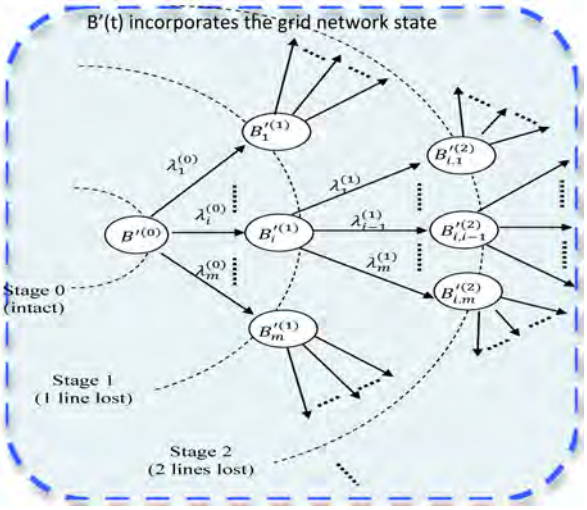
Research Objectives

Our specific objectives are as follows:

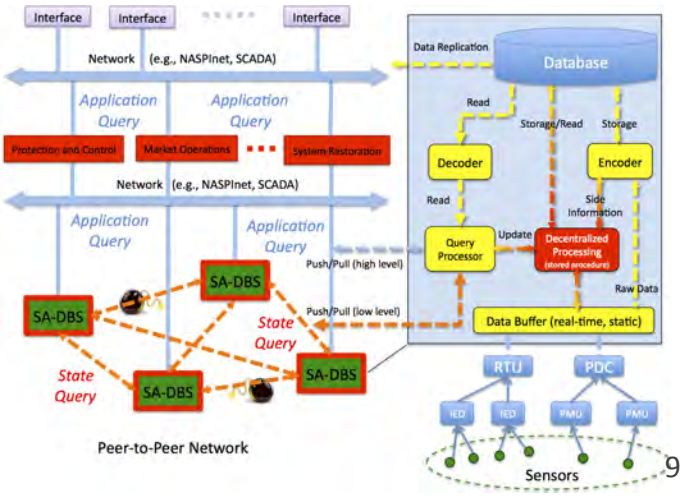
1. Regarding the use of Smart Grid data, we derived metrics that gauge the vulnerabilities of the grid that are based on first- and second-order statistics of the line flows.
2. Considering the problem of managing large amounts of sensor information, we proposed a scalable decentralized (peer-to-peer) architecture to store, process, and deliver the data reliably and rapidly. The key idea is to exploit the structure of the data and the class of queries that are typical of cyber-physical systems (CPS).

Technical Description and Solution Approach

Part I – Metrics of grid vulnerability to cascading failures: We have developed a stochastic model to study cascading failures in power grids. In our model, the grid state is conditionally Markovian, given a certain line flow. The transition rates of the line from the on to off state depend on the sojourn time of the line flow above the overload threshold of the line switch. We used the statistics of the sojourn time of line flows, derived from a Gaussian model, to obtain the expected active time of the line. These expected times provide a metric of the risk of cascading failures and also the time margin to perform corrective action. In our study, we derived the first- and second-order statistics of the flows from a DC power flow model applied to the load and generation data. However, in the future, we plan to use flow measurements and sensor data to compute the metric online directly.



Part II – State-aware distributed database systems: The Smart Grid is going to produce an enormous amount of data that stream continuously from the sensors to the database that is set to contain them. The management of this database is a critical problem, since the integrity and accessibility of the data are a potential bottleneck for putting them to good use. We have investigated how to further develop the concept of peer-to-peer (P2P) architectures to specifically address the needs of the power grid cyber-physical infrastructure. P2P architectures are generally more scalable and resilient than the centralized client-server architectures. The new architecture we propose for streaming P2P



Database Systems (DBS) that will be generally useful for Cyber-Physical Systems (CPS) is called "State-Aware" Distributed DBS (DDBS). The SA-DDBS comprises a stored routine for decentralized state estimation and a data representation and archival model that utilizes the stored routine to obtain 1) a reliable and flexible data replication mechanism and 2) a faster method for querying measurement data across the SA-DDBS. In particular, the state information will always be one "hop" away from any application client. Furthermore, using consistent state information across the DBS as well as storage codes that encode measurement residuals, the SA-DDBS will provide reliable access to the archived records in an efficient way.

Results and Benefits

- **Part I – Metrics of grid vulnerability to cascading failures:**
  The project has been completed, and its results include:
  - A model of grid states as conditionally Markovian, given the process of line flows F(t).
  - A model for the line flow statistics, using measurement data on generation/loads.
  - New vulnerability measures. The metric developed is the expected active time of each line before the advent of a line trip.
  - Experiments and validation of the model proposed.
  - Software tools for vulnerability analysis and a simulation package have been developed.
- **Part II – State-aware distributed database systems:**
  Initial experiments involve the "stored procedure" to distribute state information in the DBS:
  - Decentralized state estimation via gossiping.
    - The procedure is effective for establishing the proposed P2P SA-DDBS architecture.
    - It leads to convergent estimates across the whole network with simple local communication and computations.

  The results also include the basic encoder/decoder model that utilizes the system state as side information to improve storage efficiency.
- **Technology Readiness Level:** The power grid cascading failures analysis tools we developed are ready to distribute; the other research results are in the phase of theoretical development.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Robert J. Thomas, rjt@cornell.edu
- Zhifang Wang, zfwang@ucdavis.edu
- Xiao Li, eceli@ucdavis.edu

Industry Collaboration

- Worked with PNNL on Part I: Metrics of grid vulnerability to cascading failures.

GridStat Middleware Communication Framework: Application Requirements

Overview and Problem Statement

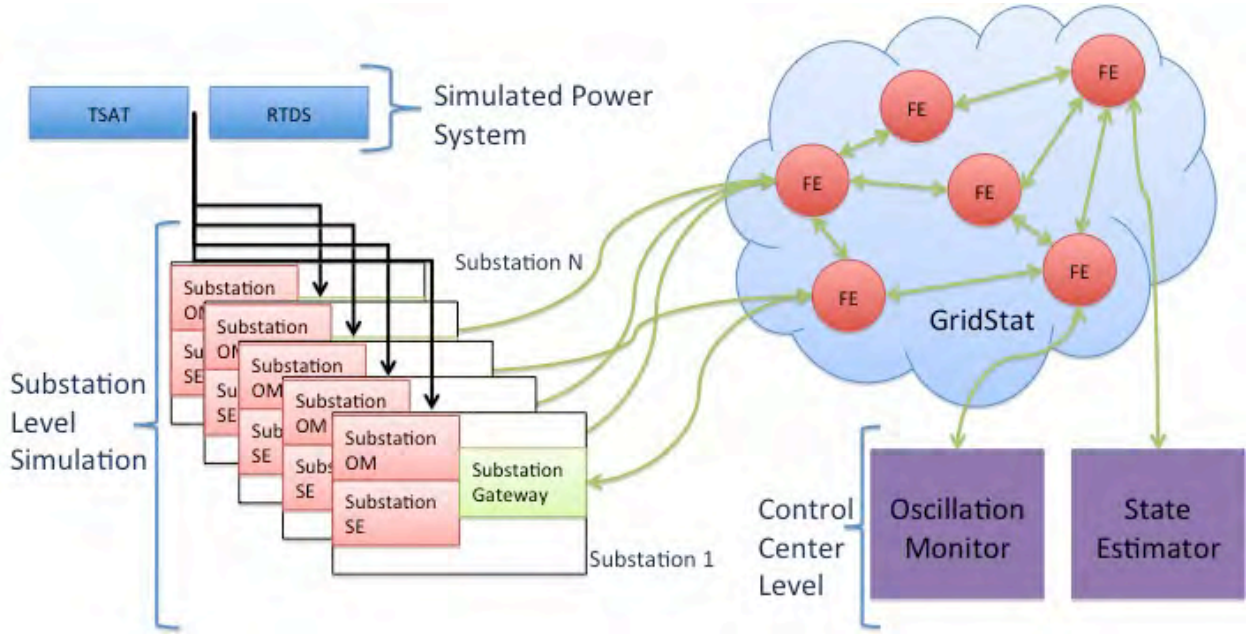
Due to changing requirements of the power grid and new opportunities for wide-area, real-time control, data delivery is required in a reliable, timely, and secure manner. GridStat is a middleware framework architecture tailored for power system data delivery. Power system applications set specialized requirements in terms of delay, rate, availability, etc., and GridStat needs to be tested and validated to meet the specific application requirements.

Research Objectives

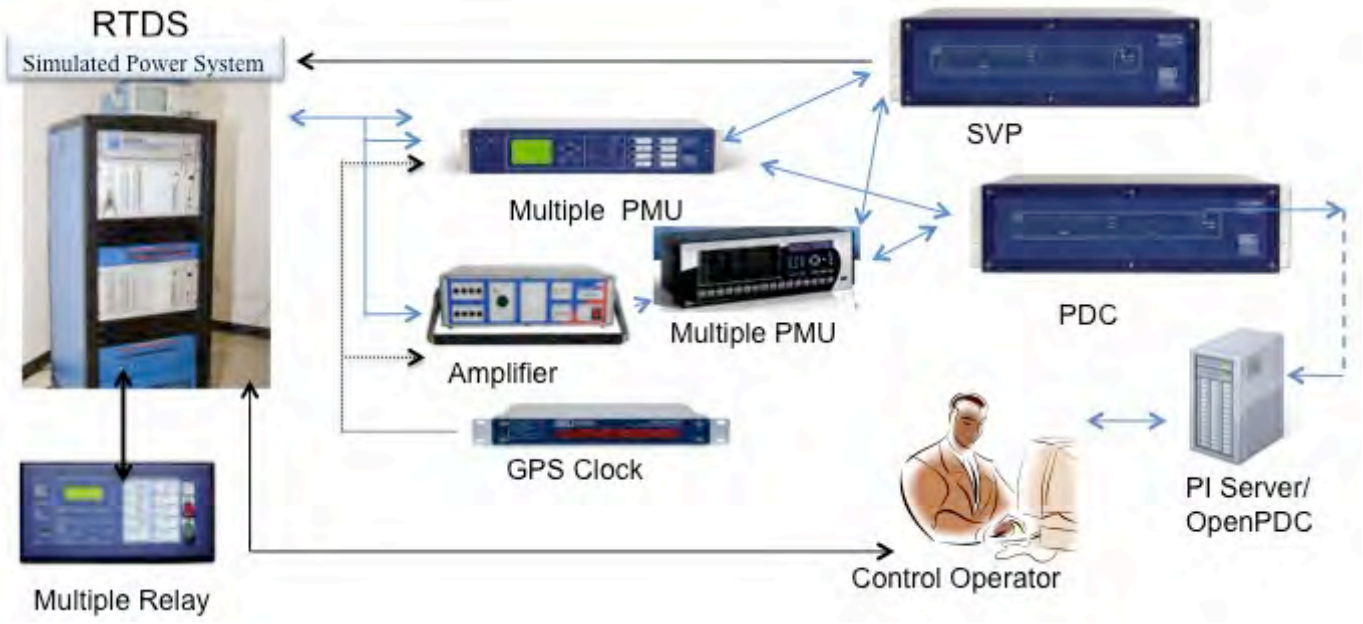
- Understand the real-time communication requirements for power system applications for the emerging smart grid.
- Develop a technical approach to assess these requirements.
- Develop a testbed integrating power grid, sensors, communication, and applications to create real-life scenarios to validate the GridStat middleware communication.
- **Smart Grid Application Area:** Communication substrate for wide-area monitoring and control of the bulk power system.

Technical Description and Solution Approach

- Based on our earlier work in developing the GridStat prototype and smart grid applications (supported by other research funds), efforts are in place to integrate the power system simulators, communication network, and application.
- Approach is to model and do integrated simulation in real time. (Part of the effort is separately funded by DOE.)



- A real-time testbed is also being developed using a real-time digital simulator to interface with GridStat.
- Transmission-level Smart Grid applications (state estimator and oscillation monitor) have been developed with the support of DOE and industry partners.



- A second effort is focused on developing graph theory-based vulnerability indices for the power grid and validating them with DC- and AC-power flow indices.

Results and Benefits

- Hierarchical Linear State Estimator has been developed (funded by TCIP and TCIPG).
- The GridSim project (separately funded by DOE) uses GridStat to integrate the TSAT power system simulator with the Hierarchical State Estimator application and a separately developed oscillation monitor.
- RTD-based testbed development is in progress (partially funded by TCIPG).
- Graph centrality-based algorithm has been validated against DC sensitivity-based algorithm. Comparison with full AC power-flow-based algorithms is in progress.
- **Partnerships and External Interactions:** SEL, NASPI, GE, RTDS, PowerTech, Schneider.
- **Technology Readiness Level:** Research in progress.

Researchers

- Carl H. Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Anjan Bose, bose@eecs.wsu.edu
- Anurag Srivastava, asrivast@eecs.wsu.edu

Industry Collaboration

- SEL, NASPI

GridStat Middleware Communication Framework: Management Security and Trust

Overview and Problem Statement

It is generally recognized that a high-bandwidth and highly available networked communication system should overlay the transmission system topology to enable new types of control and protection applications that will make the grid more efficient and more reliable. Those applications will make use of data originating at many locations in the grid, which may be under the control of operators with various levels of competency and motivation, or even under the control of attackers. The research in this activity addresses two aspects of cyber security in this emerging environment. The first is that of *message origin authentication* when the data delivery model is multicast. This is a challenging technical problem for which various solutions exist, but all exhibit trade-offs between multiple quality of service dimensions, so there is no universally best solution. The second aspect concerns how to make control decisions using information from sources whose trustworthiness is unknown a priori. We observe that, in any system the size of the power grid involving thousands of participating entities, security will inherently be imperfect and uncertain. The approach being pursued here attempts to use trustworthiness assessment in combination with decision theory to make good control decisions, even in the face of uncertainty about the trustworthiness of some inputs.

Research Objectives

- Assess the ability of a variety of multicast data origin authentication protocols to meet quality-of-service requirements for smart grid applications.
- Make several multicast authentication protocols available in the GridStat framework, allowing application designers to choose a protocol that best meets the application's needs.
- Develop a mathematical model or models for trust assessment and decision-making that are appropriate for use in power grid control settings.
- Design approaches to trust data collection for power grid devices and participants so as to be able to usefully instantiate the models and maintain the instantiations over time.
- Incorporate instantiated trust models as part of the security design of wide-area control systems.
- **Smart Grid Application Area:** Wide area monitoring and control.

Technical Description and Solution Approach

- We are assessing the security and performance characteristics of several multicast authentication protocols from the literature using analysis and experimentation. Included protocols are HMAC, CMAC, RSA, DSA, TESLA, and TV-OTS. For each, we are evaluating publisher and subscriber computation costs, key disclosure delay, and network delay leading to assessment of latency.
- We are implementing a selection of protocols in the GridStat framework using the previously designed and implemented modular security system (see poster and demo).
- Trust models investigated thus far include a Bayesian probabilistic estimation model for incorporating trust information and its uncertainty and a new ranking-based approach that provides useful, if less complete, trust input to decision-making while requiring less input information (see poster).

Results and Benefits

- Multiple multicast message authentication protocols are now available in the GridStat data plane.
- Paper on multi-cast message authentication trade-offs and guidance to appear in the security track of the power systems symposium at HICSS-2012.

- Paper on the Bayesian trust framework presented at the IFIP WG 11.10 Conference in March 2011, to appear in the *Proceedings*.
- **Partnerships and External Interactions:** NASPI
- **Technology Readiness Level:** Multi-cast data origin authentication is essentially completed research. Industry applications are sought; trust is ongoing fundamental research.

Researchers

- Carl Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu

Industry Collaboration

- SEL

Lossless Compression of Synchrophasor Measurement Unit Archives

Overview and Problem Statement

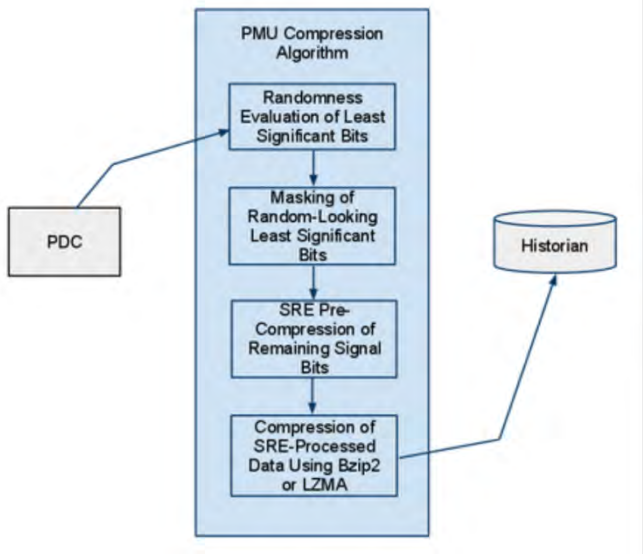
Data from syncrophasor measurement units, or PMUs, promise to increase wide-area situational awareness of grid conditions like no previous technology. However, as PMUs become more widely deployed, and as their reporting rate grows from 30 measurements per second to higher levels, the amount of data that must be archived and retrieved for later analysis and reporting requirements will grow to cumbersome levels. The purpose of this work is to develop a compression technique for PMU data that preserves the data's meaningful signal content.

Research Objectives

- Develop a compression technique tailored to the unique characteristics of PMU data.
- Characterize the bits of PMU data in terms of signal content and possible noise.
- Extract meaning from PMU data even when metadata identifying the nature of individual data streams are lacking.
- **Smart Grid Application Area:** Wide area visualization and coordination.

Technical Description and Solution Approach

- Power system data exhibit temporal and spatial coherencies. This tendency toward continuity across time and space is similar to the continuities that exist in images, characteristics used by image compression techniques.
- Similar to PNG compression, our compression algorithm estimates the next value of a measurement based on its previous value and the change seen in a neighboring measurement. The algorithm stores the difference between the expected value and the actual value. If these differences tend to be small, they will lie within a narrow range, and the resulting stream will therefore be more compressible.
- An analysis of the bits in each PMU value reveals some interesting characteristics related to randomness and noise. The least-significant bits of the data in our test streams passed NIST randomness tests, suggesting that they are not part of the meaningful signal content. Our compression approach filters these bits.
- A block diagram of the approach is shown below.



Results and Benefits

- Compression ratios of up to 20 to 1 have been seen with actual PMU data.
- **Partnerships and External Interactions:** Data and tool support from GPA.
- **Technology Readiness Level:** After further testing, the algorithm will be ready for integration with existing PMU archiving software ,like openPDC.

Researchers

- Ray Klump, University of Illinois, klump@illinois.edu
- Zeb Tate, University of Toronto, zeb.tate@utoronto.ca

Industry Collaboration

- Paul Trachian and Ritchie Carooll from TVA. Have also been supported with data and PMU streaming tools by the Grid Protection Alliance (GPA).

PMU Data Quality

Overview and Problem Statement

Phasor measurement data (synchro-phasor data) are envisioned as a key technology enabling real-time power grid measurement and control. The nascent integration of PMUs and synchro-phasor data has yet to gain widespread trust among power system operators due to availability and accuracy issues.

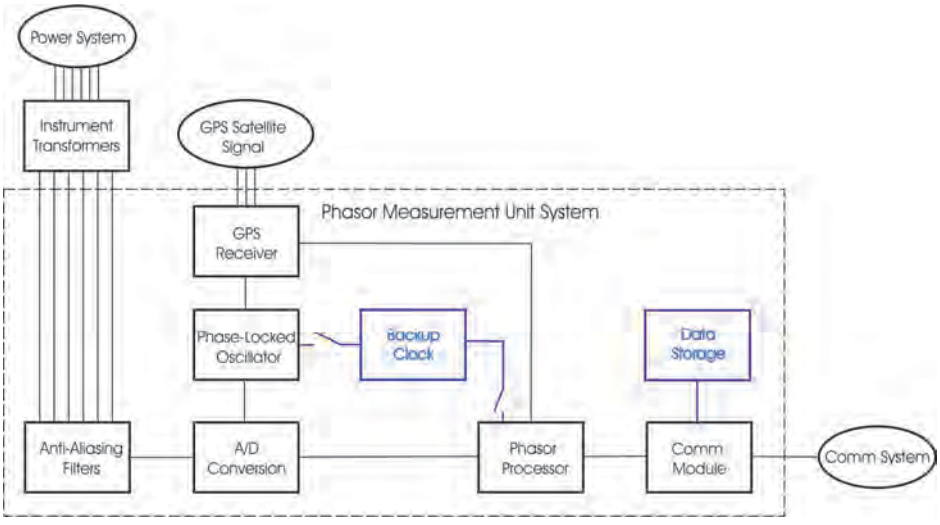
The "PMU Data Quality" research activity is investigating the sources, effects, and implications of absent or erroneous PMU data. The research is pursuing a fundamental understanding of real-time synchro-phasor measurement challenges, PMU data quality measures (error, availability, and reliability), methods for detecting faulty PMU data, and the implications of and remedies for defective PMU data.

Research Objectives

- Gain a fundamental understanding of phasor measurement challenges.
- Characterize synchro-phasor data quality (error, availability, reliability).
- Investigate PMU data utility for Smart Grid applications.
- Investigate state estimator sensitivity to measurement errors.
- Identify methods for detecting faulty synchro-phasor data.
- Investigate implications and remedies for faulty synchro-phasor data.

Technical Description and Solution Approach

- Build and test an open-box synchro-phasor measurement device; understand the challenges of measuring, processing, synchronizing, and integrating synchro-phasor data. (Collaboration with National Instruments.)
- Research the application of synchro-phasor data to power system Thevenin equivalent circuit representations.
- Characterize the error, availability, and reliability of field measurements and phasor measurement devices.



Results and Benefits

- New project, started September 2011.
- Preliminary work is analyzing PMU reliability and PMU data availability.
- Assembling a student team and resources to build a working PMU in Fall 2011.
- **Partnerships and External Interactions:** Electric Power Research Institute (EPRI); National Instruments.

Researchers

- Prof. Pete Sauer, psauer@illinois.edu
- Karl Reinhard, reinhrd2@illinois.edu

Industry Collaboration

- Paul Myrda, Electric Power Research Institute (EPRI)
- Andrew Watchorn, National Instruments

Overview and Problem Statement

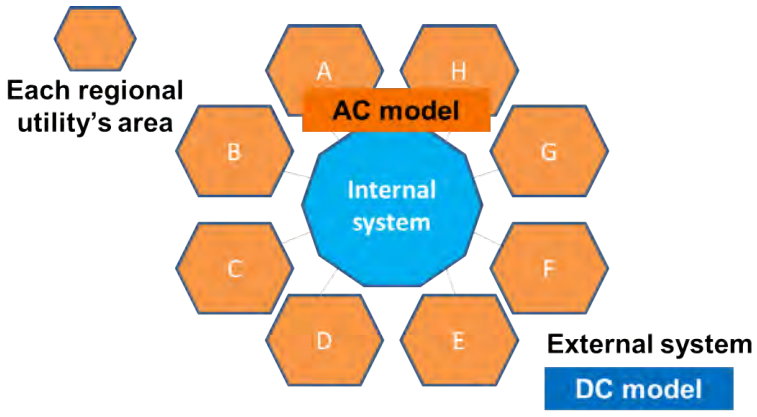
This project explores the direct application of Phasor Measurement Unit (PMU) data into the power flow algorithm. PMUs are beginning to be widely deployed in electric power systems, and this trend is expected to continue. However, even with this increase in the number of installations, PMUs are still deployed at only a small percentage of system buses. This presents a challenge: how to get useful information from a small number of data points. The key driver for PMU technology is the application of the precise time sources provided by GPS (Global Positioning System) satellites to accurately measure the relative voltage and current phase angles at buses across an interconnect. This characteristic of being able to measure the phase angles directly across an interconnected power grid is a key advantage that PMUs have over SCADA (with the other advantage being the much faster PMU sampling rate). In contrast to the widely known application of PMU values in the state estimator (SE), this project considers how PMU values can be utilized in an operational and/or analysis context beyond their use in SE. The motivation for this application arises from the fact that SE results may not be available in a variety of situations. For example, smaller utility control systems may not have an SE, the SE may have failed to converge during rapidly changing system conditions, there may be a need to combine SE results with a larger system model, or people involved in nonoperational aspects of the power grid, such as marketers and power system planners, may not have access to SE results. However, a power flow case is often available that at least approximates (to some degree) the current operating condition. This project presents an optimal power flow (OPF) based algorithm to demonstrate how PMU measurements can be included within a traditional power flow to improve the representation of a particular system operating point.

Research Objectives

- Develop a framework to allow PMU measurements to be directly incorporated into existing power flow algorithms.
- Develop power flow algorithms for solving part of a power network using the standard ac model and other parts using the more approximate dc model.
- Develop voltage stability assessment method with PMU values in order to prevent voltage collapse.

Technical Description and Solution Approach

- This project is developing power flow algorithms for solving part of the network using the standard ac model, whereas other parts of the network are solved using the more approximate, more robust dc model. The new model gives an advanced power flow model that has a fast solution without sacrificing accuracy in areas of interest.



- The project explores the direct use of PMU data for voltage stability assessment.

Results and Benefits

- A key benefit will be algorithms that are embedded within existing power flows that can accommodate PMU values for improved situational awareness. This has positive benefits in operations, since these algorithms could be used when a state estimator solution is not available.
- The advanced power flow algorithm can improve solution speed without sacrificing accuracy in areas of interest, and it can be used for fast steady-state and transient analysis.
- A new online voltage stability assessment method can predict present stability condition and margin.
- **Technology Readiness Level:** The algorithm was implemented with Matlab; it is necessary to integrate the developed algorithm into actual power system code.

Researchers

- Tom Overbye, overbye@illinois.edu
- Soobae Kim, kim848@illinois.edu

Industry Collaboration

- PowerWorld

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Real-Time Streaming Data Processing Engine for Embedded Systems

Overview and Problem Statement

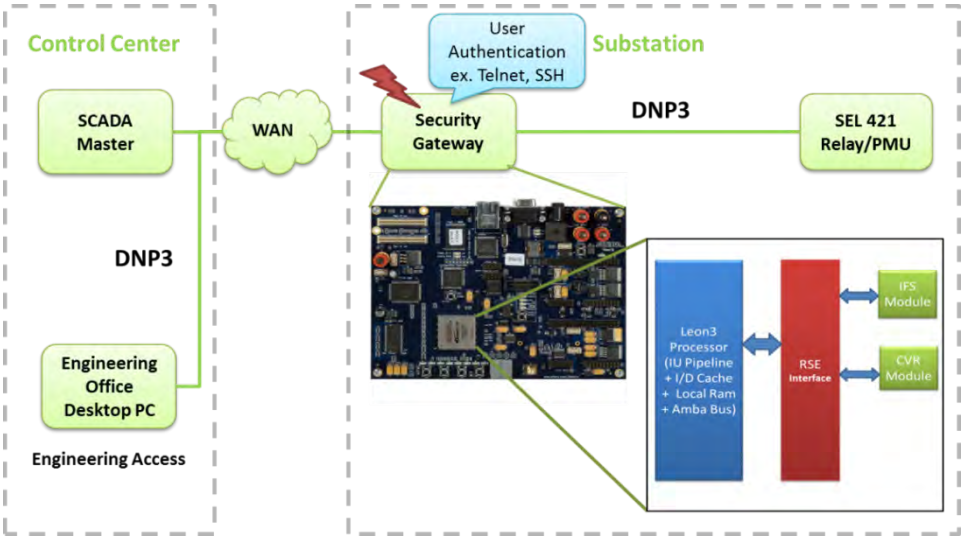
The objective of the project is to develop low-cost, application-specific techniques to achieve secure and reliable execution of applications that compute critical data, in spite of potential hardware and software vulnerabilities. In addition, we provide a flexible and high-coverage method for ensuring reliable and secure computing without incurring much software and hardware overhead. In particular, we are creating an embedded device that can be inserted in the Substation Security Gateway to protect the data stream against corruption due to accidental errors or malicious attacks. In the future, it will be possible to integrate the techniques into the chip itself (e.g., a dedicated core).

Research Objectives

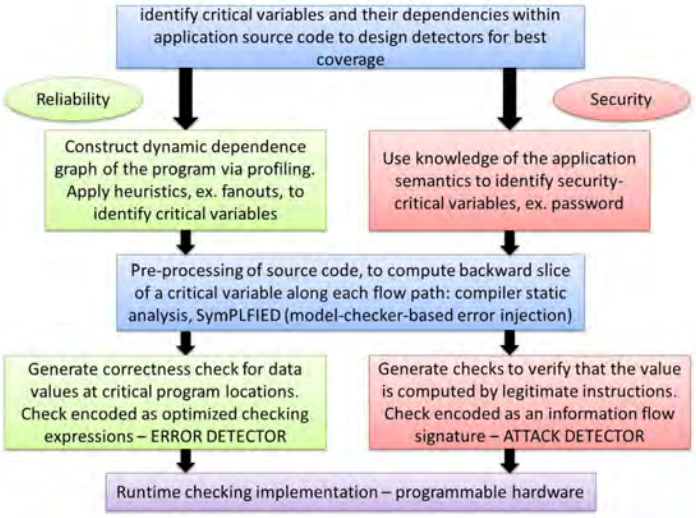
- Protect critical power grid data from malicious tampering or accidental errors.
- Detect application-level external and internal attacks.
- Create a unified hardware framework to integrate error-checking mechanisms.
- Achieve low-cost, low-overhead, high-performance, and scalable security and reliability checking.
- **Smart Grid Application Area:** Apply our Assured Streaming Data Processing Engine on the PMU Data Concentrator or Substation Security Gateway to protect the integrity of critical data, such as password or power grid data.

Technical Description and Solution Approach

- Developing the Assured Streaming Data Processing Engine, which provides a standard interface between a processor pipeline and hardware modules that implement reliability and security services.
- Using IFS (Information Flow Signature) and CVR (Critical Value Re-computation) to serve as security and reliability services, respectively.
    - **Information Flow Signature (IFS)**: Analysis of the program to derive the instruction backward slice that manipulates the critical data and to instrument it with code to ensure that runtime modifications of the critical data follow the language-level semantics of the application.
    - **Critical Value Re-computation (CVR):** The application source code is statically analyzed to extract the backward slice for the critical data and then instrumented with the check instructions to recompute critical values.
- **Assured Streaming Data Processing Engine System Architecture**

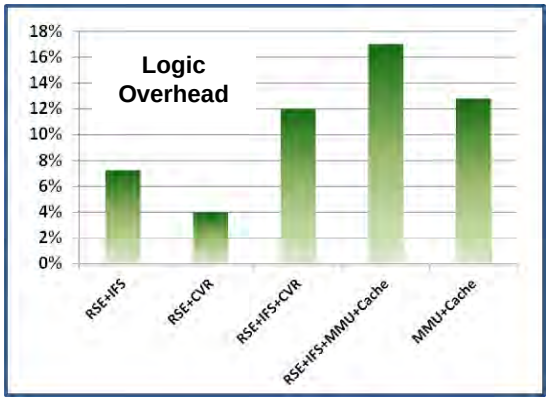


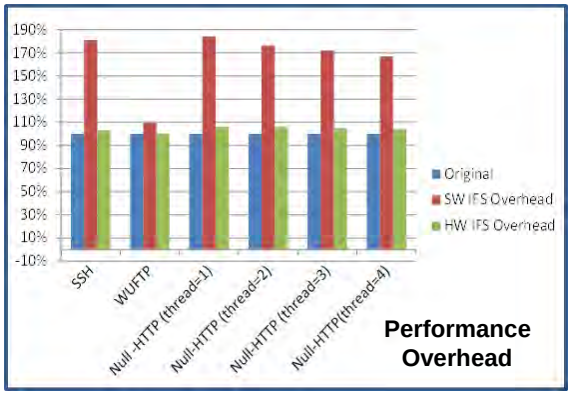
- **Unified framework for reliability and security**



Results and Benefits

- Leon 3 processor, RSE framework, and IFS module synthesized to Altera Startix II FPGA.
- IFS module demonstrated using SSH, WuFTP, and NullHTTP applications on top of Linux OS with low performance overhead (3-4%) and 100% coverage for insider attacks.





- **Technology Readiness Level:** We have implemented the Assured Streaming Data Processing Engine along with the modules IFS (Information Flow Signature) and CVR (Critical Value Re-computation) on our Stratix II Altera Board as a working prototype to evaluate our techniques.

Researchers

- Kuan-Yu Tseng, ktseng2@illinois.edu
- Keun-Soo Yim, yim6@illinois.edu
- Zbigniew T. Kalbarczyk, kalbarcz@illinois.edu
- Ravi K. Iyer, rkiyer@illinois.edu

Industry Collaboration

- Altera, SEL

Research Cluster

Trustworthy Cyber Infrastructure and Technologies for Active Demand Management

Trustworthy Cyber Infrastructure and Technologies for Active Demand Management Page No.

Cluster Lead: Tom Overbye ..... overbye@illinois.edu

Development of the Information Layer for the V2G Framework Implementation

Overview and Problem Statement

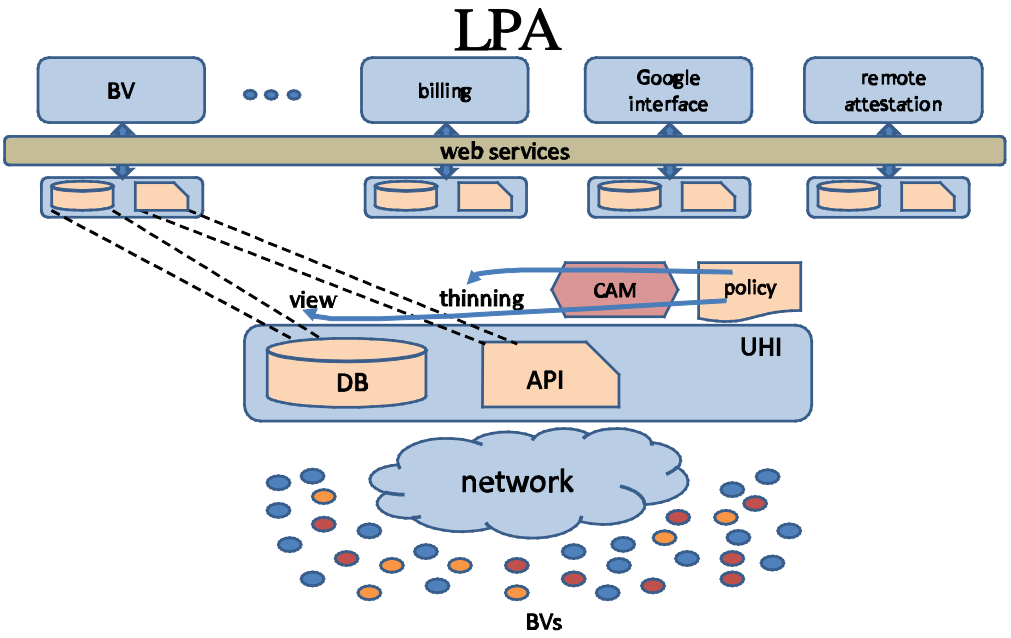
The Vehicle-to-grid (*V2G*) concept integrates Battery Vehicles (*BVs*) into the grid as controllable loads and generation/storage devices. An *Aggregator* is needed to control the *BVs* and to economically provide services to the grid. The *Aggregator's* communication layer requires extensive bi-directional communication and therefore is vulnerable to cyber attacks. The lack of adequate security measures is a major impediment to the effective integration of battery vehicles (*BVs*) into the grid.

Research Objectives

- To show that the cyber security protection of the *V2G* communication layer can be cast into a form such that the Least Privilege Architecture (*LPA*) provides an appropriate structure to protect the cyber security of the grid.
- To adapt *LPA* to the specific needs of the *V2G* problem.
- To demonstrate the ability of the adapted *LPA* to operate effectively in the *V2G* framework.
- **Smart Grid Application Area:** Active Demand.

Technical Description and Solution Approach

- The *LPA* framework provides a mechanism that facilitates the work of the new player in the integration of the *BV*s into the grid, specifically the *BV Aggregator*. The architecture enables the decomposition of the *Aggregator*'s functions into logically disjoint services.
- These mechanisms effectively limit the privileges of each service so that an entity interfacing with the *Aggregator* can only access the functions and data it needs to fully complete its tasks.
- The proposed approach minimizes the impacts of a successful attack on each service provided by an *Aggregator.*
- **Technology Readiness Level:** The concept is worked out, but the scalability to large aggregations needs additional investigation.



Results and Benefits

- LPA provides mechanisms to effectively limit the privileges of each service so that it can access only the functions it needs to fully complete its tasks.
- LPA provides restricted access to the database to each service at a level commensurate with the requirements to complete the service tasks.
- LPA facilitates the decomposition of the *Aggregator's* functions into logically disjoint services, leading to enhanced security.
- LPA minimizes the impact of a successful attack on a single service.
- LPA allows room to securely expand services to third-party vendors.
- LPA facilitates the easy expansion of the number of BVs and parking lots in the aggregation.
- **Partnerships and External Interactions:** LM

Researchers

- George Gross, gross@illinois.edu
- Carl A. Gunter, cgunter@illinois.edu
- David D. Riddle, ddriddle@illinois.edu

Industry Collaboration

- Eileen Denz, Lockheed Martin

Password Changing Protocol

Overview and Problem Statement

Power distribution uses devices such as sensors and capacitor banks in electric poles. The health and stability of power lines and the location of faults due to any kind of damage are monitored using the voltage and current ratings from these devices. To collect data, usually an operator/maintenance person drives a truck under a pole (in the range of Wi-Fi) and logs into the sensor device with a common password. After collecting data from one pole, he or she moves to the next pole. Currently thousands of operators are involved in data collection, and all use the same password to access the devices; hence, the security of the password is very weak. Furthermore, the long duration of a single password creates vulnerability to attack; even in the case of data misuse, it is hard to find the responsible operators.

Research Objectives

- Our goal is to provide a secure password changing protocol to ensure data safety.
- The protocol should consider suspicious behavior and movement of the operators while collecting data.
- At the same time, the solution should be cost-effective and fast.
- **Smart Grid Application Area**: Security, networking.

Technical Description and Solution Approach

- Our approach is to design a secure password changing protocol considering:
  - Cyber information (password), and
  - Physical information (identification, timestamp, location of the operators) while operators collect data.

Results and Benefits

- The resultant protocol will allow secure access at devices in the field level and ensure accurate billing without data alteration. For example, if a truck is stolen or someone uses a snooping tool and gets the password, this protocol makes sure that he or she can't get access to the devices and can't change telemetric measurements, which could lead to wrong measurements being sent to the utility company.
- Even if the intruder breaks the password, the protocol will still secure the data inside the devices.
- The responsible operators can be identified if attacks occur.
- **Partnerships and External Interactions**: We are interacting with the project "Trustworthy Framework for Mobile Smart Meters."
- **Technology Readiness Level:** Initial stage.

Researchers

- Prof. Klara Nahrstedt, klara@illinois.edu
- Rehana Tabassum, tabassu2@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Smart-Grid-Enabled Distributed Voltage Support

Overview and Problem Statement

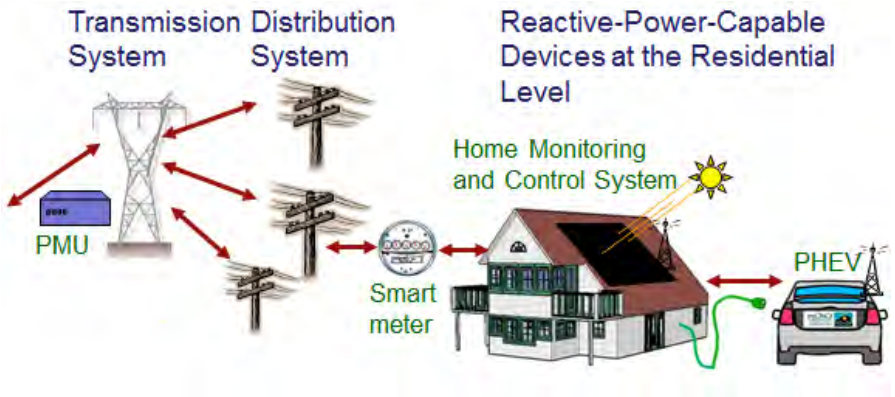
The motivation for this research lies in the use of emerging smart grid devices, such as PHEV/EVs and solar panels, to supply reactive power as a means of distributed reactive power support. Power factor compensation closer to the load improves transmission line loading and efficiency. We examine requirements for a secure communication framework to interact with the large number of devices that would be present. The focus of this project is on determining the cyber infrastructure needed to obtain this reactive power control.

Research Objectives

- The project seeks the ability to utilize large amounts of distributed resources, so there are major challenges to ensure that the devices cannot be used to harm the system instead of to improve it.
- Information received by the devices must be trustworthy so they will respond only in an intended way.
- Availability of the resources is important, and the capabilities of the system at any time should be known, since having wrong or out-of-date information about resource availability may cause the scheme to be unsuccessful.
- There are also questions about the best way to utilize the support from a power system perspective; for example, should the system operate so that it receives the distributed support all the time, or just for a few minutes in response to certain events?
- Another challenge is to investigate what the implications would be for potential contingencies of this system so that the system can be designed to avoid them. For example, if an adversary were to gain control of a neighborhood's distributed reactive power control system and tell all the devices to maximize their output, could all the fuses trip at the same time?
- **Smart Grid Application Area:** This project is developing a framework to allow secure control of distributed resources in an intelligent manner.

Technical Description and Solution Approach

- Example power systems, such as distribution feeders, are being modeled to show the benefits of local injections of reactive power. Varying load and supply voltage conditions are being modeled.
- Algorithms are being developed to determine the validity of using distributed reactive power control with different assumptions about the cyber infrastructure, such as local control versus global control.
- Impacts of cyber disruptions are being studied.
- A control system has been proposed for a battery-inverter device that can be used to inject reactive power. The system has been simulated in Simulink prior to implementation.



Results and Benefits

- Reactive power is most effective locally, and voltage problems tend to start in the distribution system. By addressing the problem at the distribution level, we can alleviate voltage problems at the transmission system level as well.
- A framework utilizing distributed reactive resources is important, because an increasing number of inverter devices that can potentially provide this support are being placed in the power grid, and this additional reactive power capability is useful from a power systems perspective.
- As noted in the 2003 blackout report, a commonality among most previous major North American blackouts was that the system was experiencing inadequate reactive power support.
- **Partnerships and External Interactions:** Energy Dashboard project, Load Control and Monitoring project, and Agent Applications project.
- **Technology Readiness Level:** The researchers plan to work with the campus distribution system facilities personnel to implement a test system on the University of Illinois campus.

Researchers

- Chris Recio, recio2@illinois.edu
- Thomas J. Overbye, overbye@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Specification-based Intrusion Detection System for Smart Meters

tcipg.org

Overview and Problem Statement

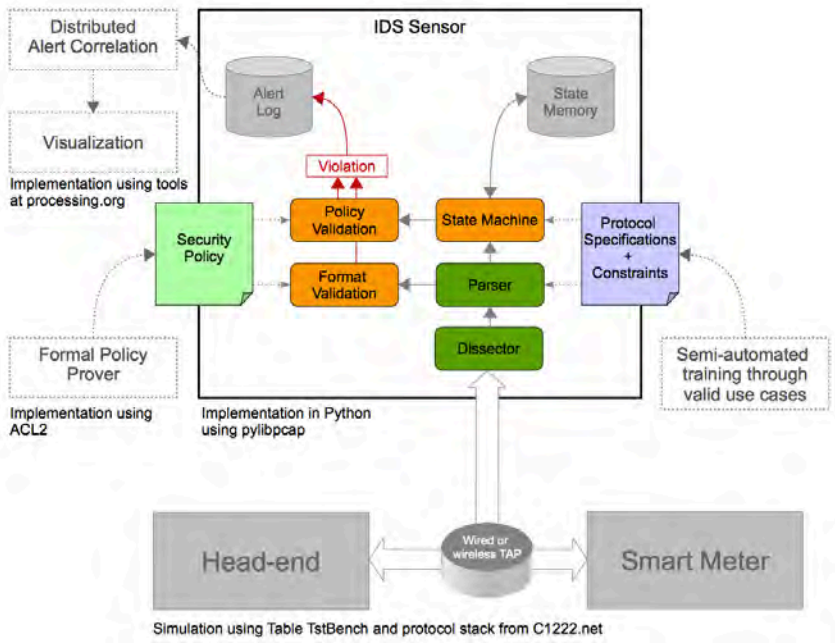
To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address this issue, we introduce a specification-based intrusion detection sensor that can be deployed in the field to identify security threats in real time. The sensor monitors the traffic among meters and access points at the network, transport, and application layers to ensure that devices are running in a secure state and that their operations respect a specified security policy. It does so by implementing a set of constraints on transmissions made using the C12.22 AMI protocol that ensure that all violations of the specified security policy will be detected. The soundness of those constraints was verified using a formal framework, and a prototype implementation of the sensor was evaluated with realistic AMI network traffic.

Research Objectives

- Identifying the threats targeting AMI.
- Developing detection technologies to run on low-computation hardware with limited memory.
- Designing a comprehensive but cost-efficient monitoring architecture.
- Providing large-scale situational awareness.
- **Smart Grid Application Area:** AMI security.

Technical Description and Solution Approach

- Identification of the characteristics of common smart meter communication use cases.
- Design of a distributed monitoring framework and a security policy to ensure the detection of violations.
- Development of a C12.22 dissector and a C12.22 state machine to monitor meter traffic in real time.
- Evaluation in an emulated AMI environment with various attacks.



Results and Benefits

- Definition of a rigorous process for utilities and vendors to develop a comprehensive monitoring architecture.
- Integration of formal methods in a practical framework to offer strong security guarantees.
- **Partnerships and External Interactions**: in discussion with Fujitsu, EPRI, and Itron.
- **Technology Readiness Level**: prototype.

Researchers

- Dr. Robin Berthier
- Prof. William H. Sanders

Industry Collaboration

- Fujitsu: Alvaro Cardenas
- EPRI: Galen Rasche
- Itron: Robert Former

Trustworthy Framework for Mobile Smart Meters

Overview and Problem Statement

We propose to install on an electric car a mobile smart meter that monitors energy usage by the car and communicates with a central utility office for billing information or pricing guidance. The approach enables us to track energy usage more easily. It also brings new energy market models, as people generating excessive energy from their solar panels can directly sell energy to electric cars, where the mobile meter on the car records the energy purchase. However, securing communication between mobile smart meters and the utility office might be challenging; the data may be routed through a combination of wired networks, open WiFi, and cellular networks. We are focusing on the question of how a mobile smart meter communicates with other meters and with the central utility office in a secure way. The ultimate goal is to design a trustworthy framework for communication between meters and a central utility, together with the corresponding secure communication protocol.

Research Objectives

- Design a general trustworthy framework for secure data storage and communication for mobile smart meters.
- Design a secure routing protocol for communication between mobile smart meters and a central utility office.
- Design a secure storage scheme to store information collected by meters.

Technical Description and Solution Approach

- Secure geographic routing protocol for communication between meters and utility office.
- Secure data storage and replication schemes to ensure data safety.
- Optimization algorithm to determine the best pricing strategy.
- Computer simulation.

Results and Benefits

- Easy monitoring and accurate tracking of energy usage: meter is directly associated with the car that consumes energy.
- Flexible pricing model: a mobile smart meter receives pricing information specifically targeted at the associated car.
- Flexible energy exchange: meter-to-meter communication makes it possible for a car to sell energy directly to another and record the exchange correctly.

Researchers

- Hongyang Li, hli52@illinois.edu
- Klara Nahrstedt, klara@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Research Cluster

Responding to and Managing Cyber Events

Responding to and Managing Cyber Events Page No.

Cluster Lead: William H. Sanders.....whs@illinois.edu

A Game-Theoretic Intrusion Response and Recovery Engine

Overview and Problem Statement

The severity and number of intrusions on computer networks are rapidly increasing. Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance and automated response techniques. Briefly, in this project, the ultimate goal of the intrusion-tolerant system design is to adaptively react against malicious attacks in real-time, given offline knowledge about the network's topology, and online alerts and measurements from system-level sensors.

Research Objectives

- Cyber-physical security-state estimation using cyber-side Intrusion Detection Systems (IDSes) and power-side Power Measurement Units (PMUs).
- A system security metric to assess and measure, at each time instant, the system-wide security level of the power grid.
- Reactive response against adversarial attacks that uses knowledge about the power grid's current security-state and its security level.

Technical Description and Solution Approach

- We make use of machine learning algorithms to automatically capture dependencies among power grid subsystems in order to minimize human involvement in the information fusion process.
- We employ the automatically learned system dependency model along with efficient and scalable belief propagation techniques to deduce how critical each security incident is globally.
- We are working on design and development of a scalable game-theoretic decision-making solution to come up with optimal response and recovery actions in real-time for large-scale power grid networks.

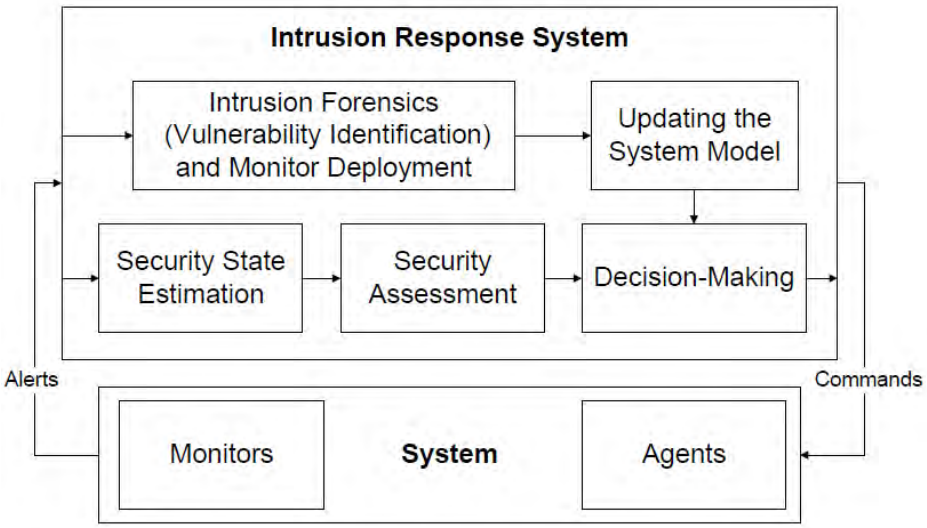


Figure 1: High-level Conceptual Architecture of the Proposed Intrusion Tolerance Solution

Results and Benefits

- Our developed tools can now automatically generate and learn system-wide dependency graphs and adversary-driven attack graphs for large-scale power grid networks. We evaluated our implementations using a simulated and realistic power grid control network topology inspired by real-world control room configurations.
- We presented and evaluated an information fusion solution to accurately estimate the security state of a cyber-physical system using online information from cyber-side intrusion detection systems and the physical sensors, e.g., power measurement units.
- We introduced a consequence-based security metric to assess the security of each possible state of the system with a minimum possible set of manual inputs from system administrators. Our security assessment tools can automatically calculate the system security metric for a given power grid topology using the Gibbs sampler method. This can be used to provide power system operators with efficient and global situational awareness support.

Researchers

- Saman A. Zonouz, saliari2@illinois.edu
- Robin Berthier, rgb@illinois.edu
- Kate Rogers, krogers6@illinois.edu
- Ahmed Mohamad Fawaz, afawaz2@illinois.edu
- Rakesh Bobba, rbobba@illinois.edu
- William H. Sanders, whs@illinois.edu

Assessment and Forensics for Large-Scale Smart Grid Networks

Overview and Problem Statement

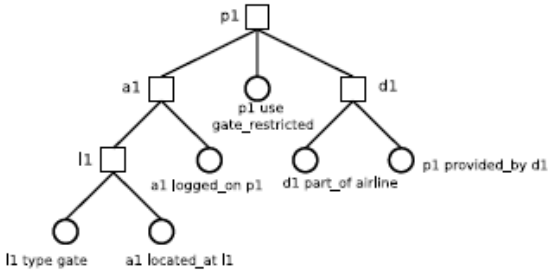
The infrastructure that supports the power grid is vulnerable to attack by intruders, who could potentially take control of certain points and cause great damage to systems. It is therefore important that organizations develop infrastructure security policies to handle unwanted configuration changes and failures within the grid. Often, large systems concentrate their security by creating central monitors that can act as single points of failure if compromised. These centralized systems are also difficult to scale up and may not adequately ensure the validity of information passed in the network.

Research Objectives

- We aim to improve the security and efficiency of automated systems for monitoring compliance of power systems to policies.
- We introduce and analyze a secure architecture for monitoring compliance based on security event monitoring at the network level, software level, and hardware level.
- Our approach is based on removing central points for monitoring to increase scalability and security.
- We will configure an architecture that protects integrity and confidentiality of the nodes within the system.
- **Smart Grid Application Area:** Distributed Systems.

Technical Description and Solution Approach

- Create a framework to input and interpret infrastructure policies in the architecture.
- Develop a compilation algorithm to transform policies into multiple redundant aggregation trees. These aggregation trees ensure a distribution of policy verification load among multiple systems for scalability. Redundancy makes the architecture resilient against a limited number of compromised nodes within the system.
- Convert the aggregation tree into a rule set and state triggers that can be added to the knowledge base of the corresponding devices.
- Commence an execution phase in which servers forward messages along multiple paths for enhanced security and redundancy.
- Create simulator to test scalability and effectiveness of architecture.



Results and Benefits

- Found that the architecture is successful in distributing policy statements across nodes in an effective manner.
- Communication in this architecture only grows linearly with the size of the infrastructure, which indicates scalability of this solution.
- System is robust in protecting itself against a limited number of attacks.
- This architecture could be useful in protecting distributed systems against attacks.
- **Partnerships and External Interactions:** Information Trust Institute, Assured Cloud Computing at UIUC
- **Technology Readiness Level:** Initial stage

Researchers

- Jonathan Chu, jmchu2@illinois.edu
- Mirko Montanari, mmontan2@illinois.edu
- Xueman Mou, mou2@illinois.edu
- Prof. Roy Campbell, rhc@illinois.edu

Industry Collaboration

- Boeing

Coordinating Black Start Operations Using Synchrophasors

Overview and Problem Statement

As synchrophasor measurement units (PMUs) become more commonplace, they promise to provide an unprecedented wide-area view of grid health. This view should give operators the ability to identify with more certainty the best opportunity to reconnect two disconnected regions. Closing across regions requires first bringing them closer together electrically. By monitoring phase angles and actuating controls to bring phase angles on the two sides of an open tie closer, an operator can take more active control of the dynamics within the two regions to make it easier and safer to reconnect them. This requires formulation of a schedule of phase angle targets in the two regions. Once that schedule has been established, controls can be activated on both sides to achieve that schedule. With the controls implemented, the steady-state operating points of the two sides should be closer, which should make it easier to reconnect them. This work is developing an algorithm that brings two regions closer together so that they may be reconnected.

Research Objectives

- To use the quickly updated voltage magnitude and phase angle data provided by PMUs to assist efforts to re-energize and reconnect regions of the grid.
- To determine and demonstrate the effectiveness of the algorithm in a laboratory setting.
- To implement the algorithm as part of the black start strategy of utilities.
- **Smart Grid Application Area:** System restoration and incident response, wide-area control.

Technical Description and Solution Approach

- Considering steady-state characteristics of power systems, we are developing a way to calculate a schedule for phase angles at the nodes within two disconnected regions to make it easier to close the tie between them.
- Here is a mathematical description of the algorithm.

  Sensitivities to injections at each end of the tie to be closed:

  $$\begin{bmatrix} \Delta\boldsymbol{\theta} \\ \Delta\mathbf{V} \end{bmatrix} = -[\mathbf{J}(\mathbf{x})]^{-1}[0 \ \ldots \ 0 \ 1 \ 0 \ \ldots \ 0 \ -1 \ 0 \ \ldots \ 0]^{\mathrm{T}}$$

  To close line tie L_{jk} between the two systems, determine $\Delta\theta_{jk}$ needed to comply with breaker setting on the phase angle difference. Set this value equal to the estimate of the post-close flow on the tie line needed to realize that angle difference.

  $$\Delta\theta_{jk} \approx P_{L\,jk}\left(\Delta\theta_j - \Delta\theta_k\right)$$

  Solve for $P_{L\,jk}$. Multiply this value by the sensitivities $\Delta\theta_i$ and ΔV_i by $P_{L_{jk}}$ to update the angles and voltages at all nodes on both sides of the tie. This establishes the schedule for voltage magnitudes and phase angles on each side of the tie.

- Given that schedule, implement controls on the two sides, such as load shedding and generator outputs, to change phase angles to match the schedule.
- Monitor the dynamics of the system to determine whether the tie between the two regions may be closed.

- Given the results of simulations, implement the strategy in a laboratory setting. Specifically, take two separated systems in the electric machines lab, perform the calculations just described, and gauge the effectiveness of the approach in helping reconnect the systems.

Results and Benefits

- If there is a major system event, restoring the system as quickly and safely as possible presents a tremendous but necessary challenge.
- If successful, this tool will help operators meet that challenge.
- It also can be used with microgrids to determine how best to connect them with the broader system.
- **Technology Readiness Level:** Purely conceptual at this point.

Researchers

- Ray Klump, klump@illinois.edu

Hardware-based IDS for AMI Devices

Overview and Problem Statement

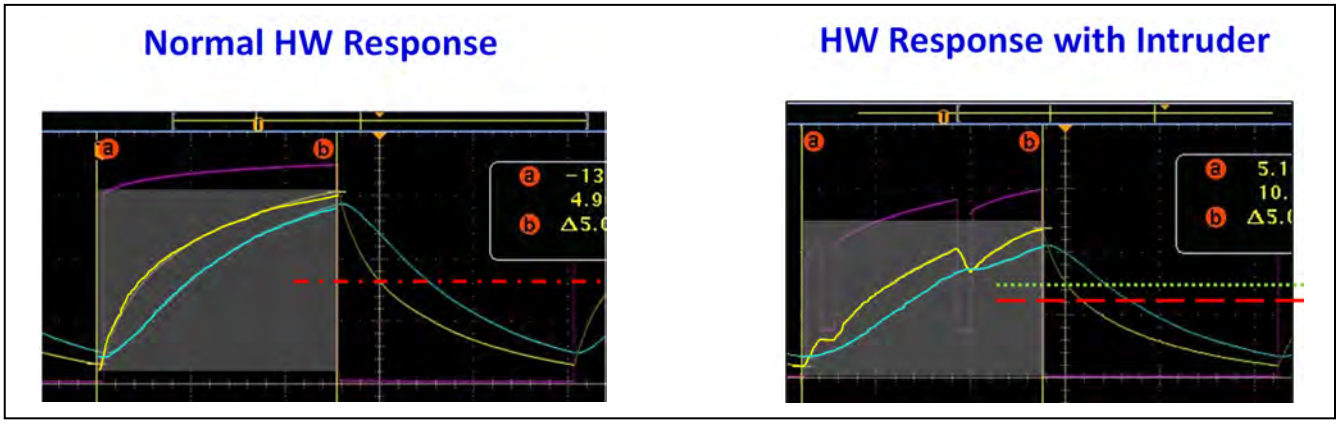
A major challenge is that many embedded system devices used in critical infrastructure applications are easily accessible (i.e., poor physical security) and can be tampered with or altered such that the authentication of the devices cannot be assured. In addition, the installation of a hardware-based backdoor gives a cyber-attacker unlimited eavesdropping access to logic-level communication within a Smart Grid device and is virtually undetectable by state-of-the art intrusion detection systems. This research activity looks at ways to identify this kind of attack at the embedded system board level, while keeping in mind the constraints of manufacturing cost and normal system performance.

Research Objectives

- Study the analog characteristics of low-cost circuit components to determine if normal manufacturing process variance is enough to create unique hardware signatures that are very difficult to replicate.
- Identify nonlinear circuit configurations that provide a differential comparison between normal inter-chip communication and unauthorized use during a hardware-based attack, without the use of stored “secret” values.
- Identify the electrical characteristics of a hardware-based logic-level attack.
- Derive a hardware detection algorithm that can be scaled to different communication bus speeds.
- Determine several design considerations with regard to IDS sensitivity and accuracy.
- **Smart Grid Application Area:** AMI, SCADA, any easily accessible Smart Grid Devices.

Technical Description and Solution Approach

- Use a low-cost Resistive-Capacitive circuit connected to Inter-chip communication bus (via transistor switch).
- Synchronously measure the dynamic analog responses (voltage and time) to challenge waveform.
- Derive peak voltages, integrals of response, 1st and 2nd order derivatives of response, difference of areas, difference of derivatives, and symmetry of waveforms.
- Compare the measured values: 1) between challenge-response pairs; 2) between charge-discharge phases.
- An intruder attached to the communication bus changes shape of waveforms and shifts line of symmetry, peak voltages, and several 1st order/ 2nd order values.



Results and Benefits

- Hardware charge and discharge phases are statistically equivalent (<5% error) and offer per-cycle detection.
- Provides a high-resolution view of the security status of AMI system.
- Low impact on system performance.
- Low-cost and easily integrated into new Smart Grid devices.
- **Partnerships and External Interactions:** SNL (DOE).
- **Technology Readiness Level:** Currently working on proof-of-concept.

Researchers

- Nathan J. Edwards, njedwar2@illinois.edu

Industry Collaboration

- Abe Clements, Sandia National Laboratories (DOE)

Usable Management Tools for the Smarter Grid's Data Avalanche

Overview and Problem Statement

The present and future smart grid has a vast population of diverse devices that generate lots of data. The variety, large volume, and spontaneous generation of data result in what one of our industry partners has called a "data avalanche." Data avalanches of the future will likely be quite large if the number of devices on the smarter grid is larger than the number of devices on the Internet.

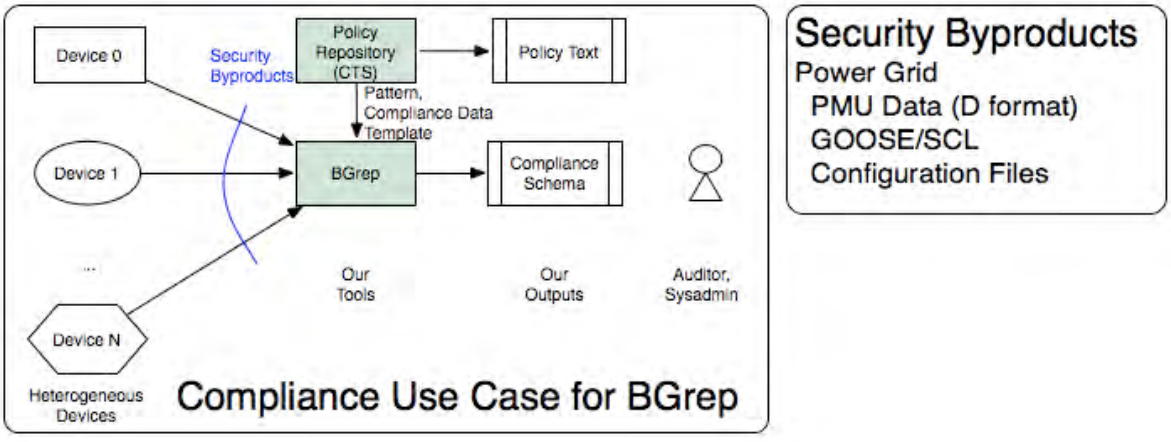
Our research focuses on the following question: How can humans deal with the smart grid "data avalanche" and thereby gain an increased situational awareness for the smarter grid?

Research Objectives

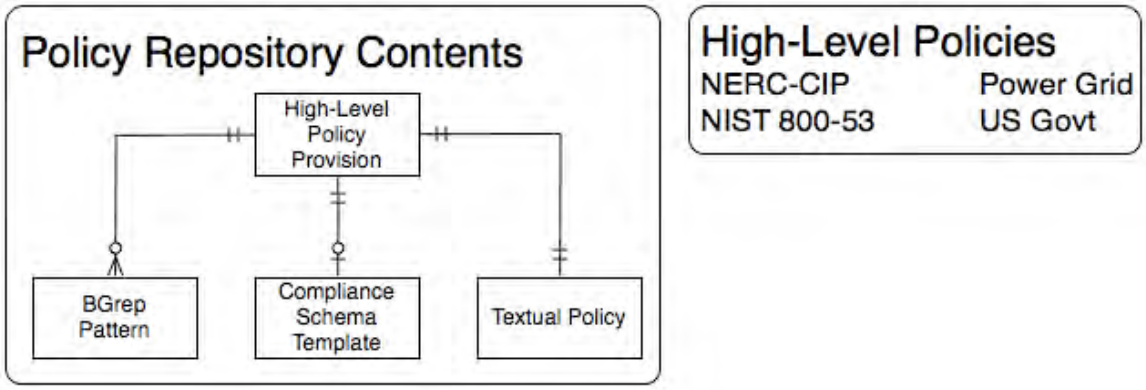
- Our tools analyze human-readable, machine-actionable security byproducts to help humans manage ever-changing security processes.
  - Can we dynamically generate evidence for CIP audits?
  - Can we continually monitor and compare device behavior despite the variety of log formats and manage the flood of PMU data?
  - Can we automatically generate change logs and reports of change?
  - Can we create a central repository of regulatory information and map high-level policies to lower-level log formats and configuration files?
- **Smart Grid Application Area:** Cyber-security situational awareness, NERC CIP compliance audit.

Technical Description and Solution Approach

- We propose to manage the data avalanche by processing human-readable, machine-actionable byproducts of security processes.
- Our approach can be used to streamline audit and to provide cyber-security situational awareness.
- Our approach has already been used successfully (and been requested by practitioners) in PKI and Network Configuration Management.
- We are going to apply our network management tools to CIP audits and monitoring.



- We are going to apply our PKI analysis tools to build a regulatory repository.



Results and Benefits

- In previous work we obtained preliminary results for our PKI policy tools, published in *EuroPKI 2009* and *IDTrust 2010*. These tools have been used by DigiCert and Protiviti.
- Preliminary results for our network configuration tools were published at *USENIX HotICE 2011*. We are working with sysadmins to improve our tools.
- Since this summer we have been actively researching IEDs (primarily PMUs) that generate lots of data in the smarter grid of the present and future.
- Our tools will provide:
  - One location for regulatory information.
  - A way to determine whether devices log enough data for audit.
  - A reproducible, consistent way to quickly obtain evidence for audit.
- **Technology Readiness Level:** New, not ready.

Researchers

- Gabriel A. Weaver, Gabriel.A.Weaver@Dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Research Cluster

Risk and Security Assessment

Risk and Security Assessment Page No.

Cluster Lead: Zbigniew Kalbarczyk ..... kalbarcz@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Automatic Verification of Network Access Control Policy Implementations

tcipg.org

Overview and Problem Statement

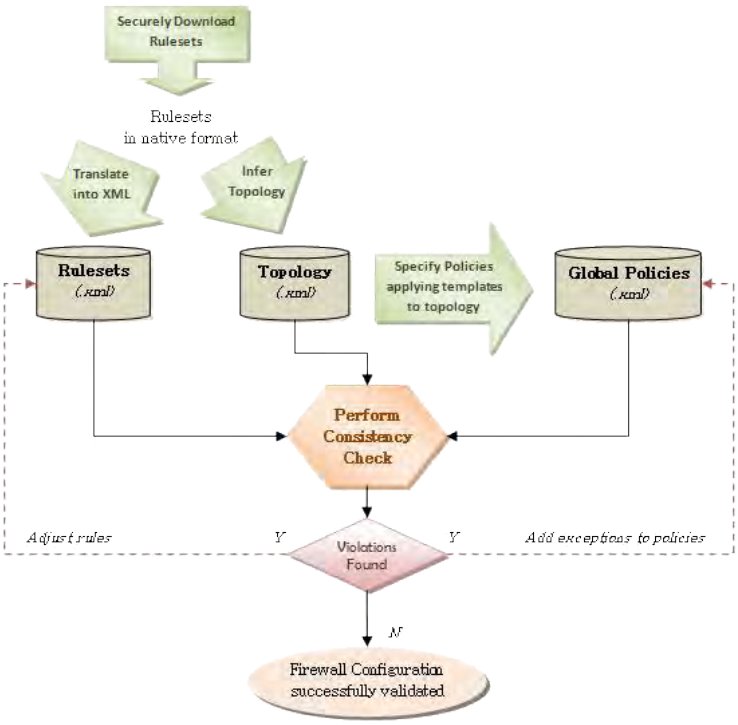
This project aims to develop a highly usable, scalable, and effective tool for analyzing security policy implementation for conformance with global security policy specification for industrial control networks. The tool provides comprehensive analysis of compliance to ensure that all access control mechanisms work collectively in harmony. The tool, called *NetAPT (Network Access Policy Tool)*, has been fully implemented and has been used successfully to aid in vulnerability assessments and compliance audits at our industry partners. NetAPT is available to potential users through an evaluation license.

Research Objectives

- Process control networks are connected to other networks in enterprise systems; access is controlled through a large number of devices, such as firewalls.
- Best practices recommendations and compliance requirements are difficult to meet rigorously without significant man-hour investment. Pressing questions include:
    - How can we express English-language recommendations for global policy in a machine-checkable form that network administrators can easily formulate and understand?
    - How can we determine whether the access control that firewalls provide precisely meets the requirements of the machine-checkable global policy?
- Any analysis method or tool must:
    - Incorporate policy rules from myriad sources.
    - Ensure scalability with size and complexity of networks.
    - Provide analytic and/or empirical demonstrations of efficacy.
- **Smart Grid Application Area:** NetAPT can be used to make sure that the access controls for the communications infrastructure of the Smart Grid are configured correctly. It can help prove compliance of the existing mechanisms with the various recommendations and standards (e.g., NERC CIP 005) and can help ensure that compliance is maintained despite any new changes to configuration of layer 3 devices (firewalls, routers).

Technical Description and Solution Approach

- NetAPT takes as input firewall configurations, and discovers the topology.
- It uses multi-layered rule-graphs and modular design to incorporate a variety of policy rules and maintain extensibility.
- It has a sophisticated graphical front-end for increased usability, along with an analysis engine optimized for performance.
- The GUI and analysis engine can be decoupled and run on separate machines (the GUI on an admin workstation, the engine on a powerful server). SSL is used to communicate between the two components.
- Specific optimizations for process control networks are included.
- NetAPT includes parameterized global policy templates encoding various best practices recommendations and compliance standards that can be quickly customized to the network being analyzed.
- NetAPT can use importance-sampling-based statistical analysis to achieve further improvement to scalability.



Results and Benefits

- NetAPT has been implemented and released to select industry partners for evaluation.
- NetAPT was used for an internal audit and vulnerability assessment at a major utility, for a network with nearly 100 firewalls and several thousand hosts.
  - Helped produce comprehensive, highly visual reports to prove compliance with NERC CIP standards.
  - Identified exceptions in firewall configurations that required policy review or changes.
- NetAPT can greatly reduce the burden of managing complex security setups in large networks, allowing for more secure networks to be built and administered.
- **Partnerships and External Interactions:** close interaction with utility partners and NERC CIP auditors.
- **Technology Readiness Level:** Evaluation licenses are available; easy-to-use installation packages and comprehensive documentation.

Researchers

- David M. Nicol, dmnicol@illinois.edu
- William H. Sanders, whs@illinois.edu
- Mouna Bamba, seri@illinois.edu
- Sankalp Singh, sankalp@illinois.edu
- Edmond J. Rogers, ejrogers@illinois.edu

Industry Collaboration

- Steve Coppenbarger, Cornbelt Energy
- Chris Johnson, Eastern Illini Electric Cooperative
- Matt Stryker, SERC Reliability Corporation

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Fuzz-testing of Proprietary SCADA/Control Network Protocols

tcipg.org

Overview and Problem Statement

Power control network asset owners may suspect that their equipment's proprietary protocols are susceptible to attacks via malformed crafted inputs, but lack the means of testing their assets and prioritizing them for protective measures (other than ordering expensive and specialized penetration tests). *Fuzzing* is a methodology for performing such testing; however, most fuzzing tools were developed for different environments and tasks (such as vulnerability development) and do not fit power network scenarios. Additionally, many tools assume that a specification of the targeted protocol is available, which is not the case for proprietary control protocols. Our LZfuzz addresses both the need for fuzzing proprietary protocols, and the specific features of a power control network environment.

Research Objectives

- Give SCADA/control network asset owners a simple way to test their assets for brittleness.
- Develop algorithms to efficiently fuzz proprietary SCADA protocols without specification or with only rudimentary specifications.
- Implement necessary network scaffolding to fuzz software/hardware that cannot be intrusively instrumented.
- **Smart Grid Application Area:** Securing control networks, in particular control center equipment and LANs such as energy management servers, front end systems, and analyst workstations.

Technical Description and Solution Approach

- LZfuzz creates a "network pipe" to intercept, analyze, and mutate targeted traffic, and does not require instrumentation of the targeted computers.
- LZfuzz uses a variant of the Lempel-Ziv compression algorithm to derive an approximate partitioning of a proprietary protocol's payload into "tokens," which it then fuzzes using a set of heuristics. Currently, these heuristics are provided by the GPF fuzzer.

Results and Benefits

- **Partnerships and External Interactions:** Used in network security assessment at a major power company.
- **Technology Readiness Level:** Beta.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Rebecca Shapiro, bx@cs.dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu
- Edmond Rogers, ejrogers@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Modeling Methodologies for Power Grid Control System Evaluation

Overview and Problem Statement

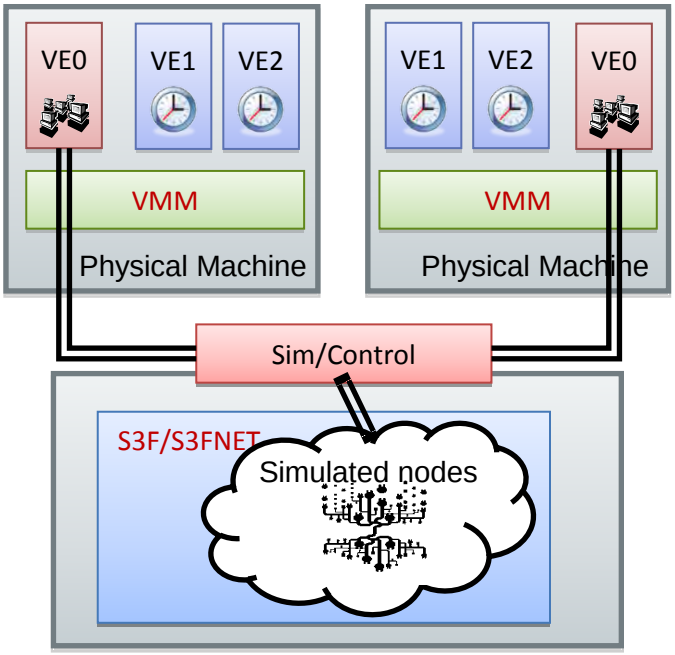
Research on various smart grid technologies requires high-fidelity experiments in realistic, large-scale settings. In this project, we are creating a high-fidelity, highly scalable simulation and emulation platform for security evaluation in power grid control networks. The testbed deploys virtual machine-based network emulation and parallel network simulation technologies to achieve this goal, and is designed to efficiently connect various virtual and real systems in the TCIPG lab as a testing and evaluation platform for other smart grid projects.

Research Objectives

- To create a backbone at the core of the Smart Grid testbed at Illinois that connects various components.
- To create models that support security assessment in a realistic large-scale setting.
- To create experimental designs and output analysis.
- **Smart Grid Application Area:** Testbed of power grid control systems.

Technical Description and Solution Approach

- Our testbed uses virtual-machine-based emulation and parallel network simulation technologies.



- Virtual-machine-based implementation of network emulation.
  - Due to the use of virtual machines, we allow unmodified application code to run in our testbed directly. This yields high functional fidelity.
  - Each virtual machine has its own virtual clock, and it perceives time as if it were running independently and concurrently with other machines in the physical world.
  - We currently have a virtual time system based on OpenVZ virtualization technologies, whose light weight provides good scalability. We are able to run 320 VEs on a single commodity server.
  - The achievable temporal accuracy of our system is subject to scheduler granularities, which are tunable in our system. We can explore the trade-off between execution speed and temporal accuracy (up to 30 µs).

- Parallel network simulation – S3F/S3FNet.
  - S3F simulation engine supports modular construction of simulation models that easily exploits parallelism.
  - The new engine design enables interactive communication with emulation.
  - It is flexible enough to create/explore various testing scenarios in a large-scale setting.
  - S3FNet provides sophisticated, low-level network layers and background traffic simulation.

Results and Benefits

- Developing S3F simulation engine, and S3FNet network simulator based on S3F.
- Implemented a virtual time system on OpenVZ.
  - High functional & temporal fidelity.
  - Good scalability: 320 VEs/single machine.
- Publications"
  - Zheng and Nicol. "A Virtual Time System for OpenVZ-Based Network Emulations," PADS'11.
  - Nicol, Jin, and Zheng. "S3F: The Scalable Simulation Framework Revisited," WSC'11, to appear.
  - Zheng, Nicol, Jin, and Tanaka. "A Virtual Time System for Virtualization-Based Network Emulations and Simulations," JOS'11, submitted.
- **Technology Readiness Level:** ongoing

Researchers

- David Nicol, dmnicol@illinois.edu
- Dong (Kevin) Jin, dongjin2@illinois.edu
- Yuhao Zheng, zheng7@illinois.edu

Industry Collaboration

- Boeing Corporation
- IBM Research

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components

tcipg.org

Overview and Problem Statement

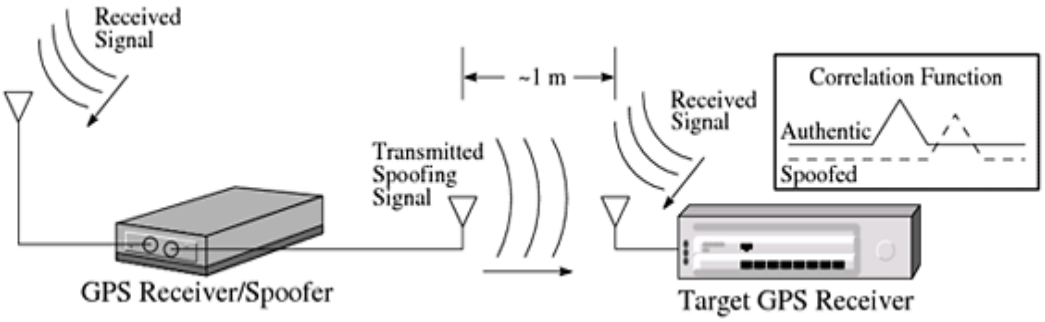
As the power system updates itself to new Smart Grid standards, its dependence on a cyber infrastructure of sensing, communication, and control is ever-increasing. Novel methods to address the coupling of this infrastructure to the physical components responsible for generation, transmission, and utilization of electrical energy need to be developed. Conventional analysis techniques mainly focus on the effects of faults in the physical components, e.g., power sources and transmission lines. Therefore, faults in the physical components are reasonably well-understood. However, the effects of faults in cyber components and their coupling with the physical infrastructure are not clear and require additional research.

Research Objectives

- Develop a taxonomy of possible faults in the cyber components pertaining to power systems.
- Investigate the effects of GPS spoofing on PMU time synchronization.
- Demonstrate the feasibility of an attack through hardware setup.
- Characterize potential PMU misbehavior due to faults in the cyber structure.
- **Smart Grid Application Area:** This research will allow for a more secure and reliable power grid.

Technical Description and Solution Approach

- The synchronization of PMUs depends on satellite GPS signals. Therefore, spoofing these signals constitutes an attack on data of the PMUs.
- The feasibility of such an attack is being demonstrated through MatLab simulation. The problem is cast into an optimization problem in which the objective is maximum phase error in the PMU data.
- The effects of losing such time synchronization for PMU data are being investigated.
- Based on the applications of PMU data, the impact of corrupted PMU data on power system dynamic performance and reliability is being characterized.



Results and Benefits

- Different methods of attack on PMU synchronization are being developed and simulated.
- Demonstration of the feasibility of these attacks is allowing for better preparedness against security threats.
- Simulation of GPS spoofing has been carried out in MatLab.

- Potential PMU misbehaviors are being identified and characterized. The possible causes of misbehavior include hardware faults, filtering algorithm implementation error, data communication failures, and/or GPS signal spoofing.
- Applications of PMU data are being investigated. A Thevenin-equivalent model to qualify the impact of PMU misbehaviors is being developed.
- **Technology Readiness Level:** Ongoing research.

Researchers

- Alejandro D. Domínguez-García, aledan@illinois.edu
- Xichen Jiang, xjiang4@illinois.edu
- Jiangmeng Zhang, jzhang67@illinois.edu

Security and Robustness Evaluation and Enhancement of Power System Applications

Overview and Problem Statement

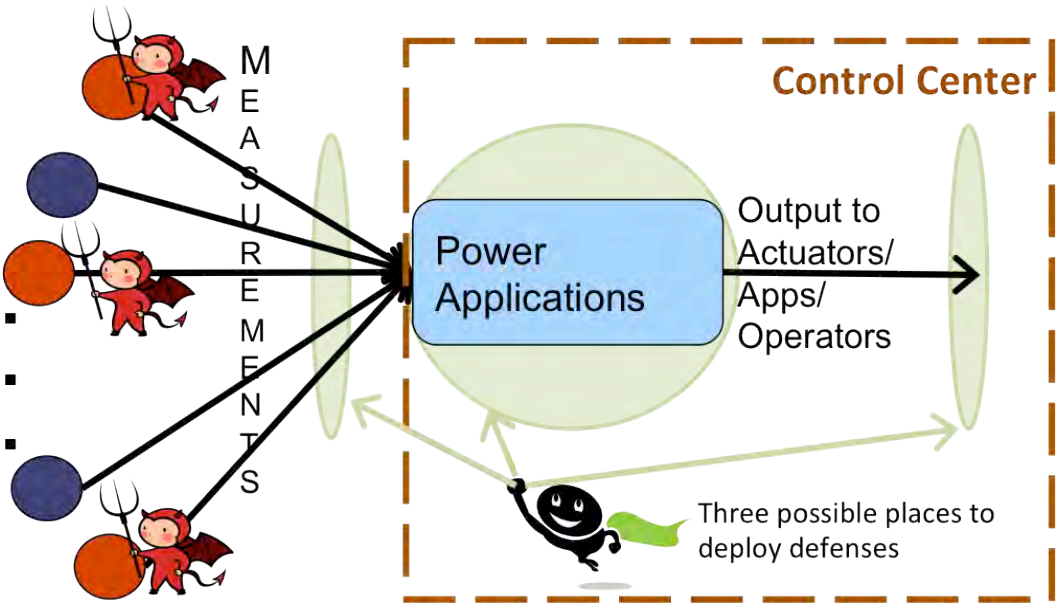
Power system operations rely on a multitude of sensor data from remote measurement devices at substations. The sensor data are communicated back to the control center using a variety of protocols (e.g., DNP3, Modbus) and communication media. The remote sensors and the communication channels over which their readings are communicated present an attack surface for adversaries wanting to disrupt power system operations. While power system applications are typically robust against erroneous sensor data and data loss due to accidents and failures, they are not robust against coordinated malicious sensor data modification. In this work, we address the problem of malicious sensor data manipulation in power systems.

Research Objectives

- Study the security and robustness of power applications in the face of malicious sensor data manipulation attacks.
- Develop effective and cost-efficient defenses against malicious sensor data manipulation attacks.
- Evolve a process to include security and robustness considerations during power system application design phase.
- **Smart Grid Application Area:** Risk and security assessment.

Technical Description and Solution Approach

- Understand the behavior of power system applications and analyze their robustness in the presence of malicious data modification.
- Leverage the physical properties (e.g., topology) of the underlying electrical network along with cryptographic and other cyber security mechanisms to design effective and cost-efficient security schemes.



Results and Benefits

- For DC state estimation, we showed that protecting a set of *basic measurements*, that is, those necessary for observability, is necessary and sufficient for detecting a class of false data injection attacks.
- Investigating a topology perturbation-based approach to defending against false data injection.
- Investigating the feasibility of leveraging dynamic system characteristics to detect malicious data.
- The outcomes of this project will be a robustness characterization of specific power applications with respect to malicious data modification attacks and mechanisms to improve the robustness of those applications.
- The outcomes of this project will provide:
    - Guidance on where to focus an organization's security budget to secure applications.
    - Input to operators and incident response engines as to when an application should be considered compromised.
- A longer-term benefit of this project would be the evolution of a process that includes security and robustness considerations during application design for future power applications.
- **Partnerships and External Interactions:** Collaborating with researchers at KTH Royal Institute of Technology in Sweden.
- **Technology Readiness Level:** This technology is currently in its infancy (research and design phase).

Researchers

- Rakesh B. Bobba, rbobba@illinois.edu
- Robin Berthier, rgb@illinois.edu
- Erich Heine, eheine@illinois.edu
- Miao Lu, mlu20@illinois.edu
- Kate Morrow, morrow4@illinois.edu
- Will Niemira, niemira2@illinois.edu
- Tom Overbye, overbye@illinois.edu
- Kate Rogers, krogers6@illinois.edu
- William H. Sanders, whs@illinois.edu
- Pete Sauer, psauer@illinois.edu
- Zheming Zheng, zheng34@illinois.edu
- Past Researchers: Qiyan Wang, Himanshu Khurana, and Klara Nahrstedt

Overview and Problem Statement

Renewable generation, energy storage, and demand response are key components of the Smart Grid vision. Effective use of these resources in future grids will require appropriate control architecture. This research focuses on investigations of control strategies for power grids with significant penetration of renewable generation, energy storage, and demand response resources. The goal is to understand how energy storage and demand response can provide ancillary services such as operational reserves and frequency regulation, thereby facilitating the use of volatile renewable generation in highly complex and constrained power networks. This understanding can lead to robust control schemes for future power grids.

Research Objectives

- Evaluate impacts of renewable generation, energy storage, and demand response on markets and operations.
- Investigate use of energy storage and demand response to facilitate integration of volatile renewable generation.
- Explore the potential for storage and demand response resources to provide ancillary services in constrained power networks with high penetration renewable generation.
- **Smart Grid Application Area:** Results can guide new policies, planning, and operations, thereby smoothing the transition towards the Smart Grid.

Technical Description and Solution Approach

- Questions of interest: How can energy storage and demand response be used in conjunction with renewable generation to provide services such as operational reserves, load following, and frequency regulation?
- Stochastic models for generation, demand, and storage that allow explicit consideration of impacts of volatility, dynamics, and uncertainty in both operations and markets are being used. Modeling abstractions for energy storage and flexible loads (e.g., HVACs and refrigerators), which explore similarities between both resources, are being developed.
- Research focus is on characterizing the control schemes to meet specific objectives. Each problem is formulated as a Markov Decision Process (MDP) and solved using reinforcement learning techniques that require very little or no knowledge of the underlying stochastic processes and can be driven by observations from real systems.
- Preliminary investigations on single bus systems are underway. Extensions to realistic network settings will follow soon.

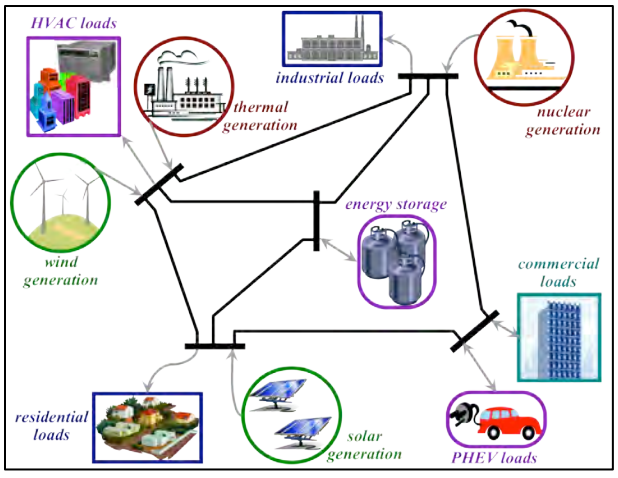


Fig. 1: Conceptual illustration of the key Smart Grid resources considered in the analysis

Results and Benefits

- A book chapter summarizing some key results on efficiency and pricing in electricity markets was submitted for publication in the book *Control and Optimization Theory for Electric Smart Grids*. An important observation from the simulation studies was the reduction in price volatility with increasing demand response (see Fig. 2).
- A conference paper investigating the role of flexible demand-side resources in the generation scheduling process was presented at the 2011 IEEE PES General Meeting. Numerical studies demonstrated the effectiveness of demand-side resources in facilitating integration of volatile renewable generation.

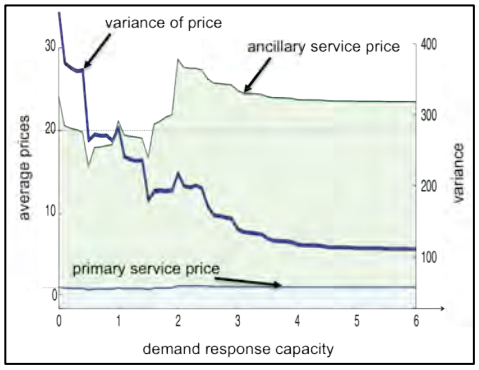


Fig. 2: Reduction in price volatility with increasing demand response

- Recent efforts have been focused on characterizing operational strategies for storage and demand-response resources to meet specific objectives, such as smoothening the output of renewable generators and providing frequency regulation services. Reinforcement learning algorithms have been tested for optimal control problems regarding use of energy storage to smoothen the output of wind generators.
- Proposed techniques can be used to develop operational tools that do not use artificial models for the system resources and environment. Also, simulation results can guide new policies, such as policies that provide incentives for ancillary services from buildings or those that promote new market mechanisms that encourage demand-side participation, and so on.
- **Partnerships and External Interactions:** Technical discussions with PNNL.

Researchers

- Anupama Kowli, akowli2@illinois.edu
- Sean Meyn, meyn@illinois.edu

Industry Collaboration

- ISONE, PJM, PNNL, UTC

Testbed-Driven Assessment: Experimental Validation of System Security and Reliability

Overview and Problem Statement

The objective of this project is to develop methods and tools for evaluating security and reliability protection mechanisms for the next-generation power grid. Specifically, this research will focus on development of a framework for error diagnosis and experimental validation of system/application resiliency to errors and attacks. In particular, we want to experimentally evaluate 1) the impact of accidental errors on microprocessor-based power grid equipment and 2) the bad data detection algorithm for PMU data.

Research Objectives

- Experimentally study the impact of errors on next-generation microprocessor-based power grid equipment.
  - Characterize error behavior and failure severity due to transient errors in the power grid equipment.
  - Understand error propagation and its impact from one piece of equipment to other connected equipment.
  - Develop and test error detection and recovery techniques to address the weaknesses discovered.
- Experimentally verify the bad data detection algorithm.
  - Study how PMU data can be corrupted.
  - Understand how to synchronize state estimation data and PMU data to achieve data redundancy.
  - Exploit the redundancy of state estimation data and PMU data for bad data detection.
- **Smart Grid Application Area:** To uncover possible security vulnerabilities in current power grid applications and investigate reliability and security protection mechanisms/strategies.

Technical Description and Solution Approach

- Experimentally study the impact of transient errors on microprocessor-based power grid equipment.
  - Build a testbed for experimental evaluation of error characterization, see Figure 1.
    - SEL-AMS simulating field transmission line voltage and current value and the line breaker.
    - SEL-421 Relay reads the voltage and current value from SEL-AMS.
    - SEL-RTAC aggregates all the signal values within the substation.
    - SCADA master pulls the substation data from SEL-RTAC.
    - SCADA master can send control signal to control SEL-421 (e.g., open/close breaker).
  - Develop a fault/error injection tool for SEL-RTAC to simulate processor and memory errors.
  - Study error propagation and its impact on adjacent connected equipment and overall control of power grid equipment.

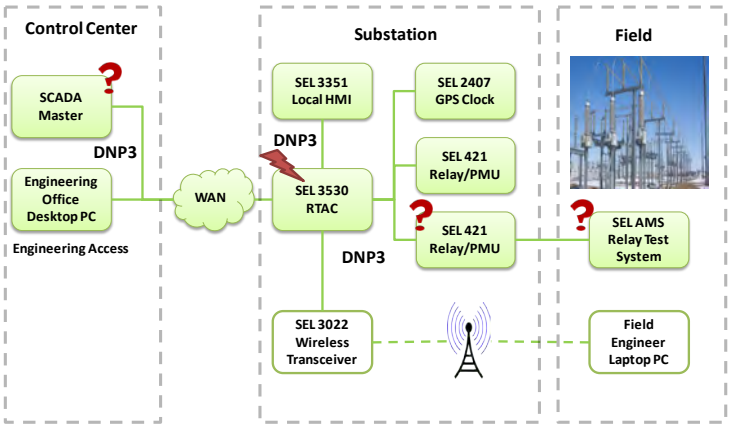


Figure 1

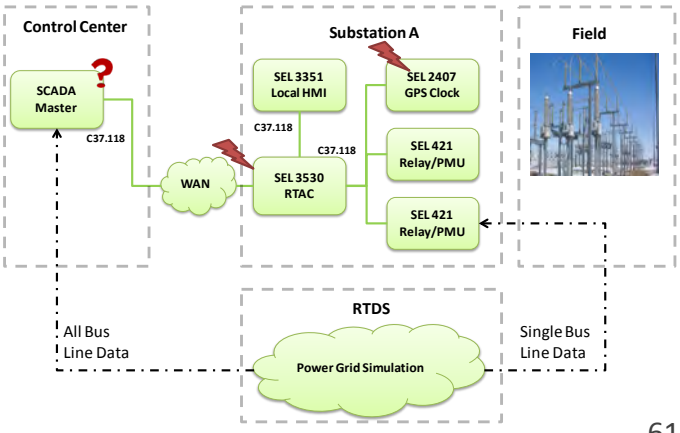


Figure 2

- Experimentally verify the bad data detection algorithm.
    - Build testbed to simulate power grid using both real power equipment and RTDS (Real Time Digital System); see Figure 2.
        - Based on the testbed setup, we added RTDS to simulate a power system.
        - PMU-monitored bus data simulated by RTDS feeds into the SEL-421 Relay.
        - Power system data simulated by RTDS feeds into the SCADA.
        - SEL-421 Relay connected with GPS clock can act as a PMU and generates synchrophasor data.
        - PMU data are aggregated and sent back to the control center.
    - Develop a fault/error injection tool to corrupt PMU data.
        - By spoofing the GPS clock transceiver so the PMU timestamp becomes incorrect.
        - By corrupting the PMU data along the communication path from the PMU to the control center.
    - Test and validate bad data detection algorithm.

Results and Benefits

- Discovered that a single-bit error in the DNP3 Client process could leave the client unable to send the most current data or receive control commands from the DNP3 Master process.
- Discovered that a single-bit error in the codesys_rte program could cause the configuration of SEL-RTAC to reset, thus causing the SCADA master to lose all communication with the devices connected to the SEL-RTAC.
- **Partnerships and External Interactions:** RTDS, SEL.
- **Technology Readiness Level:**
    - Testbed infrastructures for both scenarios are in place.
    - Fault/error injector to create transient errors has been developed.
    - Fault/error injector to spoof the GPS clock has not been implemented yet, but we can inject faults to corrupt PMU data along its communication route.
    - Early prototype of bad data detection algorithms has been developed for evaluation.

Researchers

- Daniel Chen, dchen8@illinois.edu
- Jiangmeng Zhang, jzhang67@illinois.edu
- Kuan-Yu Tseng, ktseng2@illinois.edu
- Hui Lin, hlin33@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks

tcipg.org

Overview and Problem Statement

Operators of wireless networks must have cheap, commodity tools for assessing security of their networks. Lack of such tools leads to unnecessary exposure and false assumptions regarding stability of these networks, as experience of 802.11/Wi-Fi has amply shown. At the very least, a network operator must know how much of his or her RF is showing and what it looks like to an attacker with a sufficiently powerful antenna and the ability to emit and inject wireless frames of the protocols used by the network. Our ***Api-do*** tools give the operators this functionality with commodity USB peripherals and software that runs on a regular Linux laptop.

Research Objectives

- Make 802.15.4/ZigBee wireless network assessment tools as easy and efficient as those for 802.11/Wi-Fi.
- Enable asset owners to survey their network footprint ("wardrive" their networks).
- Enable asset owners to test the effects of crafted frame injection and reflexive/selective jamming.
- Facilitate the exploration of the 802.15.4/ZigBee attack surface.
- **Smart Grid Application Area:** 802.15.4/ZigBee is the networking technology of choice for SCADA systems, home automation, and smart meter connectivity.

Technical Description and Solution Approach

- Api-do tools use commodity digital radio platforms built on chips such as Chipcon CC2420 and similar ones, with custom firmware (based on Travis Goodspeed's GoodFET). Frames received by digital radio chips are processed by a microcontroller on the peripheral (such as the MSP430 or Atmel AVR). This allows fast interaction with the target network, which is difficult to achieve with more expensive software-defined radios.
- "Security does not improve until tools for practical exploration of the attack surface become available" – Joshua Wright.

Results and Benefits

- First generation of tools released, presented at security practitioner conferences, and used in assessments.
- Important signaling vulnerability exposed in 802.15.4 digital radios, presented at USENIX WOOT 2011.
- **Partnerships and External Interactions:** Contributions and improvements to KillerBee tools (Joshua Wright), Scapy suite.
- **Technology Readiness Level:** Beta, tools in ongoing development.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Ryan M. Speers, Ricky Melgares: contact through http://code.google.com/p/zigbee-security/

Industry Collaboration

- Travis Goodspeed, Joshua Wright, other contributors

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Trustworthiness Enhancement Tools for SCADA Software and Platforms

Overview and Problem Statement

Our ultimate goal is to develop tools that help maintain the trustworthiness of the various embedded control systems being rolled out as part of the smart grid. Since embedded power systems must satisfy certain restrictive conditions (constant availability, strict application timing requirements, etc.) on top of the resource restrictions inherent to embedded devices (less memory, slower processors, etc.), the "standard" approaches to securing devices—for example, installing patches and using virtualization in some manner to monitor the system—cannot feasibly be applied. Thus, any tools we design must be performance-aware and allow the devices they protect to perform their primary duties without interference.

Research Objectives

- Identify the constraints under which embedded control systems in the grid operate.
- Design tools that incorporate the ideas behind the "standard" approaches, and find ways to apply them such that they conform to the rules of engagement in the power grid.
- **Smart Grid Application Area:** Embedded SCADA systems that perform mission-critical tasks and cannot afford to be taken out of service or spend much time performing security computations.

Technical Description and Solution Approach

- We have developed two tools to address the problems stated above:
    - **Katana:** A hot-patching tool that allows users to reason about the results of applying a patch (to ensure that the patch will not adversely affect the system), and then install the patch without taking the target system out of service.
    - **Autoscopy Jr.:** A lightweight intrusion-detection system that operates inside the kernel, monitoring its host for control-flow anomalies indicative of a malicious program while still allowing the host to perform its primary duties unhindered. The program also includes a system profiler, which allows a user to intelligently manage the system's mediation scope to better balance security with performance.

Results and Benefits

- Our Katana prototype has been completed and released publicly (http://nongnu.org/katana/).
- We evaluated the performance impact of Autoscopy Jr. on a non-embedded kernel configuration, and found that after our profiler was applied, it imposed less than a 5% overhead on our benchmark tests.
- **Partnerships and External Interactions:** Currently, we are in talks with SEL to test Autoscopy Jr. on examples of embedded power systems, and potentially incorporate our system into their products.
- **Technology Readiness Level:** Currently, both projects are in the prototype stage, but we are working with SEL to refine Autoscopy Jr. for use in industry.

Researchers

- Jason Reeves, reeves@cs.dartmouth.edu
- Sergey Bratus, sergey@cs.dartmouth.edu
- Sean Smith, sws@cs.dartmouth.edu
- James Oakley (2009–2011)

Industry Collaboration

- Schweitzer Engineering Laboratories

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Vulnerability Assessment Tool Using Model Checking

tcipg.org

Overview and Problem Statement

This activity focuses on identification of potential vulnerabilities in software. We use a combination of symbolic execution and model checking to systematically analyze corruptions of the application data and identify cases that lead to a successful attack. The results from the analysis can then be used to remove application-level vulnerabilities and guide design of defense mechanisms to protect applications from attacks.

Research Objectives

- Design a technique and a tool to discover vulnerabilities in an application using symbolic execution and model checking.
- Generate signatures for critical data to be checked at runtime.
    - Identify critical data, i.e., data that, if corrupted, lead to a successful attack.
    - Identify critical code sections, i.e., instruction sequences during the execution of which corruption of critical data allows the attacker to achieve objectives (e.g., login with an invalid password).
- Demonstrate the tool on applications used in the context of power grid applications.

Technical Description and Solution Approach

The core component of our approach is SymPLFIED, a formal framework that uses symbolic execution and model checking to:

- Identify conditions (e.g., what data and when at runtime to corrupt) under which the attacker (e.g., an insider) can penetrate the system.
- Introduce memory errors and propagate the error's consequences using symbolic execution and model checking.
    - Output produced:
        - *When to inject the fault:* at which instruction.
        - *Where to inject:* what memory address.
        - *What to inject:* what value (range of values).
- Determine memory locations that need to be protected to prevent application failure or system compromise.

The proposed overall formal framework is shown in the below figure.

Results and Benefits

The analysis conducted using the SymPLFIED-based formal framework allows generation of trusted signatures, which can be used to implement runtime checking. They consist of two parts:

- *Instruction Signature:*
    - Stores unique identifiers (e.g., PC) for critical instructions.
    - Only critical instructions can write to critical data (prevents code injection).
- *Data Signature:*
    - Stores addresses of critical data in the program.
    - Content of critical memory locations is tracked on all writes through maintenance of a copy of the data.
    - On all reads, the copy of the data fetched by the program is checked against the one stored as part of the data signature (ensures data integrity).

The SymPLAID tool is available as a research prototype and can analyze applications compiled for SPARC or MIPS ISA (Instruction Set Architecture). The tool has been demonstrated on real-world applications, including embedded code and network applications, e.g., SSH.

Researchers

- Prateek Patel, patelprateek@gmail.com
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

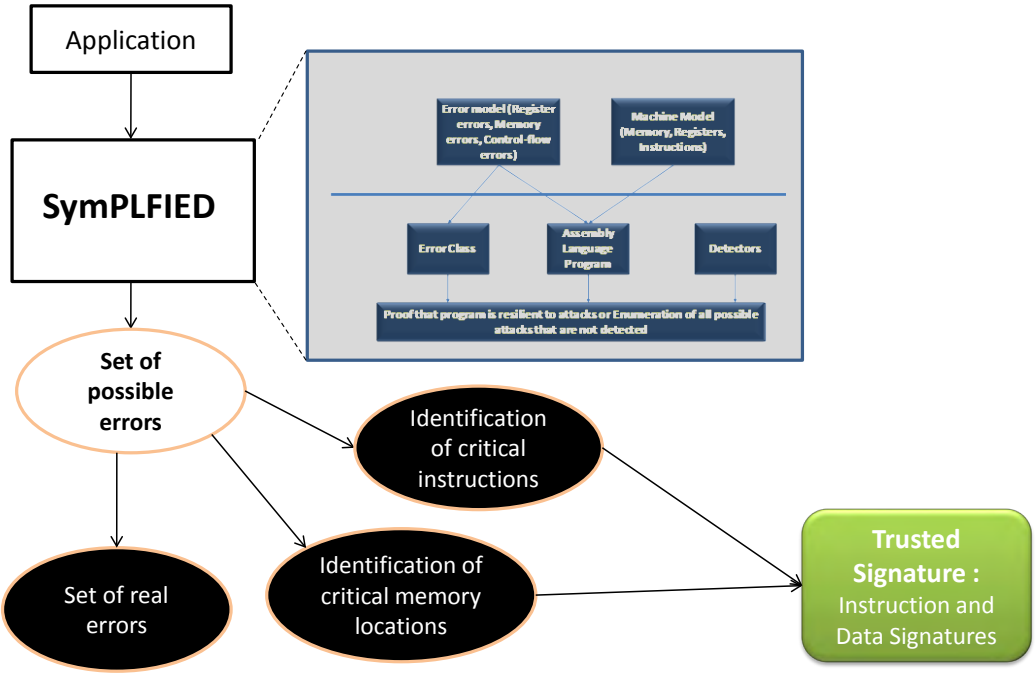


Figure 1: Formal Analysis Framework

Research Cluster

Cross-Cutting Efforts

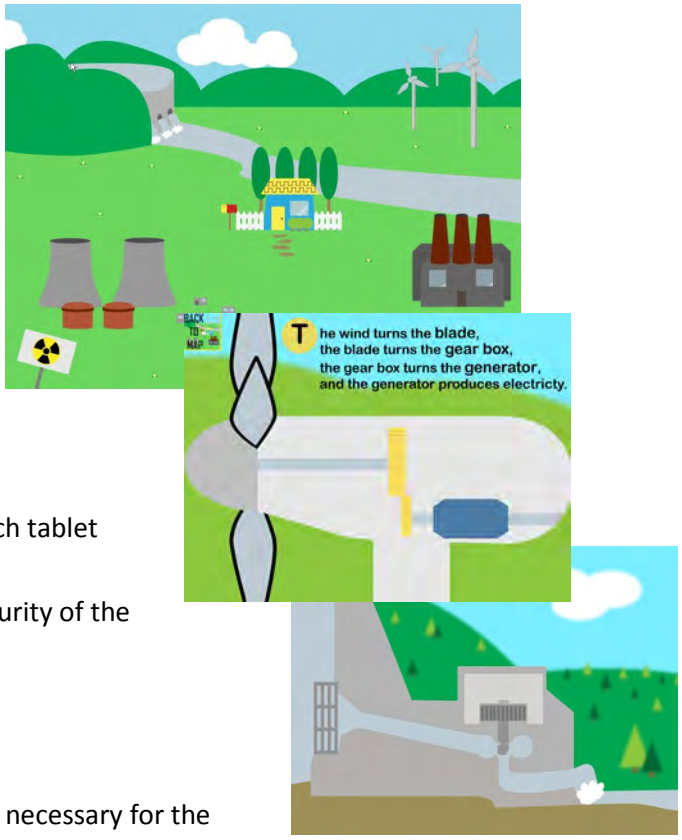
Cross-Cutting Efforts Page No.

TCIPG Education and Engagement

Overview

The success of the modernization of the U.S. electrical grid depends on research, engineering, and policy, but also on the education and acceptance of electricity consumers. Members of the TCIPG Education team work with other TCIPG researchers to develop a variety of educational opportunities. Our activities are designed to engage learners of all ages. We develop curriculum materials that involve young people in virtual power system simulations. Our most recent efforts involve producing an interactive e-book for younger children using the iPad and other touch tablet devices. The materials provide information about the importance and workings of current and future electricity generation and delivery systems. They are designed to engage students who may pursue careers in related industries. Nearly one hundred practitioners, researchers, and graduate students attended the TCIPG-sponsored Cyber Security for Smart Energy Systems Summer School held June 13-17, 2011, in St. Charles, Illinois. The program provided background in the basics of cyber security and in the traditional generation, transmission, and distribution systems of the power grid. TCIPG engages in public outreach through participation in the annual Engineering Open House at the University of Illinois at Urbana-Champaign and through the ongoing interactive "Mission Smart Grid" exhibit at the Orpheum Children's Science Museum in Champaign, Illinois. A traveling exhibit is in the planning stages.

Objectives



- Link researchers, educators, students, and consumers in efforts to realize a modern electrical system.
- Provide engaging interactive curriculum, appropriate for middle-school-level and older students, featuring:
  - time-sensitive pricing
  - demand-side management
  - impacts of plug-in hybrid vehicles
  - distributed generation
  - technologies that increase energy efficiency and reliability
  - concepts related to communication networks
- Create an interactive e-book for the iPad and other touch tablet devices that is appropriate for young learners.
- Develop a CyberCIEGE scenario related to the cyber security of the power grid.
- Create smart grid picture resource cards.

- **Smart Grid Application Area:**
  - Reach the wider audience of educated citizenry necessary for the successful implementation of smart grid technologies.
  - Educate consumers to use new technologies that allow them to actively manage their energy use and costs.
  - Engage pre-university students who may pursue a related career.

Results and Benefits

- Java applets and curriculum materials illustrating time-of-use pricing and concepts related to communication networks.
    - Updates to print materials.
    - New versions for use with touch tablet devices are being piloted.
- Interactive e-book for the iPad and other touch tablet devices.
- Cyber Security for Smart Energy Systems Summer School, a workshop for researchers and practitioners from industry, national laboratories, and academia, was held June 13-17, 2011 in St. Charles, Illinois.
    - Provided background in the basics of cyber security, and in the traditional generation, transmission, and distribution systems of the power grid.
    - Idaho National Laboratory offered a hands-on SCADA Security Lab.
- **Partnerships and External Interactions:**
    - Exhibit at the Orpheum Children's Science Museum (OCSM)
    - Curriculum connections with National 4-H SET (Science, Engineering and Technology) Initiative
    - Curriculum connections with KidWind and WindWise Education
    - Inclusion in Project Lead the Way middle-school curriculum materials for Energy and Environment
    - Inclusion in WindWise Education curriculum (funded by NYSERDA)
    - Inclusion in The 8 Best Electricity Grid Primers – GridWatch
    - Inclusion in CIP Vigilance Power Grid posts
    - Inclusion in GM Education Teacher Blog

Events

- Project Lead the Way Core Training Preparation, April 28–30, Las Vegas, Nevada
- University of Illinois Public Engagement Symposium, March 9, Champaign, Illinois
- Green and Renewable Energy Workshop, June 20–30, Lewis University, Romeoville, Illinois
- Project Lead the Way Summer Training, June 19–July 1, University of Illinois at Urbana-Champaign

Education Team

- Jana Sebestik, sebestik@illinois.edu
- George Reese, reese@illinois.edu
- Zeb Tate, zeb.tate@utoronto.ca
- Quinn Baetz, qbaetz2@illinois.edu
- Jason Mormolstein, jmormol2@illinois.edu
- Andrew Gazdziak, gazdzia1@illinois.edu

Testbed Overview

Overview and Problem Statement

- How does one provide a large-scale, realistic, end-to-end power grid experimentation platform that is both repeatable and flexible to cover both legacy and emerging research?
- How does one leverage real equipment, simulation, and emulation to provide the necessary capabilities?
- How does one programmatically integrate, control, and interact with power grid equipment that was not designed with that in mind?

Research Objectives

- Provide for experimental support/integration of TCIPG projects.
- Provide a simulation and emulation environment with real hardware and software used in the power grid.
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems.
- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities.
- **Smart Grid Application Area:** End-to-End.

Technical Description and Solution Approach

- Develop new modeling and evaluation technologies to enhance evaluation capabilities of the testbed.
- Continue to expand the equipment capabilities, features, and functionality through strategic integration of both software and hardware.
- Develop integration glue to seamlessly integrate power grid equipment and software into the testbed by coupling simulation, emulation, and real equipment.
- Leverage existing and emerging research from other areas when the testbed effort can benefit from it.

Results and Benefits

- Real-time Immersive Network Simulation Environment (RINSE): large-scale network simulation.
- Virtual Power System Testbed: cyber/physical coupling of simulation, emulation, and real equipment.
- Network Access Policy Tool (NetAPT): policy tool to evaluate network access paths and verify compliance with a global policy.
- **Partnerships and External Interactions:**
    - Enabling smart grid research and transition of technology.
    - Leveraged for other industry interactions and projects.
- **Technology Readiness Level:** Extending capabilities, but fully functional and in-use.

Capabilities

- Full end-to-end “Smart Grid” capabilities.
- Real, emulated, and simulated hardware/software.
- Real data from the grid, industry partners, etc.
- Power simulation, modeling, and optimization.
- Network simulation and modeling.
- Visualization.
- WAN/LAN/HAN integration and probes.
- Security assessment tools (e.g., static analysis).
- Protocol assessment tools (e.g., harnesses, fuzzing).

Hardware and Software

- RTDS, PowerWorld, PSSE, PSCAD, DSAtools Suite, DynRed.
- RINSE, testBench, LabView, OSI PI, OSIi Monarch, SEL suites.
- GPSs, substation comps, relays, testing equipment, PLCs, security.
- RTUs, F-Net, ICS firewalls, inverters, DAQs, oscilloscopes, multimeters, gigabit firewalls and switches, embedded devices.
- Home EMS, monitoring devices, Zigbee, automation.
- Display wall, visualization platforms, training.
- Mu Dynamics, Fortify, security research tools.
- DETER/Emulab integration and extension.

Use Cases

- Provide a multi-faceted approach to security through testbeds, education and training, field testing, and tool creation.
- Facilitate collaboration among researchers and industry to work towards creation of more resilient critical infrastructure.
- Facilitate rapid transition and adoption of research by industry.
- Provide positive real-world impact through engagement.

Researchers

- Tim Yardley, yardley@illinois.edu
- David Nicol, dmnicol@illinois.edu
- William H. Sanders, whs@illinois.edu
- Jeremy Jones, jmjone@illinois.edu
- Erich Heine, eheine@illinois.edu

Industry Donations

Byres Security, Endace, GE, InStep Software LLC, Mu Dynamics, Open Systems International (OSI), OSIsoft, PowerWorld, Schweitzer Engineering Lab, Siemens AG, Trilliant Inc.

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security