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

Overview and Problem Statement

Information technology systems are increasingly being incorporated into power systems as a significant part of the smart grid vision. The interaction of cyber components and physical components adds higher levels of uncertainty, vulnerability, and complexity to the power grid. For instance, potential cyber-attacks, device faults, and even noisy measurements and communication networks may raise challenges for system operations. Meanwhile, deep penetration of renewable-based generation introduces an additional source of uncertainty, which may require advanced cyber infrastructure for fast response. Those uncertainties from cyber and physical components are the main factors affecting system monitoring and control performance. This study will quantify the impacts on power systems of those physical and cyber challenges.

Research Objectives

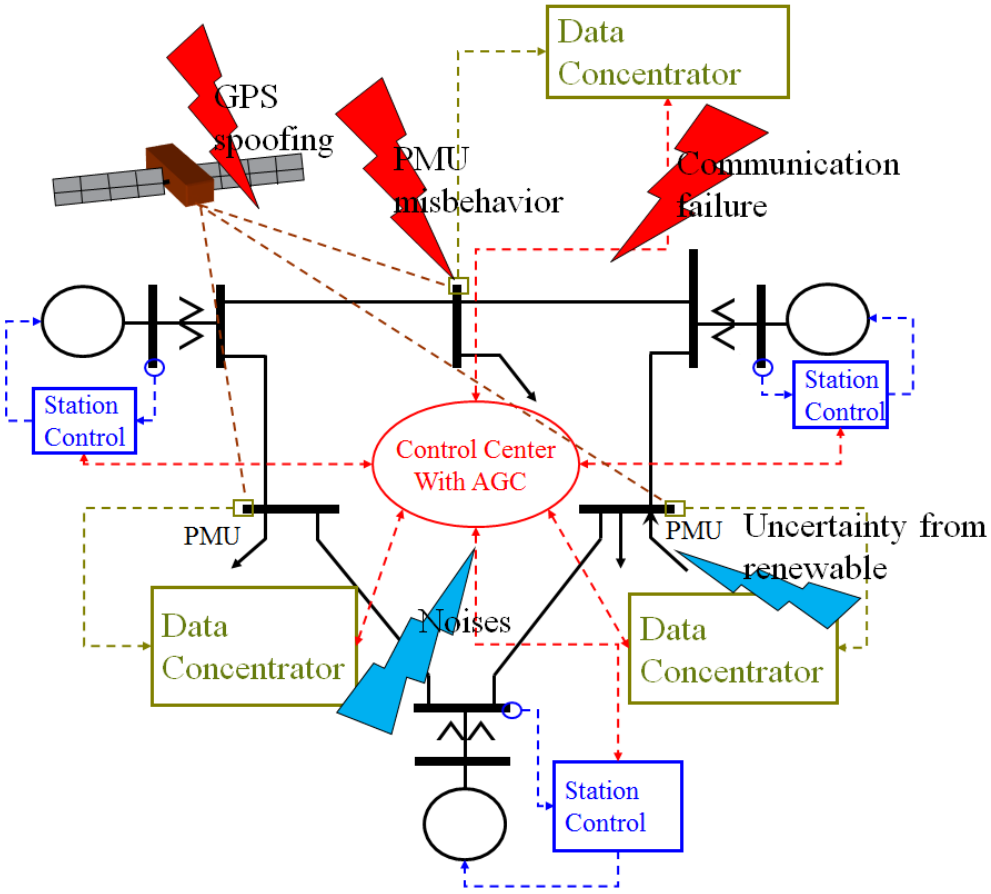
- Develop an exhaustive taxonomy of uncertainty factors in both cyber and physical components in a power grid:
    - Physical-related events: potential faults in physical infrastructure for generation and transmission, and uncertainties from renewable energy sources;
    - Cyber-related events: potential faults, attacks, and noise in cyber infrastructure for measuring, communication, and control.
- Construct appropriate models to quantify the impacts of uncertainties defined in the taxonomy on system dynamic performance and reliability.

Technical Description and Solution Approach

- Identify faults and misbehaviors of cyber components commonly used for communication and control in the power grid. In terms of the impact on the transmitted data quality, the faults/attacks are grouped into two classes: one impacting data integrity (e.g., data are manipulated because of device faults or man-in-the-middle attacks), and the other impacting data availability (e.g., communication delay due to network traffic or malicious DoS attacks).
- Assess the impact of the uncertainties affecting system operations and control on overall system dynamic performance and reliability, through tools from stochastic system analysis.

Results and Benefits

- Uncertainty due to renewable-based generation, measurement and network noise, and potential continuous attacks on communication networks is properly modeled as a set of stochastic processes.
- A framework to evaluate the impact of various uncertainty factors has been set up. First, a comprehensive power system model with automatic generation control has been formulated as a stochastic hybrid system. Based on the model, the statistics of system performance metrics (e.g., system frequency) are being evaluated.



- We have proposed a variety of system communication network attack scenarios that would adversely affect power system performance metrics. Two classes of attack scenarios have been identified that would significantly degrade the system performance. One scenario is to impose properly tuned random noise into the measurements. The other one is to introduce random delay in the communication network.
- **Technology Readiness Level:** Ongoing research. Preliminary results are being obtained as expected on test systems.

Researchers

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