Cyber-Physical Aspects of Energy Systems for the 21st Century:

A Perspective from the NSF ERC FREEDM Project

Frank Mueller

Department of Computer Science, North Carolina State University, Raleigh, NC, mueller@cs.ncsu.edu

---

SUMMARY

Power grids worldwide are undergoing a revolutionary transition as so-called "smart microgrids" that exploit renewable energy sources are emerging. Due to distirbuted generation capabilities of these microgrids, centralized control needs to be replaced by distributed control.

This paper discusses challenges within and beyond the scope of the NSF ERC FREEDM project for a future power grid. The cyber challenge lies in the realization of distributed control of a large number of power devices for future power management that is driven by microgrids with renewable energy generation capabilities. Instead of operator-based monitoring, such microgrids require full automation combining the cyber and physical worlds of distributed utilities.

The combination of distributed control and automation consequently requires novel technology to sustain high reliability, availability and serviceability (RAS) of power as a utility, even in the presence of localized faults and with capabilities to prevent faults from cascading. Distributed control also poses the challenge of software security as a cyber compromise can lead to physical outages or even damaged power devices.

We discuss these challenges in detail and also highlight novel opportunities for selective power delivery during power outages via islanding of smart microgrids.

islanding RAS distributed network overlay hierarchical control via leader election security

1. Introduction

The power grid in the US is one-century old and aging in terms of infrastructure. However, the power industry is slowly undergoing a revolution and modernization through new technologies. Distributed generation (DG) and the microgrid concept are critical means to modernize the electricity system to become a "smart grid". A *microgrid* is a tiny power system with a cluster of loads and DGs based on micro-sources operating together through an energy manager and Flexible AC Distribution System (FACDS) devices (such as DG interfacing inverters, voltage control/support devices, and power flow controllers) within a certain local electric power area. It is one area where the cyber and physical worlds meet.

Reliability and security of such DG and electricity systems have a critical impact on society. Both natural effects/disasters and malicious attacks are great threats to the Nation's power grid. When modernizing the electricity system through microgrids, security and reliability of microgrids must be one of the top priorities.

This paper discusses challenges (1) within and (2) beyond the scope of the NSF ERC FREEDM project for a future power grid as seen by the author.

The vision for the ERC for Future Renewable Electric Energy Delivery and Management (FREEDM) Systems is an "efficient electric power grid integrating highly distributed and scalable alternative generating sources and storage with existing power systems to facilitate a green energy based society, mitigate the growing energy crisis, and reduce the impact of carbon emissions on the environment." The objective of the NSF ERC FREEDM project is to "develop the fundamental and enabling technology to demonstrate the system and, through such development and demonstration, foster a revolution in innovation and technology in the electric power and renewable energy industries, providing long-term energy security and environmental sustainability for the U.S."

As such, key aspects of future power grids are (a) the realization of distributed control, (b) sustained power delivery through built-in fault tolerance, (c) software security to significantly increase the bar to compromise control but also (d) support for limited power delivery via islanding during partial outages and increased efficiency of power transmission.

2. Distributed Control

The combination of distributed control and automation consequently poses a challenge as well as an opportunity to redesign the power grid. One of the main objectives of this redesign must be to address fault tolerance such as to ensure sustained reliability, availability and serviceability (RAS) of power.

Within the FREEDM project, we see a need to specify system management requirements for the distributed grid intelligence within the Intelligent Energy/Fault Management (IEM/IFM) nodes. We are envisioning a fault-tolerant communication layer that, independent of physical networking topologies, provides sustained connectivity during link failures. There is also a need for hierarchical distributed control to ensure RAS of power utility in the presence of IEM/IFM node or device failures. Both of these objectives require distributed algorithmic support at different layers and, when combined, contribute to fault localization and prevention of cascading faults.

3. Cyber Security for Power Grids

A future landscape of microgrids also need to sustain cyber attacks through safe-mode transitions and/or system recovery. By combining distributed power control with systematic software design for reliability and security in the power domain of cyber physical systems, we envision a multi-faceted approach to software design for security and reliability.

We envision a combination of static and dynamic analysis and protection methods to increase reliability and security through a new school of systematic software design for power systems. We have identified a need for techniques and tools to ensure software integrity on intelligent power devices and to control computers in microgrids. We see a particular challenge in monitoring and control of

microgrids to detect and prevent cyber intrusions, and to provide fall-back services in the event for control residing with adversaries.

While origination from power systems, these design methodologies are aimed more widely at arbitrary distributed utilities and even distributed control systems in general (industrial, transportation and beyond).

4. Islanding and Efficiency

Microgrids further provide novel opportunities for sustained power delivery to selected devices during short-haul/long-haul power transmission interruptions through "islanding" (temporary isolation with selective sustained local power). Local generation capabilities (PV, wind) provide the means to supply power to critical devices in homes (e.g., emergency or medical equipment for the elderly). This requires intelligent device control at the end user within homes and within a local microgrid during islanding.

Distributed control and grid intelligence also opens the doors to more fine-grained control of transmission quality, which allows the deployment of sophisticated control systems. Once implemented, automated negotiation of transmission metrics between devices has the potential to drastically increase the transmission efficiency, in part due to better quality of power transmission and in part due to more localized transmission sources to reduce the loss over large distances due to resistance, storage and transformation.

5. Summary

We have identified several challenge areas in future power grids. Distributed control poses novel requirements on fault tolerance and RAS. The networked nature of future grids further requires cyber security and embedded software design to become an integrated discipline with a systematic methodology. Smart grids further provide novel opportunities for islanding and increased power efficiency through intelligent control. While these aspects apply directly to the domain of power, the overall methodology should generalize to distributed control systems per and in particular distributed utilities.