Engineering the Advanced Power Grid: Research Challenges and Tasks*

M. L. Crow[1], C. Gill[2], F. Liu[3], B. McMillin[3], D. Niehaus[4], and D. Tauritz[3]

Abstract — The electric power transmission systems of tomorrow must incorporate advanced hardware and software technologies to increase reliable long-distance power transfer. While new hardware technologies can improve transmission system capabilities, software technologies are also needed to coordinate these hardware technologies safely, securely, and effectively. To prevent system failures, future transmission systems must (1) integrate advanced hardware and software technologies across new and existing facilities, (2) allow revolutionary improvements in power grid utilization, and (3) still offer verifiable assurance of system safety even in the face of faults or malicious attack. To achieve these goals, advances are needed in the security and networking of distributed real-time and embedded systems, particularly in support of system-wide monitoring and distributed computer-based transmission control to detect and react promptly to changing system conditions. These capabilities are needed to protect the grid not only against traditional threats to reliability (such as storms and other natural events), but also against deliberate disruptions.

Index Terms—Power generation and transmission control, Faults and adversarial attack, Distributed real-time computing, FACTS devices

I. INTRODUCTION

Bulk power transmission systems form one of the largest and most complexly inter-connected networks ever built, and their scale makes controlling them extremely difficult. Recent federal deregulation [1] mandates, requiring that generation and transmission of electric power must be owned and operated independently, further increase the difficulty of control. Even now, providers must coordinate power transmission over numerous possible pathways with little or no means of coordinated control. This frequently leads to considerable congestion and overload of major transmission corridors. Heavier power transfers resulting from independent ownership and potentially widespread use of distributed energy generation will make power systems increasingly vulnerable to cascading failures in which a small series of events leads to a major blackout. The *Advanced Power Grid* [2] must include support for decentralized energy generation and transmission controllers, whose local actions can be coordinated for integrated and efficient control of the power grid as a whole.

Decentralized power grid controllers based on power electronics, such as Unified Power Flow Controller (UPFC) style Flexible AC Transmission System (FACTS) [3] devices (shown in Figure 1), consist of: (1) an embedded computer, using (2) a low voltage control system for digital signal processing, and (3) a high voltage power conversion system for switching power rapidly. Each device controls one power line, and multiple devices can interact with each other using a dedicated network to produce distributed real-time coordination effects from actions taken by each device.

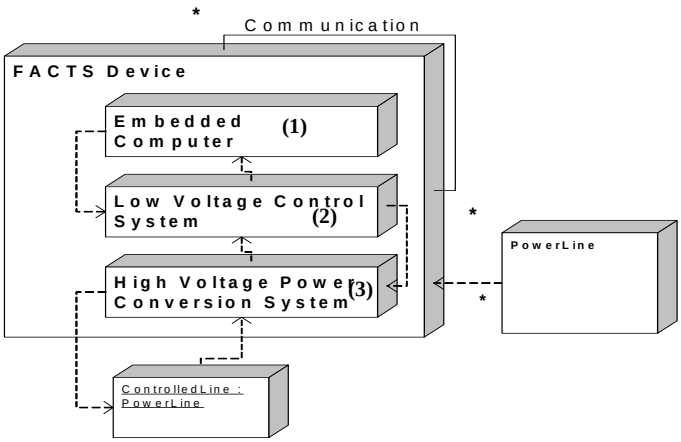

Figure 1. UPFC FACTS Device Operational Schematic

Two compelling needs – for integrated control at multiple time scales, and for decentralized operating paradigms for interacting devices – pose significant research challenges. Power system operating paradigms are typically defined by time-scale: operating (long-term) control (minutes), dynamic control (seconds), and local control (fractions of seconds). FACTS embedded control software employing distributed algorithms has the potential to coordinate devices' actions using a combination of local sensing, exchange of transmission system status information, and local actions. A set of networked FACTS devices can thus form a distributed real-time system called a FACTS Power System, which is consistent with the U.S. Department of Energy's vision of the Advanced Power Grid. However, significant research

1. School of Materials, Energy, and Earth Resources and the Intelligent Systems Center at the University of Missouri-Rolla (e-mail, crow@umr.edu).

2. Department of Computer Science and Engineering, Washington University in St.Louis (e-mail, cdgill@cse.wustl.edu)

3. Department of Computer Science and the Intelligent Systems Center at the University of Missouri-Rolla (e-mail, {ff,tauritzd,fliu}@umr.edu)

4. Department of Electrical Engineering and Computer Science, University of Kansas (e-mail, niehaus@eecs.ku.edu)

*Our prior work described in this paper was supported in part by NSF through MRI award CNS-0420869 (UMR), CAREER award CCF-0448562 (WUSTL), and EHS award CCR-0311599 (KU); by DOE/Sandia (UMR); and by DARPA through PCES contract F33615-03-4111 (WUSTL and KU)

challenges for developing and using FACTS Power Systems still remain, including research problems in three main areas: modeling and semantic integration, real-time control, and fault tolerance and security.

Developing, deploying, and coordinating transmission controllers effectively and robustly requires a close interaction between power electronics engineers and computer scientists so that the control algorithms, supporting system hardware and software infrastructure, and system verification and validation techniques are co-designed to ensure that the system's behavior (1) meets specified constraints even under adverse conditions and then (2) can be optimized with respect to other important concerns such as cost of operation. We now describe three critical categories of research topics that must be investigated: modeling and semantic integration which we consider in Section II, real-time control which we consider in Section III, and fault tolerance and security which we consider in Section IV. Finally, Section V offers concluding remarks on the broader impact beyond power management that addressing the research problems presented here will have.

II. Modeling and Semantic Integration

The high-level structure of the Advanced Power Grid can be modeled using a Context Object Diagram [4] as Figure 2 shows, where objects can represent either single hardware or software elements, or combinations of hardware and/or software elements.

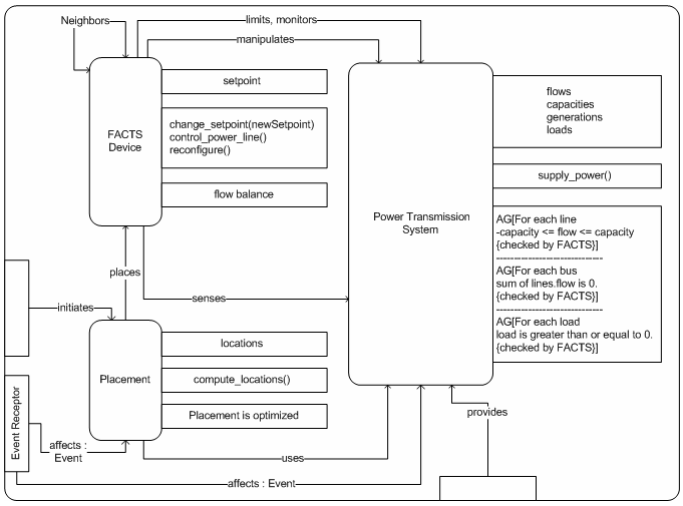

Figure 2. FACTS Power System Object Decomposition

Crucially, modeling hardware or software elements in isolation, without reference to other design domains, ignores important interactions between them and thus risks over-constraining or under-constraining their design. Development of accurate and usable formal models of the physical power-grid and its supporting cyber-infrastructure, together with integration of hardware/software semantics (e.g., through *co-design*), are thus important research challenges to ensure compliance with system constraints, allow optimization, and manage the complexity of the system. Important open research problems in the area of modeling and semantic integration for the Advanced Power Grid include:

- What formal models must be developed to capture the timing and concurrency behavior of all middleware and OS elements of the power grid infrastructure?
- Can domain-specific state space optimizations allow practical verification of real power grid systems?
- What important semantic mismatches currently exist between application requirements, system software behavior, resource management precision, and behavioral information collected about the system?
- Can co-design of applications, system software, resource management, and system monitoring to remove semantic mismatches result in verification and validation that has higher fidelity to the actual system?
- Can co-design of applications, system software, resource management, and system monitoring improve the rigor with which timing and other QoS properties can be specified and enforced?

III. Real-time Control

FACTS devices must act in real-time to respond to contingencies such as component failure, storm damage, or adversarial attack. Examples of approaches to *long term control* include distributed algorithms [5], agent frameworks, and/or optimization problem solutions. A key challenge for any long term control approach is that if its deadlines are not met, the system may not be able to avoid cascading failures.

Dynamic control assumes a particular model of the power transmission system dynamics, and controls its frequency response. If the dynamic control misses its deadline the model in effect changes, which can impact essential control properties. For example, two FACTS devices can compete, in effect causing the controlled system to "ring" as is shown by the controlled frequency response curve in Figure 3. How to achieve effective real-time coordination of both long term and dynamic control across multiple distributed networked FACTS devices is thus an important open research challenge.

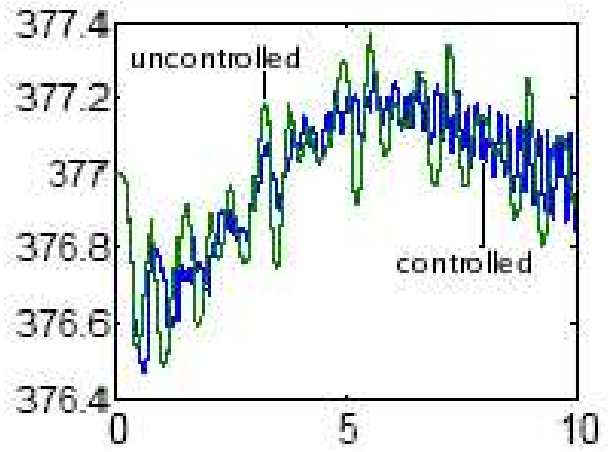

Figure 3. Possible Ringing in FACTS Dynamic Control

In current practice, transmission system control involves a patchwork of controllers that have evolved over time. Recent work in the *GridStat* [6] system provides a consistent picture of a power system's status, but does not address control, which the effective use of FACTS devices in the Advanced Power Grid would enable.

Integrating distributed status information into FACTS control systems effectively requires advances in (1) real-time gathering and delivery of information across the network of FACTS devices, (2) modeling and verification of timing constraints in key FACTS control scenarios, and (3) enforcement of timing properties in supporting system hardware and software [7]. Important open research problems in the area of real-time control for the Advanced Power Grid include:

- What are the effects of different communication and computation delays on both long-term and dynamic control properties?
- Can co-design of control, monitoring/feedback, and actuation infrastructure help to reduce delays and/or their impacts on system properties?
- Can delay sensitivity information be used to improve scheduling and other resource management decisions?
- What formal models must be developed to capture the combined timing behavior of power grid control, monitoring/feedback, and actuation elements in conjunction with the system software elements and resource management policies and mechanisms upon which their operation depends?
- How can model checkers best be extended to support complete sets of abstractions in the application (e.g., controllers), system software (e.g., threads and objects), scheduling (e.g., criticality), and monitoring (e.g., event arrival) semantic domains, both accurately and efficiently?
- Can extending model checkers to support arbitrary policies for scheduling their exploration of model state spaces help to balance verification efficacy and cost?

IV. Fault Tolerance and Security

The safety, liveness, fault tolerance, information security, and robustness of system design and implementation are critical to power grid control [8]. Since the processors in the FACTS devices and the interconnecting communication network may fail, or processes running on them may crash, approaches to ensuring system correctness under a wide range of operating conditions must be developed. In addition to the assurances of timing and information flow discussed in Section III, robust power grid management approaches therefore must also provide security from interference with crucial system computation and communication activities by faults or adversarial actions.

Based on our previous research on scheduling of distributed real-time embedded image processing systems [7], Figure 4 illustrates the limitations of currently available off-the shelf scheduling techniques to address the crucial properties of isolation (that critical computation and communication are protected from interference) and non-bypassability (that policies and mechanisms used to enforce isolation cannot be circumvented). In the application scenario depicted in Figure 4, two critical image processing computations (CS1 and CS2) fully saturate the available cycles on a processor, preventing three non-critical image processing computations (NCS3, NCS4, and NCS5) from progressing as long as the two critical computations have work to do. For the first 25 image frames processed by each of the critical computations, real-time priority scheduling with run-to-completion (SCHED_FIFO) semantics in Linux is sufficient to enforce two essential properties of the system: that the critical computations make equivalent progress and that their progress is strictly preferred over the progress of the non-critical computations.

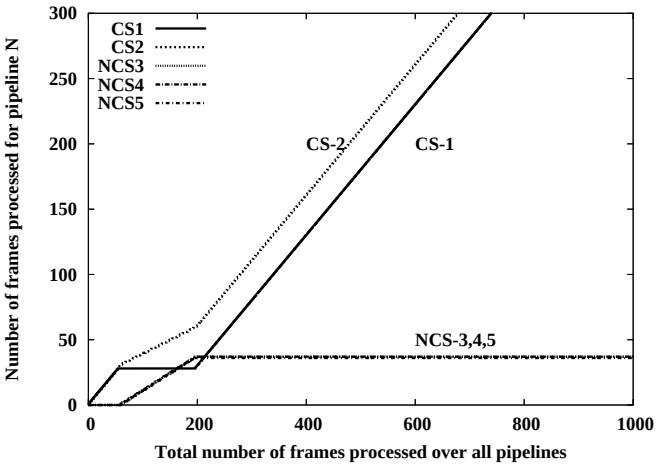

Figure 4. Bypassable Isolation with POSIX-based Scheduling

However, if after its 25th frame critical computation CS1 crashes (e.g., due to a software error such as a null pointer dereference or a division by zero, or due to a malicious kill signal from another process), even if CS1 is restarted, it does not recover fully by catching back up to CS2, even through the non-critical streams only made progress while computation CS1 was out of operation. Thus, although the scheduling semantics provided by many POSIX-based operating systems can be configured to support isolation of critical processing from the effects of non-critical processing, the potential for faults or malicious attacks to bypass the configured scheduling semantics is a more daunting challenge to address.

To provide such security, two main research challenges must be addressed – modeling the interaction pathways through which faults and attacks can interfere with system computation and communication activities, and developing novel techniques for enforcing isolation of system computations and communication from interference, which are non-bypassable and formally verifiable. Important open research problems in the area of fault-tolerance and security for the Advanced Power Grid include:

- Can implicit interaction channels in real-world power grids be identified via empirical/simulation studies?
- Can composition of formal models of individual application, system software, resource management, and monitoring elements reveal additional interaction channels not seen in the empirical/simulation studies?
- Can a common scheduling framework for all OS and middleware level components provide non-bypassable isolation of computation and communication from accidental or adversarial interference?
- Can model checking, proof, and other techniques be used to verify formally the non-bypassability of specific scheduling configurations in real-world power grids at a realistic scale and reasonable cost?
- Can co-design of application, system software, resource management, and monitoring elements remove undesired interaction channels while preserving desired ones according to application-specific design criteria?

V. CONCLUDING REMARKS

This paper has outlined key research issues relevant to the design of an Advanced Power Grid. The system principles and research problems described here, while influenced by the nuances of power grid control in particular, are relevant to a wide variety of other critical infrastructure systems in other engineering domains such as automotive, petrochemical, aerospace, manufacturing, and medical device systems. As diverse engineered systems upon which society depends become more complex, are subjected to increasing performance demands, and are increasingly interconnected to other systems through which faults and attacks can propagate, the need for new research into modeling and semantic integration, real-time control, and fault tolerance and security for those other classes of systems is also evident.

The set of research problems that we have described here motivates a sustained cross-disciplinary investigation that integrates a range of topics from computer science, power engineering, control theory, and other disciplines, within a combined field of study: *power informatics*. Similar cross-disciplinary fields are evident in other engineering domains, with their own nuances and particular research problems. While addressing the open research problems we have described for the Advanced Power Grid will promote better understanding of those engineering domains, additional research will be needed to solve new problems posed by those other cross-disciplinary fields of study.

REFERENCES

[1] R. Green, "Competition in Generation: The economic foundations," *IEEE Proceedings,* vol. 88, no. 2, February 2000.

[2] U.S. Department of Energy, "Grid 2030 A National Vision for Electricity's Second 100 Years." **www.electricity.doe.gov/documents/Electric_Vision_Document.pdf**

[3] IEEE Power Engineering Society FACTS Application Task Force, *FACTS Applications,* IEEE Publication 96TP116-0, 1996.

[4] M. Ryan, S. Markose, F. Liu, B. McMillin, and Y. Cheng, "Structured Object-oriented Co-analysis/Co-design of Hardware/Software for the FACTS Powers System ," *29th Annual International Computers Software and Applications Conference*, Edinburgh, U.K., July 26-28, 2005, pp. 396-402.

[5] A. Armbruster, M. Gosnell, B. McMillin, and M. Crow, "Power Transmission Control Using Distributed Max-Flow," *Proceedings of the 29th International Computers, Software, and Applications Conference,* Edinburgh, Scotland, July, 2005, pp. 256-263.

[6] K. Tomsovic, D. Bakken, V. Venkatasubramanian, and, A. Bose, "Designing the Next Generation of Real-Time Control, Communication and Computations for Large Power Systems," Proc. of the IEEE, Vol. 93, No. 5, May 2005, pp. 965-979.

[7] T. Aswathanarayana, V. Subramonian, D. Niehaus and C. Gill, "Design and Performance of Configurable Endsystem Scheduling Mechanisms", 11th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS '05), San Francisco, CA, March 7-10, 2005.

[8] L. Phillips, M. Baca, et al., "Analysis of Operations and Cyber Security Policies for a Systems of Cooperating and Flexible Alternating Current Transmission System (FACTS) Devices," *SANDIA Report SAND2005-7301*, Sandia National Laboratories, 2005.