NSF Center for GRid-connected Advanced Power Electronic Systems (GRAPES)

Quantifying the Impact of FACTS Devices on Power Grid Reliability with Cybersecurity Considerations

Lingfeng Wang, UW-Milwaukee

Semi-Annual Meeting

May 24, 2016

PI Name: Lingfeng Wang, Associate Professor

Overall Project Budget: $40,000
Motivation of the Proposed Research

- With the growth of electric power demand, there is an urgent need to better utilize the existing transmission assets to achieve greater operational flexibility and enhance the reliability of the power delivery infrastructure.

- The advancements in power electronics and control theory have made Flexible AC transmission system (FACTS) a promising solution to addressing challenging issues in contemporary power grids.

- The normal operation of a FACTS device is dependent on both its physical system and the associated cyber system (considering uncertainties due to physical failures and cyber vulnerabilities).

- As more information and communication technologies are being integrated into the current power grid, cybersecurity is becoming a more realistic issue.

- Malicious cyber attacks may impact the reliability of FACTS itself as well as that of the entire power grid.
Cyber-Physical Structures of Unified Power Flow Controller (UPFC):

Fig. 1 UPFC’s physical structure

Fig. 2 UPFC’s cyber system
An Example: Cyber Vulnerabilities of UPFC

Example Scenarios:

- Intrusion into the control center;
- Man-in-the-middle attack (MITM);
- Replay attack against ACCS LAN;
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attack against the communication switch;
- DoS and DDoS attack against ACCS LAN;
- Malware attack against the ACCS computer or database;
- Intrusion into the ACCS LAN or UPFC LAN;

Fig. 3 Attack tree of UPFC operations
There was very limited existing research associated with the impact of various FACTS devices on power system reliability.

All the existing research was limited to studying the reliability impact due to the FACTS’ physical part, and no cyber-physical interactions, cyber vulnerabilities, and mitigation strategies were considered.

The proposed research relating to FACTS devices features a high industrial relevance and business need considering the promising benefits brought about by the wider and optimal deployment of various FACTS devices in the current and next-generation power grids.

The proposed research will be highly beneficial to enabling the broader deployment of FACTS in power grids in a secure, economical, and dependable manner.

The proposed research is highly relevant to GRAPES IAB in the fields of power electronic and electric power systems.
Project Objectives

- In this project, the cyber architectures of various FACTS devices will be analyzed, and the possible cyber attack scenarios will be examined.
- Based on the interdependency of the physical part and the cyber part for each type of FACTS device, integrated probabilistic cyber-physical reliability models for the major FACTS devices will be built.
- The impact of FACTS on overall power system reliability will then be quantified in a systematic manner, where the effect of cyber attacks against FACTS is accounted for.
- Effective cybersecurity mitigation strategies for FACTS will be proposed and tested in various scenarios. Optimal locations of FACTS devices will be identified for congestion management such that the overall power system reliability can be improved.
- A commercial-grade, comprehensive GUI-based software package will be developed for enabling informed decision-making in FACTS-related cyber-physical assets management for a broad range of users.
In this project, comprehensive probabilistic cyber-physical reliability models for all the major FACTS devices will be developed accounting for their cyber vulnerabilities.

Different FACTS devices feature different cyber-physical structures coupled with different control strategies, but their reliability impacts on power grids could be studied based on a unified framework proposed in this project.

Major Research Tasks:
- Task 1: Cyber structure analysis of FACTS devices;
- Task 2: Cybersecurity analysis of FACTS devices;
- Task 3: Integrated cyber-physical reliability modeling of FACTS devices;
- Task 4: Reliability evaluation of the overall power grid including FACTS devices;
- Task 5: Development and test of mitigation and optimization strategies; and
- Task 6: Software tool development and test.
Expected Deliverables

- At least two graduate students and one undergraduate student will be involved in this project.
- Detailed documentation on all the system models, solution methodologies, and research outcomes.
- A fully functional decision-making software tool with all the desired features. The tool will be commercialized.
- A detailed user manual for explaining how to use this tool.
- Detailed introductions of multiple example applications:
  - Long-term planning (e.g., bulk transmission planning);
  - Short-term operations (e.g., congestion mitigation).
- Publications in top journals and conferences.
Broader Impact of the Project

- The deployment of FACTS devices can bring a myriad of benefits to the electric power system by increasing the transmission capacity without investing new power delivery infrastructure.

- The proposed research will enable the wider deployment of advanced power electronic devices in the contemporary power grid for achieving more secure, economical, reliable, environmentally aware operations of the power grid.
  - For example, the wider use of FACTS devices is beneficial to enabling a higher penetration of renewable energy resources.
  - The software tool will enable informed decision-making concerning FACTS-related cyber-physical assets management for various users.

- We will also perform comprehensive case studies for practical electric power systems provided by the GRAPES IAB.

- The research outcomes will be integrated into educational curricula and outreach activities.