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

A. D. Domínguez-García and J. Zhang

## GOALS

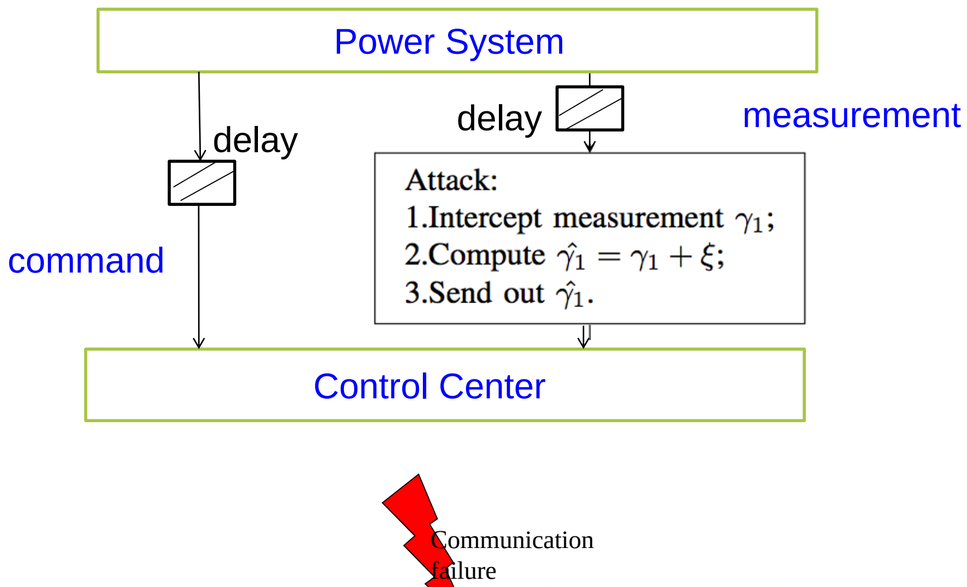
- Develop an exhaustive taxonomy of the potential faults in cyber components.
- Construct appropriate models to quantify the impacts of such faults on the physical system's stability and reliability.
- Build an overall framework for combining cyber and physical information to monitor, control, and protect power systems.

## FUNDAMENTAL QUESTIONS/CHALLENGES

- The operation of most modern electrical energy systems is dependent on a cyber infrastructure of sensing, communication, and control devices (cyber components). However, conventional analysis methods are:
  - Focused on impact of faults in the physical infrastructure for generation and transmission.
  - Not well-equipped to describe the impact of faults in the cyber infrastructure that controls the physical infrastructure.
- Without adequate emphasis on the impact of integrating new technologies, ad hoc system designs will likely lead to the deployment of poorly understood, unreliable, and unsafe systems, which could have catastrophic consequences.

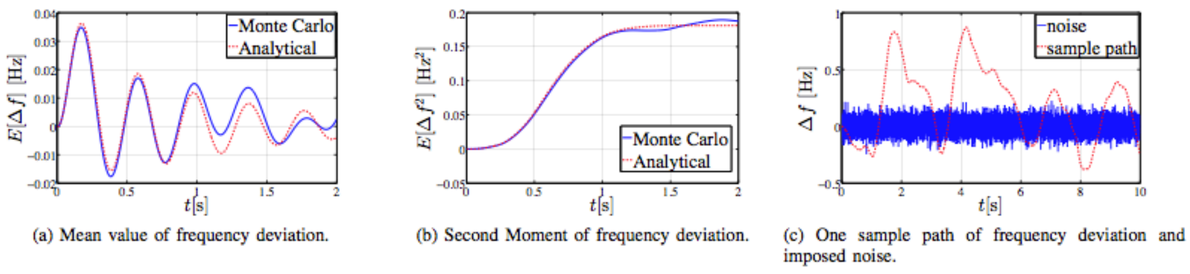
## RESEARCH PLAN

- Identify faults and misbehaviors of cyber components commonly used for communication and control of the power grid.
  - On data integrity.
  - On data availability.
- Characterize the effect of these faults on overall system dynamic performance and reliability through tools from developed hybrid system analysis.
  - Determine that a class of hard-to-detect failures/attacks on measurement integrity may destabilize power systems by introducing random noise.
  - Determine that a class of failures/attacks on measurement availability (e.g., communication delays, DoS attacks) may destabilize a power system.
- Develop analysis tools to improve system stability and reliability by exploiting information from advanced cyber components.



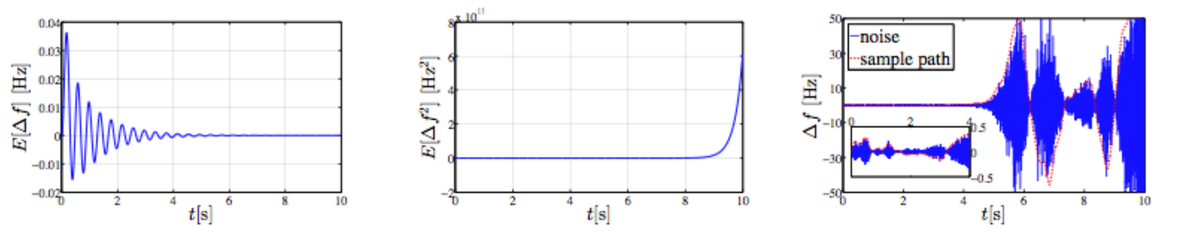

## RESEARCH RESULTS

- Impact of failures/attacks on data integrity
  - With white noise, the system is stable.

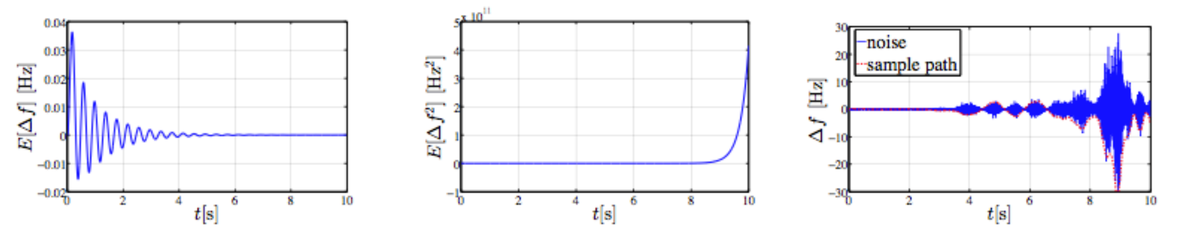



(a) Mean value of frequency deviation. (b) Second Moment of frequency deviation. (c) One sample path of frequency deviation and imposed noise.

  - With intensity-tuned noise, the system is unstable.

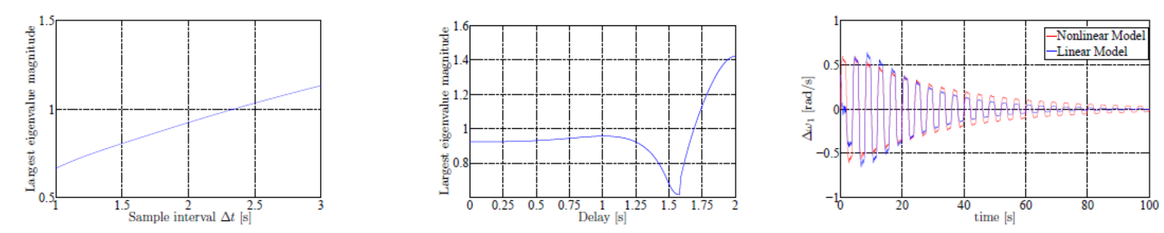



(a) Mean value of frequency deviation. (b) Second Moment of frequency deviation. (c) One sample path of frequency deviation and imposed noise.



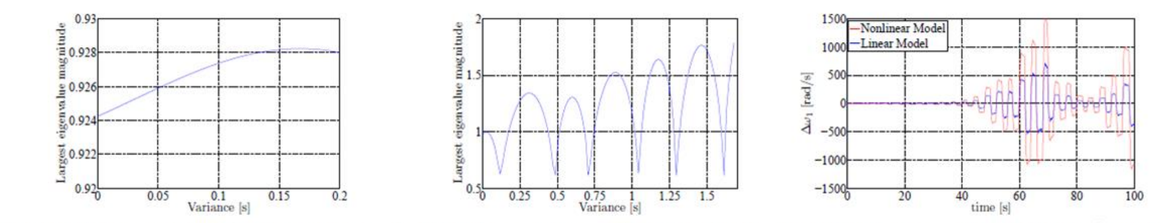

(a) Mean value of frequency deviation. (b) Second Moment of frequency deviation. (c) One sample path of frequency deviation and imposed noise.

- Impact of failures/attacks on data availability (i.e., delays).
  - With deterministic delay.




(a) Eigenvalues vs. sample interval. (b) Eigenvalues vs. communication delay. (c) Simulation with 1.7 s deterministic delay.

  - With random delay




(a) Eigenvalue vs. variance with a mean of 0.2 s. (b) Eigenvalue vs. variance with a mean of 1.70 s. (c) Simulation at 1.7 s delay with 0.02 s$^2$ variance.

## BROADER IMPACT

- The research will help accomplish the Smart Grid vision by providing powerful tools for engineering more reliable and more responsive electrical energy systems.
- Attack vector identification serves as the first step to develop secure cyber and physical infrastructure in the power grid.
- The methods and tools developed will also help to broaden the understanding of cyber-physical systems.

## INTERACTION WITH OTHER PROJECTS

- Activity "understanding and mitigating the impacts of GPS/GNSS vulnerabilities" has investigated one specific cyber component that can introduce impactful failures/attacks.

## FUTURE EFFORTS

- Exhaustive summary of the impact of faults/attacks in cyber components is under development.
  - The sensitivity of attack performance to system parameters needs to be studied quantitatively.
  - The impact of similar attacks on control commands is left to investigate.
- Further analysis on protection/defense in depth is part of ongoing research.
  - Robust control design.
  - Advanced situational awareness technique.
  - Overall framework of combining cyber and physical information to monitor, control, and protect power system.


FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T