# Next Generation Smart Grid: Enabling Optimization, Security, and Trust in Intelligent Energy Distribution and Generation

**Position Paper**

**November 8, 2013**

John A. Orr (PI), Alexander M. Wyglinski, Alexander Emanuel, Lifeng Lai, Krishna Venakatasubramanian
*Worcester Polytechnic Institute, Worcester, Massachusetts*
*{orr, alexw, aemanuel, llai, kven}@wpi.edu*

The basic capabilities and desired features of a *smart grid* electric energy generation, transmission, and distribution infrastructure are well known. Further, the necessary hardware and communications components are available to deploy a system that can implement the fundamental operational functions of the *smart grid*. However, there still exist significant technical challenges that impact the ability of such a system to meet the goals of economy, reliability, security, and sustainability. **In this effort, we propose to devise a framework for next generation smart grid that would enable: (1) real-time customer interactions with the infrastructure, (2) real-time distributed optimization of smart grid operations and resources, (3) secure smart grid operations that immediately identify possible intrusions and attacks, and (4) implementation of trust mechanisms to ensure that all components of the smart grid are legitimately employed within the infrastructure.**

The operation of the electric energy system can be modeled as a collection of time-varying random events, where the generation and delivery of energy can be affected by weather-related events or disturbances to the energy grid, while the demand is based on the instantaneous needs of the customers that fluctuate on a minute-by-minute basis. Further, these *customer needs* are influenced by an exceptionally wide range of factors. For the individual, that need might be his/her perceived comfort level. For a manufacturing plant, the need would be shaped by a product delivery schedule together with the need to minimize production costs. Consequently, two related factors are in play: (1) today's energy distribution infrastructure must be ***agile*** with respect to satisfying customer demand via the generation and delivery of energy; (2) the smart grid must ***interact*** with the customer on a real-time basis to optimize an objective function that includes both the system parameters (such as generation and transmission costs) as well as customer needs and desires.

To enable this agility within the energy distribution infrastructure, it is necessary that the various components that make up the grid possess a substantial degree of automatic decision-making capability. These decisions must be extraordinarily reliable given the criticality of continuous grid operation and the potentially catastrophic consequences of erroneous decisions. In communications networks, erroneous decisions will most likely only result in data delay or loss. In contrast, erroneous decisions in the electric grid can physically destroy major capital equipment with long (years) lead time for replacement. Hence, substantial work is needed in validating and extending previous work in Inference and Decision systems. In order for these algorithms to make appropriate decisions based on prevailing operational conditions, they require real-time access to information regarding the status of the energy distribution infrastructure, customer needs, and other factors. This information can be delivered using wireless access technologies such as cellular telephony (e.g., 3G, 4G LTE/LTE-A), wireless local area networks (e.g., WiFi), or wireless regional area networks (e.g., IEEE 802.22).

Consequently, we envision that for the *next generation smart grid* to be realized, innovative and collaborative work is needed in several key areas, and that the authors of this position paper are well equipped to carry this out. The specific areas are:

- **Distributed, Intelligent Decision-Making in Smart Grids**: The concept of optimizing resources across a network has been extensively studied in fields such as management science and wireless networking. However, a smart grid consisting of agile units capable of deciding on how energy is distributed within a network can also be viewed as a distributed resource optimization problem. Consequently, it is necessary

to devise a framework that would enable *distributed optimization of the smart grid*, where each agile unit would possess a state machine-based decision making capability that configures itself based on the prevailing operating conditions at its own location as well as agile units within the vicinity. Issues such as information latency and incomplete state information from other agile units, using different wireless access technologies for facilitating information exchange, and identifying an optimal range for sharing state information with other agile units, would need to be addressed in order to realize a reliable optimization framework for the next generation smart grid.

- **Smart Grid Security – Intrusion Detection**: When a device depends on information obtained from a remote source in order to support its operation, it then becomes susceptible to attack by a malicious user. There exist numerous examples of these attacks in other applications, such as web servers connected to the Internet, computer-based automotive functions employed in cars, and credit card fraud by leveraging WiFi-based financial transactions. In the case of the next generation smart grid, there exists the danger of a malicious user accessing one or more of the agile, decision-making units and influencing it to perform operations that can potentially be detrimental to the overall functionality of part or all of the energy distribution infrastructure. To combat these attacks, statistical signal processing techniques such as *distributed change-point detection* can be used to identify the presence of an intruder to the smart grid and classify the type of malicious activity being performing, from which actions can be taken by the smart grid to contain the attack and prevent any disruption to the infrastructure.
- **Concept of Trust and Privacy within the Smart Grid Infrastructure**: Although the detection of malicious activities on the next generation smart grid is essential to mitigate any intentional disruption to the delivery of energy to the customer, preventative measures should also be considered. Specifically, devising *trust mechanisms* between the agile units within the next generation smart grid would help minimize intrusions into the network by malicious users by challenging the addition of any new units by requesting specific credentials in order to validate their identify and intent. The objectives of introducing trust within the next generation smart grid include devising protocols that minimize the probability of missed detection of malicious users, minimizing the probability of false alarm when legitimate units request to added to the infrastructure, and devising trust protocols that are difficult to spoof by an informed malicious user with resources available to generate more sophisticated attacks. Furthermore, to prevent data breaches within the next generation smart grid infrastructure, which could reveal customer information to malicious entities, *privacy mechanisms* will also be devised to ensure that customer information remains secure.
- **Effective means of interacting with customers on a real-time basis**: Much of the potential energy savings from the smart grid is dependent on customer behavior change – either via active decision making in real time regarding energy use, agreement to allow external control of loads, or some hybrid combination of these two approaches. Commercial smartphone applications such as joulebug™ represent promising initial steps in this direction for individuals. Overall, it is expected that the opportunities for efficiency gains, as well as the challenges in behavioral change, are both substantial if there exists closed-loop feedback between the needs of the customer and the energy savings provided by the smart grid. One key component to achieving this interaction between the customer and the smart grid is to assess the behavior and characteristics of the customer by performing data analytics on the customer's history of energy needs and consumption. Once this analysis has been performed, it is possible for the smart grid to predictively tailor the delivery of energy resources to a specific customer based on his/her expected energy needs. However, data analytics alone is not sufficient, and "closing the loop" with these interactions between the customer and the smart grid is necessary. One approach for closing the loop is to observe if the customer makes any modifications to the tailored energy delivery, which can then be used to adjust the tailoring process. Consequently, via a combined approach of automated smart grid processes and customer interactions, it is expected that energy will be delivered efficiently to satisfy the needs of the customer.

**Overview of Cyber-Physical Interrelations**

Given how these areas constitute several key components of next generation smart grid, it is important to describe how they are integrated into an energy CPS infrastructure. The individual energy generation, transmission, and

distribution equipment and their associated control mechanisms, such as transformers, turbines, and energy storage facilities, are one class of the two "physical" classes of components of an energy CPS framework since they are mechanical, man-made systems that are responsible for providing energy to the customer. The other "physical" components of this energy CPS framework are the customers themselves, since their human (mechanical) actions and behavior directly impact the smart grid in terms of energy required to be generated and delivered in order to satisfy their needs. As for the "cyber" aspect of this energy CPS framework, the mechanical control mechanisms of each energy generation, transmission, and distribution entity will be interfaced via a communications system with an embedded processor or some other digital processing platform, which will translate commands generated by software into mechanical actions. These programs will control the operations of the energy equipment, and a distributed optimization engine will operate in parallel to the software system in order to provide it with configurations that would enable more efficient utilization of smart grid resources. Another "cyber" aspect is the human-computer interface (HCI) needed between the customer and the smart grid, where the former communicates to the latter his/her desires and requirements and receives feedback on their impact. The commercial smartphone application joulebug™ is an example of this HCI, where the customer (physical) expresses his/her needs to the smart grid via an electronic interface and wireless information infrastructure (cyber) and receives both individual and social feedback with respect to the impact of his/her actions.

**Educational Components**

One critical component for the realization of energy CPS is *enabling multidisciplinary education and training* of the next generation of scientists, engineers, researchers, and technologists who will design, implement, and enhance these cyber physical systems. Fortunately, WPI is well positioned to introduce energy CPS education into the curricula due to its established tradition of excellence in engineering, science, and technology education. In addition to a substantial *graduate research* program being employed in order to conduct the activities specified in this position paper, multidisciplinary educational activities focusing on energy CPS will also be pursued at the senior *undergraduate* level via several *Major Qualifying Projects* (MQPs), which are a quintessential component of the "WPI Plan" that every undergraduate student must complete. The MQP is designed "to provide a capstone experience in the professional discipline, to develop creativity, instill self-confidence and enhance the ability to communicate ideas and synthesize fundamental concepts. The investigators are planning to advise and mentor several MQP teams annually, each of which will consist of three or four undergraduates, resulting in a growing number of graduates conversant with CPS.

**Investigators**

The following investigators are pursuing research in support of this effort, all of whom possess highly relevant qualifications/expertise:

**Dr. John A. Orr**, Professor of Electrical and Computer Engineering. Expertise in smartgrid technology as well as the application of stochastic signal processing and analysis to power systems, and power systems curriculum development.

**Dr. Alexander M. Wyglinski**, Associate Professor of Electrical and Computer Engineering. Expertise in wireless communications, cognitive radio, software defined radio, distributed optimization/reconfiguration/adaptation.

**Dr. Alexander Emanuel**, Professor of Electrical and Computer Engineering. Broad and extensive expertise in all aspects of electric power systems.

**Dr. Lifeng Lai**, Assistant Professor of Electrical and Computer Engineering. Expertise in wireless communications, information theory, and stochastic signal processing, particularly with respect to their security implications.

**Dr. Krishna Venakatasubramanian**, Assistant Professor of Computer Science. Expertise in cyber-physical systems and their security, privacy, and trust. Particular foci include system interoperability, credentialing, and maximization of open-source development.