On Multidisciplinary R&D and Education for the Smart Grid

The Smart Grid is front and central in the Nation's critical energy infrastructures, where the issues of reliability, security and resiliency are of paramount importance. Computer-based control systems, such as the supervisory control and data acquisition (SCADA) systems, perform vital functions across many of these infrastructures by collecting sensor measurements and operational data from the field; then process and display aggregate information, as well as relay control signals to the remote equipment. Securing control systems is a multifaceted problem that calls for a multidimensional approach. Control systems, due to their criticality, tend to lack resilience to cyber attacks or threats. Classic countermeasures of "detect, protect, correct" will not be adequate in time sensitive systems such as the Smart Grid.

Of equal importance is an exemplary instructional model for incorporating the principles of SCADA into advanced undergraduate and graduate courses in embedded systems. The approach must be one of vertical and holistic integration: rather than focusing on one narrow segment of the topic, the model will address SCADA along a range of perspectives, from the "micro" to the "macro." The intent is not merely to give students knowledge of the specifics involved, but to see how, in the real world, it all fits together. This will result in a learning experience that is *system-centric* rather than *device-centric*, one giving the learners a global view, and improving the relevance and impact of what is learned. This education model affords future generation workers in energy systems with the skill set needed for the evolving technology.

An energy cyber-physical system, the Smart Grid necessitates multidisciplinary research to lay the foundation in real-time analytics of reliability, security and resiliency, focusing on at least the following key areas: (1) reliability analysis for phasor and wide area measurement and control system networks with stochastic and fuzzy models, (2) advanced dynamic divide (decouple) and conquer (control) strategies for supporting critical energy infrastructures, and (3) holistic cyber security analytical methodology utilizing data visualization. The emphasis on the real-time constraints in all these areas cannot be underestimated, given the fast dynamics and stringent control requirements, as well as criticality such a system presents under cyber security stresses. Potential research directions to address these 3 areas of concern can be formulated in the following way:

For area (1), develop robust and real-time reliability analytics for wide area measurement and control systems (WAMCS) and regional networks (RN). This involves fuzzy reliability analysis and modeling of RN and WAMCS. We should consider 2 scenarios: protective operation and recovery operation. For each scenario, we would develop methods for computing reliability indices and obtaining the two-state fuzzy Markov model for RN and WAMCS. For protective operation, we should consider the shortest route approach to minimize the likelihood of failures. For recovery operation, we would examine connectivity and fuzzy reliability models at cut-sets, similar to that used for the phasor measurement unit (PMU). PMU networks are modeled as networks of PMUs, taking into account data fusion and filtering issues.

For area (2), develop advanced decoupling and control techniques, using the physical phenomena or knowledge of the system dynamics, and if needed, optimal control. Based on block diagonalization of the Hamiltonian matrices arising in Riccati equations in optimal control, the Hamiltonian approach presents a more efficient way for removing ill-conditioning and obtaining well-conditioned, reduced-order slow and fast controllers; and thus should be given serious consideration. The fixed-point recursive technique

culminating in the Hamiltonian approach can provide a near exact (or highly accurate) slow-fast decomposition suitable for various types of control problems. The wind energy conversion system (WECS) plant control strategies, as applicable to the resiliency of the Smart Grid, seem an plausible fit for this Hamiltonian approach.

For area (3), develop visualization models for the real-time reliability, resiliency and security analytics. The visualization models should be extensible and sufficiently plastic to allow researchers to rapidly evaluate the effectiveness of their models. In parallel, both Big Data analytics and visualizations should be used to examine systems for architectural and systematic vulnerabilities to support continuous monitoring. The visualization system will help with analyzing the two major challenges, identified as dynamics of the Smart Grid and the hierarchical nature of the intermediate aggregators, as well as the controller models in terms of their dynamic behaviors.

Figure 1 illustrates the configuration of a prototype test bed that has all the key components represented as a subnet of the Smart Grid. Figure 2 illustrates an instrumented network showing the relationship between a network's components. The visualization can be modified by drag-and-drop operations to provide rapid feedback on the effect of changes.

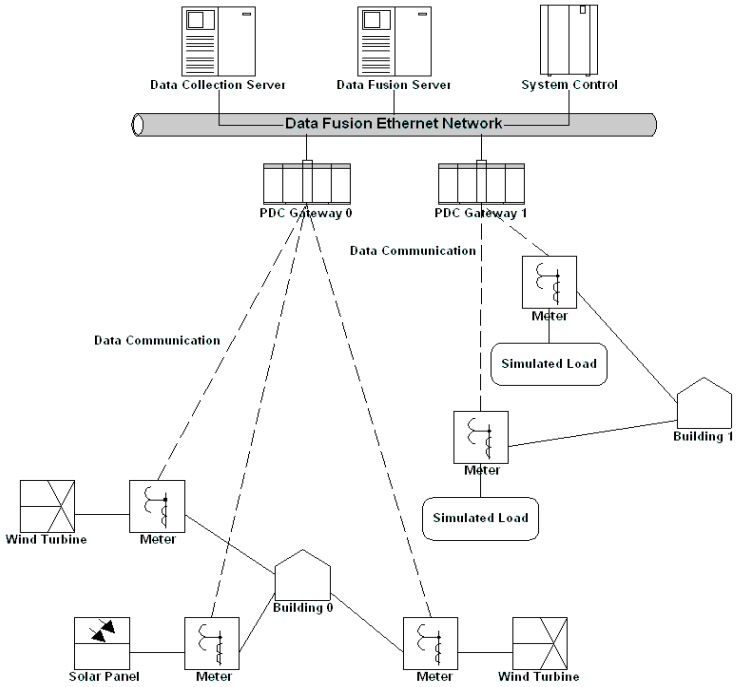

Figure 1. Prototype test bed for real-time analytics

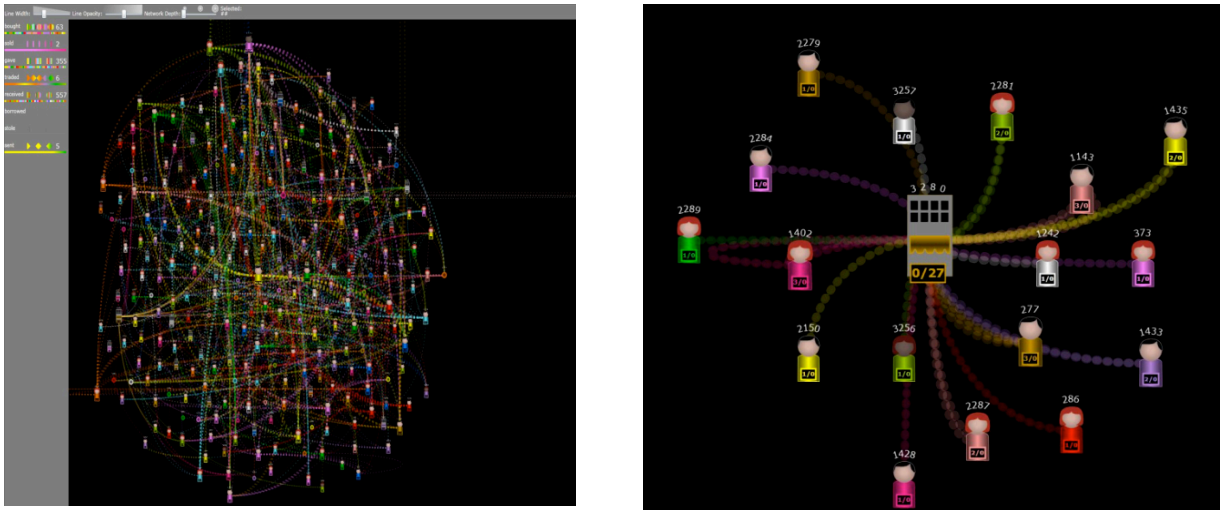

Figure 2. Visualization of an instrumented network showing shortest connecting paths of a model (left) and all related (but not necessarily connected) nodes in a subnet (right)

A typical SCADA system consists of a networked collection of sensors and controllers, a computer, and a human-machine interface that acts between the system and a human operator. SCADA systems rely on Internet-based open standard communication protocols for data and signal transmission, typically on wide-area networks. While such protocols have provided increased connectivity and user acceptance, they have also become much more vulnerable to security attacks. Given these attributes of SCADA and its deep-rooted connection to embedded systems, it is imperative to enhance undergraduate STEM education in embedded systems with a better approach. The students' learning experience should be enhanced by first addressing the breadth, then the depth, of the concepts and applications of embedded systems. The selection of cross-sectional and longitudinal topics must also be relevant to emerging technology needs. Student learning outcomes must be directly measurable. For performance assessment, there should be objectives that specify a direction and amount of change, and a time frame in which the change must occur. There should also be a baseline performance against which the change is measured.

To facilitate breadth, a foundation of general concepts need be built. This includes knowledge and skills universal to all embedded systems and devices. Topics to be covered include classical concepts and techniques such as I/O, memory, interrupts, and peripherals. Students should be expected to acquire sufficient background to perform hardware and software co-design and critical problem-solving skills. To facilitate depth, an upward vertical integration, going from device to subsystem to a complete application (i.e. domain problem) will be employed. For SCADA, topics such as wireless communications, network security and parallel and distributed computing are needed to give students a comprehensive view, and thus an ability to design embedded devices and subsystems integral to a complete application.

In summary, innovative multidisciplinary research and education, a vision of which has been briefly described in this position statement, are essential not only in advancing the technology but also assuring the adequate preparation of future work force in energy cyber-physical systems.