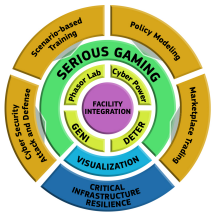
SMART AMERICA

SMART ENERGY CPS



The Nation's energy infrastructure is a complex cyber physical system (CPS) that forms the lifeline of modern society, and its reliable and secure operation is of paramount importance to national security and economic well-being. Our energy infrastructures are aging and highly vulnerable to natural events (e.g. hurricanes, earthquakes, etc.) and to man-made malicious events such as sophisticated cyber attacks. A critical need is the significant undertaking of fundamental and applied research that can transform our legacy infrastructures into smart ones that are resilient against extreme events, secure against cyber attacks, efficient in performance, and sustainable.

RESEARCH CHALLENGES:

- **Efficient Smart Energy Designs**
  - Methodologies for "co-design" of information, communication, and controls for wide-area monitoring, protection, and control of power grids.
  - Standards and technologies for time synchronized CPS networks.
  - Development of distributed and parallel algorithms for grid monitoring and control.
- **Resiliency and Cybersecurity**
  - Fundamental architectural paradigms and technology building blocks transforming "fault-resilient grid of today into an attack-resilient grid of the future".
  - Pragmatic risk modeling and mitigation framework capturing cyber-physical interdependencies and the dynamic nature of cyber threats and uncertainty using game-theoretic and behavioral models.
  - Understanding sophisticated coordinated attacks, cascading failures, and developing robust defensive technologies to achieve security, privacy, and resiliency.
- **Federated CPS Infrastructures and Testbeds**
  - Development of a national-scale high-fidelity, federated CPS testbed with remote access capabilities, to accelerate the pace of innovation and R&D.
  - Experimentation methods for the design and analysis of multi-resolution wide area control experiments for coherent simulation at appropriate time scales.
  - CPS Cloud architecture, algorithms, and services for resource provisioning, allocation, and control across federated facilities for large-scale, high-fidelity experimentation requirements.
  - A open and shared experimentation infrastructure for cross cutting CPS sectors (e.g. gas and oil and power and energy).
  - Serious games to explore the resiliency control and economic incentives in wide area control.

Terry Benzel, USC-ISI
Aranya Chakrabortty, NC State
Manimaran Govindarsau, Iowa State
Adam Hahn, Mitre Corp
Alefiya Hussain, USC-ISI
Brian McCleery, National Instruments
Jason Nichols, Scitor Inc

Related References:

Aranya Chakrabortty

1. A. Chakrabortty, "Wide-Area Control of Large Power Systems Using Dynamic Clustering and TCSC-Based Redesigns," *IEEE Transactions on Smart Grid,* vol. 3(3), Sep. 2012.
2. A. Chakrabortty, J. H. Chow and A. Salazar, "A Measurement-based Framework for Dynamic Equivalencing of Power Systems using Wide-Area Phasor Measurements," *IEEE Transactions on Smart Grid,* vol. 1(2), pp. 68-81, 2011.
3. T. R. Nudell and A. Chakrabortty, "A Graph-Theoretic Algorithm for Localization of Forced Oscillation Inputs In Power System Networks, " *American Control Conference,* Portland, OR, June 2014.
4. S. Chandra, D. F. Gayme, and A. Chakrabortty, "Coordinating Wind Farms and Battery Management Systems For Inter-area Oscillation Damping Control: A Frequency Domain Approach," *to appear in IEEE Transactions on Power Systems*, 2014 (available online in IEEExplore).
5. A. Chakrabortty and Y. Xin, "Hardware-in-the-Loop Simulations and Verifications of Smart Power Systems Over an Exo-GENI Testbed," *proceedings of 2nd GENI Research and Educational Experiment Workshop*, GREE2013, Utah, Mar. 2013.

Manimaran Govindarsau & Adam Hahn

1. S. Sridhar and M. Govindarasu, "Model-based Attack Detection and Mitigation for Automatic Generation Control," IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580-591, March 2014.
2. A. Hahn, A. Ashok, S. Siddharth, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," IEEE Transactions on Smart Grid, vol. 4, no. 2, pp. 847-855, June 2013.
3. M. Govindarasu, A. Hah, and P. Saure, "Cyber-Physical Systems Security for Smart Grid", "The Future Grid to Enable Sustainable Energy Systems" PSERC Publication 12-02, prepared for U.S. DOE, Feb. 2012.
4. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical Security for Electric Power Grid," Proceedings of the IEEE, Special issue on Cyber Physical Systems, vol. 100, no. 1, pp. 210-224, Jan. 2012.
5. A. Hahn and M. Govindarasu, "Cyber Attack Exposure Evaluation Framework for the Smart Grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835-843, Nov. 2011.
6. C.-W. Ten, M. Govindarasu, and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," IEEE Transactions on Systems, Man, and Cybernetics - Part A, vol.40, no.4, pp.853-865, July 2010.

Alefiya Hussain

1.A. Hussain, et al, "Enabling Collaborative Research for Security and Resiliency of Energy Cyber Physical Systems", IEEE Workshop on Cyber-Physical Systems Security (CPS-Sec), Marina Del Rey, California, May, 2014
2. Saurabh Amin, Galina A. Schwartz, Alefiya Hussain: In quest of benchmarking security risks to cyber-physical systems. IEEE Network 27(1): 19-24 (2013)
3. A. Hussain and S. Amin, "NCS Security Experimentation using DETER", Proceedings of the First Conference on High Confidence Networked Systems, Hi-ConS '12, CPSWeek, Beijing, China, April 2012.
4. A. Viswanathan, A. Hussain, J. Mirkovic, S. Schwab, J. Wroclawski, "A Knowledge Framework for Data Analysis in Networked Systems," Proceedings of the 8th USENIX Symposium on Networked Systems Design and Implementation, NSDI '11, Boston, MA, pp 127–140.
5. A.Hussain, J. Heidemann, C. Papadopoulos, "Identification of Repeated Denial of Service Attacks", Proceedings of 25th IEEE International conference on computer communications, IEEE INFOCOM '06, Barcelona, Spain, pp 1–15.