

BLANK PAGE

Table of Contents

1 Introduction 5

2 Executive Summary 6

2.1 Structural Features of Future Energy Systems: Implications for New Modeling and Control Needs 6

2.2 Toward a Formal Framework for Designing Energy Related CPS 6

2.3 High Efficiency Building Technologies and Demand Control 6

2.4 Cyber-Enabled Smart Distribution Systems and Smart Grids 7

2.5 Towards a Trustworthy Future Power Grid 8

2.6 Enabling Technologies 8

2.7 Summary 8

3 Structural Features of Future Energy Systems: Implications on New Modeling and Control 7

3.1 Modeling Challenges in Electrical Energy Systems 9

3.2 Control Challenges in Electrical Energy Systems 11

4 Toward a Formal Framework for Designing Energy-Cyber-Physical Systems (CPS) 13

4.1 Introduction 13

4.2 Future Needs 13

4.3 Barriers 14

4.4 Enabling Technology 14

5 High Efficiency Building Technologies and Demand Control 15

5.1 Introduction 15

5.2 Future Needs 15

5.3 Barriers 16

5.4 Enabling Science-Based Technologies 18

5.5 Research Challenges 18

6 Cyber-Enabled Smart Distribution Systems and Smart Grids 23

6.1 Introduction 23

6.2 Challenges 23

6.2 Enabling Technologies 23

7 Towards a Trustworthy Future Power Grid 25

7.1 Introduction 25

7.2 Barriers 25

7.3 Challenges 27

7.4 Research Strategies 30

7.5 Roadmap 33

7.6 Conclusion 34

7.7 Related Sources 34

8 Appendix 35

8.1 Workshop Working Groups/Writing Teams 35

8.1.1 Structural Features of Future Energy Systems: Implications on New Modeling and Control Needs. 35

8.1.1.1 Participants 35

8.1.1.2 Writing Team 35

8.1.2 Toward a Formal Framework for Designing Energy-CPS 35

8.1.2.1 Participants 35

8.1.2.2 Writing Team 35

8.1.3 High Efficiency Building Technologies and Demand Control 36

8.1.3.1 Participants 36

8.1.3.2 Writing Team 36

8.1.4 Cyber-Enabled Smart Distribution Systems and Smart Grids 36

8.1.4.1 Participants 36

8.1.4.2 Writing Team 36

8.1.5 Towards a Trustworthy Future Power Grid 37

8.1.5.1 Participants 37

8.1.5.2 Writing Team 37

8.2 Organizers 37

8.3 Acronyms and Definitions 38

8.4 Workshop Program 40

8.5 Acknowledgements 46

# Introduction

The report on *Research Recommendations for Future Energy Cyber-Physical Systems:* *A Community* *Report for the 2009 Workshop* is an output of a two-day NSF-funded *Workshop on New Research Directions for Future Energy Cyber-Physical Systems[[1]](#footnote-1) (ECPS)* held June 3-4, 2009 in Baltimore, Maryland. The report focuses national attention on the R&D challenges and opportunities for designing, deploying, and operating the next generation of high-confidence cyber-physical systems (CPS)[[2]](#footnote-2) for energy management. The report also aims to catalyze progress towards a conceptual framework for a more efficient, clean, and reliable cyber-enabled energy services.

Workshop deliberations by academic, government, and industry experts addressed the strategic role that CPS R&D plays in building energy cyber-physical systems that are innovative, resilient, and sustainable. Discussions centered on the strategic role of CPS R&D to:

* Spur innovation and enable safe and secure production of electricity from existing and emerging energy technologies (*e.g.,* coal, hydrogen, clean renewables, nuclear, and other emerging energy resources)
* Develop secure and reliable energy services for key civilian and national security sectors, *(e.g.,* buildings, industry, and transportation)
* Ensure energy efficient grid-tied/islanded micro-grids
* Integrate energy resources, carriers, and consumers to tackle future energy and environmental needs
* Develop standards and protocols to enable performance and innovation in future cyber-physical energy systems

Workshop participants assessed the current state of practice and identified basic technology research, transition, and adoption roadblocks. They provided a vision for transforming today’s physical energy systems to fully cyber-physical systems capable of safe, reliable, and sustainable service to all, with differentiated service beyond today’s basic service.

The Workshop was co-chaired by Professor Marija Ilic of Carnegie Mellon University and

Dr. Clas Jacobson of the United Technologies Corporation. Material in this report was compiled from presentations and discussions, breakout session reports, and white papers. The technical sections were developed by a group of leading university and industry researchers from the areas of power systems, networking, control, and computer science who served on the workshop’s writing teams. Special thanks go to Professor Dagmar Niebur of Drexel University, who worked tirelessly to coordinate this report.

The ECPS Workshop was one of a series of technical activities organized by the National Science Foundation in collaboration with other member agencies of the High Confidence Software and Systems (HCSS) Coordinating Group (CG) of the Networking and Information Technology Research and Development (NITRD) Program.

The ECPS workshop agenda and presentation slides are included in the report appendices. Additional material can be found at the Carnegie Mellon University website at <http://www.ece.cmu.edu/~nsf-cps/>.

# Executive Summary

The following is a summary of the key findings and conclusions of the workshop’s six working group topics:

## 2.1 Structural Features of Future Energy Systems: Implications for New Modeling and Control Needs

*Problem:*

Historically, control of electrical energy systems has been hierarchical and administered by humans. Local controllers must make relevant territorial decisions that are overseen by central controllers who monitor overall system measurements and take actions to minimize the global impact of a fault. Yet, cascading failure events occur at speeds that exceed the ability of human controllers to effectively respond.

*Key Finding:*

Distributed control architectures not only promise reliable operation in the presence of uncertainty, but are also likely to be more resilient when failures occur in the control architecture itself. Distributed control inherently relies on tight coupling between the cyber and physical layers, and therefore, must be designed to cope with degradation of that coupling.

*Conclusion:*

It will be necessary to migrate to a new architecture based on distributed automated control strategies. This proposed new control paradigm would allow highly automated local controllers to make decisions based on local information together with partial system information in order to simultaneously achieve local and global efficiency and reliability goals.

## 2.2 Toward a Formal Framework for Designing Energy Related CPS

*Problem:*

The acceptance of energy-related CPS is a major social challenge since they may require, in many cases, a greater producer-consumer interaction and a generation-utilization coexistence that is uncommon at present..

*Finding:*

A new design methodology for hardware/software development of energy-related CPS is required.

*Conclusion:*

Overcoming this challenge requires, among other things, a multi-scale environment, ranging from small sensing devices to high-end distributed system nodes and low-end communication needs in RF/wireless to low latency/high bandwidth constraints for fiber-optics. The models for this methodology must exist at multiple scales in both discrete and continuous spaces. Some salient aspects that must be addressed include real-time constraints, fault tolerance, islanding, integration of energy, storage, and standardization.

## 2.3 High Efficiency Building Technologies and Demand Control

*Problem:*

The built environment contributes a significant fraction of energy and water use and waste production, greenhouse gas emissions, transportation, and health-care energy service requirements.

*Key Finding:*

With new developments in environmentally friendly technologies (*e.g.,* decentralized generation, storage, Plug-in hybrid electrical vehicles (PHEVs), Grid Friendly Appliances, and the accompanying power electronics, buildings will increasingly assume an active role in energy management services that will rapidly transform their conventional role as a mere consumer of energy. This needs to be guided by system-wide economic and environmental considerations as well as human-dynamical physical constraints and variations.

*Conclusion:*

A vision for High Efficiency Building Technologies and Demand Control is to significantly improve the quality of life of building occupants in particular, and the citizenry at large, through a cyber-physical-system (CPS) based smart-building/neighborhood (SBN) research agenda. Many research challenges exist to develop the requisite science base, technology, and algorithmic frameworks for source/load-optimized energy efficiency. This entails developing technology that builds in adaptive and distributed control and communication technology to support self-sustaining, resilient, and carbon-neutral operations.

Among the challenges are:

* Optimizing the size and environmental sustainability of the SBN footprint
* Achieving efficiency and cost effectiveness of SBN services
* Building resilient infrastructures
* Integrating reliability and security into SBN services

## 2.4 Cyber-Enabled Smart Distribution Systems and Smart Grids

*Problem:*

Cyber-enabled distribution systems will be a two-way network in which consumers are also co-generators transforming the formerly passive to an active network with dynamic topology. Reliable two-way communications are not supported. More importantly, the shift away from primarily centralized control of a relatively constrained set of energy resources to a vastly distributed and highly variable set of resources is incompatible with current architectures.

*Key Finding:*

The emergent network architectures for the future market-based distribution grid will consist of a mix of existing heterogeneous (wired and wireless) communication technologies. Selecting from among the multiple possibilities will involve the interplay between potential network architectures, data-transport needs, and application constraints, and most critically, laying the foundations for interoperability as well as meeting new efficiency and robustness criteria. New temporal, topological, and operational complexities exist.

*Conclusion:*

Significant research challenges exist. These include:

* Managing the multiple time scales and variations
* Managing topology changes
* Large numbers of distributed sensors for local as well as global observation
* New multi-objective optimizations
* New dynamic estimation/control theoretic formulations for the new grid
* Development of new hardware and software infrastructures

## 2.5 Towards a Trustworthy Future Power Grid

*Problem:*

Since the 1970s, the power grid control framework has gradually evolved from a closed monolithic structure to a more open networked environment which brings with it all of the cybersecurity challenges of an Internet Protocol (IP) based system for wide area communication. The increasing dependence upon SCADA[[3]](#footnote-3) communications over the Internet has added to the significance and magnitude of the problem. Moreover, the deployment of smart sensors increases the exposure of the power grid to cyber attacks.

*Key Finding*:

Cybersecurity and trustworthiness of the power grid are pressing issues for today’s electric power grid and in the emerging smart grid.

*Conclusion:*

Realizing the vision of a “trustworthy future power grid” demands that fundamental technical, social, and multidisciplinary cybersecurity challenges be addressed. These require new research and synergistic collaboration between universities, national labs, and industries to create fundamental science and engineering in this area and to transform technologies for deployment in the modern smart grid.

## 2.6 Education and Training

*Problem:*

The gap in power systems education that occurred in the last decades of the 20th century has not been closed fully. The lack of CPS skills and investments in this industry has slowed adoption of available technologies. There are many research, education, and industry tasks that are performed well today. However, they are done either in the cyber domain or in the power-system domain, but not in an integrated CPS domain that is required for the future power grid. The CPS research focus is critically important to understand and analyze the reliance of the power grid on the cyber system (and vice-versa) and to empower the future power grid with resiliency and trustworthy properties through suitable designs and upgrades.

*Key Finding:*

A new generation of researchers and industry professionals who are *inclusively* trained in the core underlying technical areas of CPS and energy must be a high concomitant priority. This requires broadening academic power-systems education and research programs to incorporate principles of CPS. Furthermore, new modes of interaction should be promoted with industry, government labs, and standards-setting organizations.

*Conclusion:*

Significant efforts are needed to create new interdisciplinary educational programs in the integrated energy CPS domain through university-industry partnerships to train highly skilled engineers for the modern workforce**.** This should include developing new courses and experimental facilities or testbeds for the CPS community to simulate and test new concepts. A multiagency education and research agenda is essential to achieve the broader energy and environmental goals of the Nation.

## 2.7 Summary

In summary, highly innovative and visionary research in energy CPS is required to develop trustworthy, efficient, open, and reconfigurable energy services. Further, this research is directly applicable to the improvement of other critical national infrastructures.

# Structural Features of Future Energy Systems: Implications on New Modeling and Control

## 3.1 Modeling Challenges in Electrical Energy Systems

Models of electrical energy systems underpin planning, equipment design, and operations. A key challenge is that the models used for these different purposes are substantially different in nature. For instance, the models used in operational-reliability studies are usually deterministic and describe the evolution of system physical variables (*e.g.,* voltages, current, and machine angles). On the other hand, models used for long-term reliability predictions use probabilistic models (*e.g.,* those based on Markov chains). In addition, and independent of the modeling purpose, there are inherent characteristics to the nature of electrical energy systems, which make their modeling a challenging task. These include

* Largeness
* Nonlinear and hybrid dynamics
* Spatial and temporal multi-scale behavior
* Structural and parametric uncertainty
* Tight interaction between the cyber and the physical layers of the system

### Largeness

According to the National Academy of Engineering (NAE), the U.S. electric grid is the most complex system ever engineered by humankind. Just the bulk power system spans a whole continent encompassing thousands of miles of transmission lines, interconnecting generators, and load centers. Once each of these components is modeled in detail (*e.g.,* a generator can be described by a 9th-order differential-algebraic equation), it becomes apparent that it is relatively difficult to develop analytically-tractable models, and it is necessary to use simulation models. In this regard, even building simulation models with acceptable computational overhead is a challenging proposition. A key research problem is to develop reduced-order models of the system while ensuring a sufficient level of granularity. Validation of these reduced-order models, from the standpoint of data availability, is also a key problem that must be addressed. For instance, while it is possible (and perhaps desirable for system-level studies) to obtain a reduced-order model of a wind farm using a model-order-reduction technique, the validation of such a model should be conducted using real data collected from a wind farm. However, availability of such data is not straightforward. Model development and validation for distribution systems is even more challenging. It is well known that load composition has an important influence on the dynamic behavior of large power systems. However load composition is impossible to determine accurately at any given instant, and continually changes. Quite complex models are required to accurately replicate the impact of loads, but such models are not identifiable using readily available measurements. The modeling of distribution systems will become even more challenging as distributed energy resources, (*e.g.,* photovoltaic modules and fuel-cell stacks, become more prevalent, and with increased participation in load response schemes).

### Nonlinear and Hybrid Behaviors

In general, electrical energy systems should be described by hybrid dynamical models, where the continuous dynamics describes the evolution of electrical and mechanical variables. The discrete events that describe transitions between different continuous dynamics are often governed by:

* Structural changes, (*e.g*., relay actions on transmission lines caused by faults
* Actuators encountering saturation limits
* Switching power-electronics actuators
* Jump-decision variables
* Singularity events (a storm-front causing a wind farm suddenly to shut down)). The control community has undertaken fundamental research on hybrid dynamical systems over the last twenty years. There has been progress defining and analyzing stability notions for hybrid dynamical systems. Most relevant notions developed for non-hybrid dynamical systems have been extended to hybrid dynamical systems, (*e.g*., stability in the sense of Lyapunov, input-to-state stability, controllability, observability, and reachability). However, the application of these techniques to electrical energy system modeling and analysis is still limited. In this regard, it is important to explore whether these techniques can actually be applied to electrical energy system problems, or whether there are fundamental barriers that cannot be overcome.

### Multi-Scale Behavior

A further complication in modeling electrical energy systems concerns their multi-scale, spatio-temporal behavior. In this regard, when assessing electromagnetic transient behavior, it is not necessary to consider machine dynamics and, therefore, a circuit representation, including transient effects in transmission lines due to inductances and capacitances (or perhaps a more elaborated wave model), suffices. On the other hand, when assessing electromechanical transients, machine dynamics play an important role and must be included in the model. Here, the time-scale separation between the electromagnetic and electromechanical phenomena introduces an additional complication to the hybrid dynamical model described above, as the continuous dynamics are no longer represented by ordinary differential equations but by a set of differential-algebraic equations. Such time-scale separation is also manifest in multi-time-horizon physical and market operations in deregulated electricity systems (primary, secondary, and tertiary control; regulation, real-time, and day-ahead markets). Analytical tools for hybrid-differential-algebraic equations are limited. Even in the control community, this topic has only recently gained attention, so fundamental work is still required. While time-scale separation is often appropriate, as described above, more and more situations are arising where fast and slow processes interact. This is particularly the case when power-electronic devices are dominant, such as micro-grids with inverter-based sources. Multi-scale spatial behavior arises due to the size of the system footprint. In a transmission study, it is very common to represent a load center like Los Angeles as an aggregated load, yet the city of Los Angeles spans more than a hundred miles from north to south. These aggregate models cannot capture load-driven phenomena such as fault-induced delayed voltage recovery (FIDVR). This phenomenon is inherently associated with stalling of residential air-conditioners. Each individual air conditioner has negligible effect, but if a certain tipping point is reached, stalling can cascade across large areas, leading to a significant transmission failure event.

### Uncertain Behavior

The sources of uncertainty when developing a model of an electrical energy system arise mainly from:

* Structural changes in the system caused primarily by random outages
* Changes in load and generation over which there is no direct control
* Unmodeled effects due to model simplifications
* Unknown parameters of well-defined components

Uncertainty modeling has always been an integral part of electrical energy system modeling. Mature models have been developed to describe random structural changes and uncertain load behavior. The impact on energy supply of random structural changes caused by outages is the subject of long-term reliability studies conducted during the planning phase. These studies usually involve a stochastic model of the supply and demand for which homogeneous Markov chains are frequently used. However, the adequacy of such a modeling framework for assessing the long-term reliability of next-generation electrical energy systems has not been investigated. Such an investigation is crucial in order to maintain a prescribed reliability level. Furthermore, standard Markov reliability modeling formalisms do not capture the influence of implementing operational policies that might be beneficial for maintaining or increasing system reliability. In this regard, Markov decision modeling formalisms are potentially a powerful tool. They can naturally incorporate the cost of system level failure into operational policy choices. Additionally, with the increased penetration of renewable- and alternative-energy resources on the supply side, there is a need to develop uncertainty models that describe the behavior of these resources and that can be seamlessly incorporated in existing system-level models. Demand-response programs could possibly make load more predictable. Additionally, with increased load diversity, dynamic load modeling becomes an issue. Should the models be derived from first principles, or should they be developed based on observed data? These fundamental questions indicate a need to develop models that capture these new features.

### Tight Interaction Between Cyber and Physical Layers

A typical electrical energy system comprises two distinct layers, including a physical layer, which includes generators, transmission and distribution elements, and loads, and a cyber layer, which includes sensing, communication, control, and computation devices that support the real-time operation of the physical layer. In existing power systems, the primary role of the cyber infrastructure is to provide supervisory control and data acquisition (SCADA) functions. With increased reliance on wide-area communications and control to improve electrical energy system efficiency, responsiveness and resilience, it is becoming increasingly important to include the cyber layer in system-modeling efforts. One might argue that the problem can be tackled if both the cyber and physical layers are separately modeled and understood. However, it is very possible that there might be emergent behaviors that are not captured unless both layers are jointly modeled. An example of this emergent behavior appears in switched systems (an abstraction of hybrid dynamical systems), where it is possible under suitable switching to destabilize a system composed of inherently stable subsystems. Modeling formalisms for cyber and physical systems are vastly different, so deriving models that are consistent across these layers is not straightforward. For example, characteristics such as signal drop-out and variable latency do not naturally fit modeling paradigms for physical systems, yet should be captured as they could significantly impact overall system performance and stability. Other key research challenges in modeling future cyber-physical energy systems lie in integrating appropriate institutional structures and incentives with physical operations for the paradigm of distributed sensing and control discussed below.

## 3.2 Control Challenges in Electrical Energy Systems

Control of electrical energy systems historically has a hierarchical structure consisting of local control that is monitored and administered by centralized control. Local controllers make control decisions based on local information (*e.g*., generators automatically adjust their excitation to regulate terminal voltage) while centralized controllers act across the overall system (*e.g.,* determining the power to be produced by each generator). Overlaying this hierarchical control is an extensive protection scheme that ensures faults are cleared with minimal disruption to system operation. When a fault occurs, protection typically acts locally based on local information (a relay will open a circuit breaker whenever measured quantities satisfy preset trigger conditions). After the fault, local controllers immediately make adjustments to minimize the local impact of the fault (*e.g*., generator controllers seek to stabilize power output, voltage, and speed). The central controller resets the local controller references in order to minimize the global impact of the fault (*e.g*., a fault might cause the frequency of the system to drop).

While the hierarchical structure has proved appropriate for ensuring a high level of reliability, it is not clear that this control structure will remain effective as electrical energy systems continue to incorporate significant renewable resources, plug-in electric vehicles (PeVs), and extensive demand-side management through smart metering devices. This is due to the uncertainty introduced by these technologies (*e.g*., wind is highly variable and difficult to forecast accurately). The goal of local controllers is to locally minimize the impact of uncertainty without regard to the rest of the system. Centralized control, on the other hand, is responsible for minimizing the effect of uncertainty on global objectives, such as maintaining system stability. Global objectives may, however, be inconsistent with those of local controllers. It therefore seems appropriate to revisit the current hierarchical control architecture and perhaps migrate towards new architectures that are based on distributed control strategies. This proposed control paradigm would allow local controllers to make decisions based on local information together with partial system information in order to achieve simultaneously local and global efficiency and reliability goals. These distributed control architectures not only promise reliable operation in the presence of uncertainty but are also likely to be more resilient to failures in elements of the control architecture itself. Distributed control inherently relies on tight coupling between the cyber and physical layers and therefore must be designed to cope with degradation of that coupling.

Technologies that will enable distributed control architectures will include

1. Adaptive relaying based on system local and global information, which will enable real-time reconfiguration of remedial action schemes,
2. High sampling-rate Phasor measurement units (PMUs), which will enable dynamic state-estimation for short-term prediction,
3. Flexible AC Transmission Systems (FACTS) devices, which will enable fast control of active and reactive power flow. Additionally, as the penetration of PeVs and renewable resources become more pronounced, the role of power electronics will become significant, providing asynchronous operation as opposed to the current operational paradigm of keeping the whole system’s frequency tightly synchronized.

New types of loads such as PeVs and “smart” appliances, are capable of altering their electrical demand in response to external control signals. That demand responsiveness could be exploited for power-system control functions such as smoothing fluctuations in wind generation. To do so however, will require a control structure that is capable of coordinating the responses of very large numbers of devices. Clearly centralized control is not feasible. Various combinations of hierarchical and distributed control have been proposed, but further research is required to fully explore (and exploit) the opportunities offered by non-disruptive forms of load control.

# Toward a Formal Framework for Designing Energy-Cyber-Physical Systems (CPS)

## 4.1 Introduction

It has been widely recognized that energy systems encompass a broad spectrum, including generation, distribution, and utilization. The need for effective CPS energy systems requires not only a smart grid that can integrate distributed power sources and sinks but also power generation and optimal power utilization that is environmentally friendly.

The increasing demands for new kinds of power generation require the development of novel control system architectures that exploit high-performance control-oriented process models, the optimization of real-time overall power plant efficiency, and consideration of environmental constraints.

## 4.2 Future Needs

Future cyber-physical power generation system requirements might include:

* Sensing and control solutions for real-time optimal integration of many subsystems
* Hardware and software solutions to support heavy computational requirements of complex real-time calculations
* Software methods for state detection and logical decision making based on a high volume of sensor information, to provide intelligent transitions between different nominal control regimes in response to changing time-dependent plant conditions and priorities
* Software methods for prediction and detection of faults followed by state-dependent logical decision making to facilitate timely transition to fault-response control methods
* Analytical and software development methods to provide guarantees of software performance with the ultimate goal of guaranteeing power plant performance, safety, and device protection.

CPS will be needed for large-scale renewable energy sources (*e.g.,* wind and solar) as well as for future development of nuclear fusion and can contribute to the more efficient and reliable integration of traditional sources such as nuclear fission and fossil-fuel plants. The growth of renewable-based power generation will be tied to the development of control schemes that can cope with the distributed and random nature of these sources of energy in an economically efficient manner. All these large-scale power generation systems require solutions that guarantee performance, reliability, safety, and optimal subsystem integration. It is envisioned that future power generation systems, including fossil systems, intrinsically safe nuclear systems, and economically attractive renewable systems, may need a level of computation, communications, sensing, controls and system integration not found in existing energy system.

Energy utilization systems are integral parts of the energy equation. Consider the energy consumption in building structures, for instance. According to the United States Department of Energy (DOE), today's buildings consume more energy than any other sector of the U.S. economy (over 70% of electricity and over 50% of natural gas), including transportation and industry. Consequently, the design, optimization, and control of energy-efficient buildings can have a tremendous impact on energy savings and greenhouse-gas-emission reduction, tackling one of the most critical challenges facing society today: climate change and global warming. Buildings are complex, multi-scale in time and space, multi-physics, and uncertain dynamic systems with wide varieties of disturbances, making their optimal control challenging. Most heating, ventilation, and air-conditioning (HVAC) systems, as well as lighting systems, employed today do not make use of state of the art IT technologies. A combination of advanced distributed control schemes, smart sensing, communication, and modern information technology can lead to an improvement in both indoor-climate comfort and energy efficiency. Advanced controls promise unprecedented levels of sensing and automated response to changes in the internal and external environment. The delivery of continuous, up-to-date information on building system and component performance will also enable more cost-effective equipment servicing and optimized building operation. Building owners and operators will see lower maintenance and operating costs, and building occupants will enjoy greater levels of comfort. CPS issues identified to support integration of CPS into the energy domain include:

* Distributed and autonomous control for self-managing solutions
* Multi-level networking for self-configuring solutions
* Reliability and availability for self-healing solutions
* Security (cyber+physical) for self-protecting solutions
* Efficiency for self-optimizing solutions
* Scalability for self-dimensioning solutions

The acceptance of these energy-CPS issues is a major social challenge, since they may require, in many cases, a greater producer-consumer interaction and a generation-utilization coexistence than is presently common. The future roles of producers and consumers, both large and small, in the public/private space are primary concerns.

## 4.3 Barriers

Barriers include tool support for cross-domain models that take into account both the hardware and software. The development of a multi-scale environment is required, ranging from small sensory devices to high-end distributed system nodes and low-end communication needs in RF/wireless to low latency/high bandwidth constraints for fiber-optics. A new design methodology for hardware/software development of energy-CPS systems is required. The models for this methodology must exist at multiple scales in both discrete and continuous spaces. Some salient aspects of these barriers include real-time constraints, fault tolerance, islanding, integration of energy storage, and standardization.

It was observed that the current American Recovery and Reinvestment Act (ARRA, aka stimulus) funding can only begin to overcome these barriers.

## 4.4 Enabling Technology

Some existing enabling technologies include simulation, advanced and intelligent control systems, distributed systems/algorithms, networked control systems, network fault tolerance, and hierarchical control. Static and dynamic analysis tools, run-time monitoring, and formal methods can ensure correctness and fault tolerance of the system.

The roadmap to success includes

* Long-term multi-agency and industry funding
* Coordination and involvement of government, industry (*e.g.,* generators, utilities, manufacturers), and academia
* Education through cross-over degrees and K-12 plus college to inspire and train new Energy-CPS engineers and scientists
* Outreach and information dissemination to promote social acceptance of new energy-CPS ideas.

The group advocates both top-down and bottom-up designs for formal frameworks. In fact, a hybrid of both may be needed.

# High-Efficiency Building Technologies and Demand Control

## 5.1 Introduction

The built environment is responsible for a significant fraction of energy and water use and waste production, and greenhouse gas emissions. Moreover, with new developments in environmentally friendly technologies (*e.g*., decentralized generation, storage, Plug-in hybrid electrical vehicles (PHEVs), Grid Friendly Appliances, and the accompanying power electronics), buildings will increasingly assume an active role in the production of energy services that will rapidly transform their conventional role as solely a consumer. Our vision for High-Efficiency Building Technologies and Demand Control is to develop the requisite science base, technology, and algorithmic tools that will enable building occupants to improve their quality of life significantly through the creation of a cyber-physical-system (CPS) based smart-building/neighborhood (SBN).

The CPS SBN can be realized with optimal control of building occupant consumption and provision of services. Optimality should be measured against:

* Size and environmental sustainability of SBN footprint, (ii) the efficiency and cost effectiveness of SBN services and resilient infrastructures, and (iii) the reliability and security of SBN services. Realization of our vision is predicated upon the following indicative list of capabilities:
* Ability to measure and to control energy/water/sewer consumption by time and by specific use, and to make data available to building occupants
* Ability to predict, model, plan, and control in real time usage and production and to make sure that they are:
  + Consistent with occupant preferences
  + Do not violate physical system requirements, capacities, integrity
  + Do not endanger utility side
* Ability to ensure efficiency and reliability of building energy/water and other services, even when the building has to disconnect from the infrastructure.
* Ability to interact with the utility side of the meter infrastructure, either through participation in existing markets or through cost and congestion information being made available to the building occupants and their decision-support tools
* Ability to deploy an information-gathering portal that connects a physical event-scheduling layer with a decision support intelligent computation and optimization layer. The physical event-scheduling layer will guarantee that the demand-response actions recommended by the intelligent layer are feasible and inform the intelligent layer about allowable action sets
* Implementation of “human in the loop” practices and the development of social networks in which building occupants are informed about the consequences of their actions, are allowed to express their preferences, and are able to optimize their demand response against building capabilities, and utility-side costs and congestion
* Recognition of quality attributes that differentiate services by environmental impact, reliability/volatility, and scarcity/congestion by time and location

The remaining subsections identify the current state of the art’s inadequacies relative to achieving the above articulated vision. Also addressed are the technical and institutional barriers, existing enabling technologies, and our assessment of research challenges.

## 5.2 Future Needs

Our vision regarding High-Efficiency Building Technologies and Demand Control R&D can be summarized as follows: the community will develop source-load energy-efficiency optimized, self-sustaining/resilient, and (possibly) carbon-neutral and recycle-material-based building technology with built-in adaptive and distributed control-communication technology guided by system-wide economic and environmental considerations as well as human-dynamical physical constraints and variations.

We anticipate the following advances over today’s scientific and technological state of the art:

* Fundamental science base advancements in network systems; including:
  + Management and control of wireless sensor networks
  + Optimization of complex interconnected stochastic systems characterized by different time-scope scales and hybrid dynamics
  + Coordination of distributed and centralized decision making
  + Static and dynamic equilibrium of multi-agent games associated with utility functions that arise in the context of building occupant decision makers and load aggregators that participate in utility-side-of-the-meter markets.
* Cost effective and scalable technologies, including:
  + Distributed generation (*e.g.,* roof top Photo Voltaic (PV) and wind)
  + Distributed storage (*e.g.,* flywheel, and battery based storage)
  + Grid friendly appliances and new building loads (*e.g.,* PHEVs, smart appliances, dimmable LED lighting)
  + Flexible power electronics accompanying distributed resources that are able to provide distributed voltage support and power factor correction
  + Advanced sensing-metering-control micro grids appropriate for new buildings and for retrofitting existing ones, such as tools capable of capturing building-wide interconnected physical processes *(e.g.* air-flow models, heat-transfer processes, acoustic phenomena, people flows, and sewage).
* Open-access, open-architecture, and bottom-up communication innovations and standards that do not impede technological development while providing developers and users open access to the smart distribution grid. These may include intelligent sensor, communication, and control networks, such as CPS event schedulers that mediate physical building and occupant state requirements and constraints and higher-level abstractions that implement software-based decision support.
* Enabling marginal costs, including external costs, congestion and stability requirements – reflective transactions through:
  + New efficient public policy and regulation
  + Creation of new markets that extend today’s by-and-large efficient wholesale power markets to retail/distribution markets and broaden market participation to the load side
  + Contract design and organizational management that optimize risk, cost, and benefit sharing among participating agents that include building occupants and service providers.

## 5.3 Barriers

The lack of a systems approach is responsible for deficiencies in current science and technology relevant to energy-CPS and for the barriers to adoption discussed below.

### 5.3.1 Technology Science

Building-scale renewable/alternative-energy generation and cogeneration, storage, and other environmentally friendly resources (*e.g*. solar, fuel cells, wind, biomass, battery-storage, water storage) are associated with varying gaps in market-ready cost effectiveness, power scalability, and durability. Although these gaps are in many cases decreasing rapidly (*e.g.*, roof-top PV, PHEV), they persist in other situations (*e.g*., fuel cells). This makes practical consideration of potential value-added opportunities and positive synergies (discussed later in the research-challenges section) difficult. In addition, environmentally sustainable technologies that are already cost effective, ,such as insulation and passive energy and water conservation, are not being adopted in substantial ways, because they are impeded by similar market failure and behavioral barriers (discussed below).

An important barrier to the requisite systems approach is the lack of relevant information collection and its dissemination. For example, consumers connected to the low-voltage distribution network do not have access to real-time information regarding their building/neighborhood. They also have no access to either wholesale market information (location and time-specific energy and reserve clearing prices) or local distribution network information (time- and location-specific marginal line losses, reactive power requirements, feeder/transformer congestion). Moreover, the ability to disseminate information in a usable and palatable form to important stakeholders, in particular building occupants/consumers and their decision support tools, is also missing or inadequate. Whereas decentralized (wireless sensor networks of sensors and controllers) as well as centralized building automation and control systems (BACnet) are affordable and in many cases installed as part of existing HVAC systems, their use is currently understood in isolation (*i.e*., without cyberspace integration). In short, sensing/actuation capability is not at the level of complexity and efficacy required properly to match the physical domain and to support building occupants’ awareness of the consequences of their actions or to support building-occupant decision support tools.

In the same vein we note that embedded and computational sensing units do exist but not at the scale of PMUs in individual rooms within a building, while heterogeneous communication infrastructure exists with probably non-uniform and non-open-access protocols.

Finally, some basic standards (*e.g.* IEEE 1547, ANSI) and codes exist, but standardization issues are still a barrier. Security issues, which include sensitive information, private consumer information, and the safety of working on repairs and maintenance on the utility side of the meter when distributed generation is active on the customer side of the meter, are still posing considerable barriers to the realization of this vision.

### 5.3.2 Institutional-Behavioral

As the smart grid and associated CPS investments progress, realization of the promise they bring will depend significantly on the rate at which institutional, regulatory, and behavioral constraints are addressed. Today’s rate structures which characterize contracts between providers and consumers of energy services, are antiquated, as they neither reflect cost and reliability/quality of services nor provide incentives for efficient allocation and use of resources. It is therefore important for policy and regulatory reform to adapt accordingly and remove associated barriers. Better markets that can utilize the information made available by the smart grid must be developed. Better contracts and rates must be established to allow efficient allocation of costs and benefits among a multitude of participants including consumers, distribution utilities, energy-service companies, load aggregators who facilitate market participation and demand response, investors who specialize in distributed resources placed on individual consumer promises, and financing entities that insure risk, to name a few.

Finally, today’s consumer attitudes are also reflective of a tradition in energy and other network transported services that were associated with averaging and socialization of costs due to expensive measurement and communication. The first steps towards changing these attitudes are to provide consumers with information about the consequences of their actions and, the ability to act on this information through a simple articulation of their decision-making preferences with appropriate tools. An efficient way to make progress is to employ cyber technology to create *social networks* of consumers who compete ethically and materially to achieve a higher quality of life. Developing technology that strives to put the *“human in the loop”* will significantly aid in the removal of behavioral barriers.

## 5.4 Enabling Science-Based Technologies

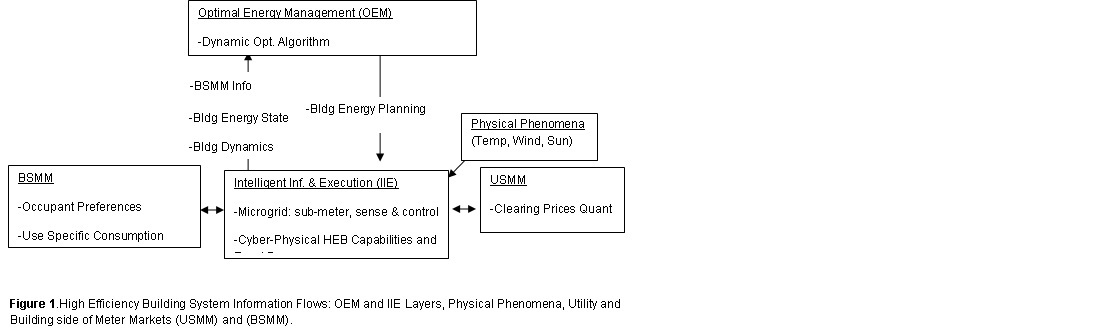
This section describes an indicative, though not exhaustive, list of existing science base achievements and technologies that provide a solid foundation for the critical research issues that follow:

* Communication, computation, estimation, and sensing networks - wired or wireless - have already reached an impressive state. They can provide a formidable launching pad for reaching our vision. For example, a smart micro grid for demand management in a building or a neighborhood can be built on existing
  + BACnets that usually accompany HVAC facilities in new large buildings. A BACnet consists of fully sub-metered and centrally controlled (switched on and off) circuits that may or may not be associated with the HVAC.
  + Wireless sensor networks that may monitor and control space conditioning thermostats (*e.g*., Millenial Net product)
  + WiFi and ZigBee wireless communication technology
* Systems and control theory, stochastic system modeling for analysis and design, discrete event and hybrid systems, and information technology
* Useful hardware developed in the past is being incorporated in smart appliances. For example, the Frequency adaptive Power Energy Regulator (FAPER) developed at the MIT energy laboratory in the 1980s is finding its way in Commercial- off-the-shelf (COTS) products (GridPoint) and grid friendly appliances (GE).
* Power electronics that accompany roof top PV, Wind, PHEV etc., are making their presence in the distribution network. In principle, power electronics can provide distributed reactive power (VAR) compensation.
* Distributed resources: PV, wind, storage (batteries, flywheels), PHEV
* LED based smart lights, communication and modulation, dimmable…
* Insulation and other passive energy conservation and efficiency design of new buildings
* Energy-efficiency retrofitting of existing buildings
* Advanced smart meters
* Physical layers and event schedulers
* Building models of HVAC
* HVAC monitoring sensors and control for efficient maintenance and operation of HVAC hardware as well as of building heat and mass transport
* Optimal power flow on transmission and particularly distribution grids. Software that is capable of modeling and analyzing the built environment surrounding a building or neighborhood so as to estimate retail/distribution costs and congestion and simulate its interaction with the utility side of the meter.
* Building energy-management software

## 5.5 Research Challenges

We believe that the synthesis of technology, degrees of freedom in specific building energy uses, occupant preferences, physical phenomena, marginal costs and congestion in the surrounding transmission, generation and distribution system and other infrastructures (*e.g*., water) with which a building interacts will provide the foundation in achieving our vision for High Efficiency Building (HEB) Technologies and Demand Control.

In addition, individual key technologies involving innovative materials, building technology, distributed resources as previously defined, and building blocks of the communication, load management, occupant input, event scheduler and optimal system interaction decision-support capabilities constitute significant research challenges. Finally, regulatory, institutional, and market-design considerations are critical research issues. In particular, since demand response will be associated with consumers connected to the distribution grid, development of a retail market responsible for efficient allocation of distribution-line losses, congested hardware capacity, and distribution-level voltage support and reactive power provision is crucial. Design of the retail-market rules and management of its operation in real time would be the object of such research.

[](https://wiki.ece.cmu.edu/nsf-cps/index.php/Image:Figure1Caramanis.jpg)

Research challenges described below are grouped into the following five categories:

* System Theory/Integration for Globally Optimal Energy Management (OEM)
* Secure and Robust Interface of Optimal Energy Management (OEM) layer with an Intelligent Information and Execution (IIE) layer capable of HEB Spatio-temporal State Observation and Event Scheduling
* HEB Technology (micro-grid, information communication, building automaton, building materials, sensing, distributed generation-storage-resources, Grid Friendly Appliances, …)
* Specific Load Characteristics and Estimation of Associated Demand Response Potential
* Distribution/Retail Market Design and Market Clearing Algorithms.

### 5.5.1 System Theory/Integration for Globally Optimal Energy Management (OEM)

A major challenge of OEM is to develop and integrate a heterogeneous set of new algorithms for the automated HEB interaction with the energy markets including reserve offers and to manage building resource and occupant preferences. These algorithms should include the following:

* Modeling of degrees of freedom in the HEB’s spatio-temporal consumption and production of real and reactive power, and in the provision of demand-control services that can be used in lieu of primary (30 seconds), secondary (5 minutes), tertiary (10 minutes) and longer reserves. The above degrees of freedom must reflect HEB equipment capabilities and building thermal properties, weather, and HEB occupant preferences. In essence, the degrees of freedom represent the set of allowable control/actions.
* Modeling of automatic demand control of smart Grid Friendly Appliances (GFAs) by FAPER/VAPER (voltage adaptive power energy regulators) -type controllers incorporating occupant preferences/authorization.
* Aggregation of degrees of freedom and impact of distributed automatically responding GFAs by physical-layer middleware so that they become available to a higher abstraction optimization layer.
* Management and control of the degrees of freedom by the optimization layer so that, in conjunction with the automatic GFA demand control, interaction with the spatio-temporal dynamics of Utility-Side-of-the-Meter markets is optimized. As mentioned above, optimal management and control of degrees of freedom should address real and reactive power consumption (*e.g*. inductive motors) and production (distributed power electronics) and stand-by reserves with different dynamics as characterized by ramp rates, capacity, and duration/storage.

### 5.5.2 Secure and Robust Interface of OEM layer with IIE Layer Capable of HEB Spatio-Temporal State Observation and Event Scheduling

The optimal management of the degrees of freedom described above will result in energy-management policies that are dynamically adaptive to the availability of local resources and external market conditions. These policies or action recommendations must be translated to specific physical actions and events (switches) scheduled so as to maintain the integrity of HEB equipment, observe building and occupant safety, and respect occupant preferences. An IIE layer must be designed so that it is capable of load-breakdown estimation and its correlation with the building usage state, while providing a modeling abstraction that manages a heterogeneous network of sensors and actuators. The IIE must be able to interface with and monitor the HEB micro-grid, energy resources, building occupant location and preferences, meteorological forecasts and measurements, and market information. Challenges in the design and implementation of the IIE layer include the incorporation of the ability to:

* Provide the OEM layer with the requisite information described above.
* Receive information from the OEM layer on the optimal operation of building systems and devices (HVAC, storage devices, appliances, etc.).
* Perform the requisite actuation functions to modulate use-specific consumption in a manner that is responsive to Independent System Operator (Wholesale Market Operator/control center) regulation service reserve related commands associated with the HEB regulation service obligations. In doing so the IIE must first enforce occupant preferences. These preferences are broadly construed and include safety related preferences such as never turning off ventilation in labs with active fume hoods and not turning off lights in an occupied room.
* Observe real-time reactive-power needs at the HEB-Utility interface and manage HEB power electronics, (*e.g*., for example roof top PV inverters, electric-vehicle battery chargers, efficient light electronic ballasts, flywheel storage electronics (to supply reactive power as needed by the retail/distribution market). This can be done through centralized coordinated commands or through autonomous distributed electronic sensors such as VAPERs. The appropriate mix of autonomous/decentralized versus coordinated management of power electronics is a research issue that depends on effectiveness of distribution network state identification at the distribution control center.
* Observe real-time frequency deviations (*e.g*., excursions beyond the acceptable 60±0.020Hz range) and manage HEB automated frequency-response reserves by instantaneously powering down thermostat operated resistive loads in order to provide automatic frequency control to the wholesale market. This will be done primarily through autonomous distributed electronic sensors such as frequency adaptive power energy regulators (FAPERs), that decrease or increase the consumption of appropriate devices such as thermostat-operated devices. Occupants may express their preference for higher participation in FAPER activity by authorizing a wider temperature band during such frequency excursions.
* Collect statistics on the building’s performance *vis-a-vis* OEM regulation service reserve obligations. The OEM layer will rely on this information to make sure that its regulation service reserve sales are not too ambitious, resulting in frequent non-performance and risking loss of the building’s license to participate in the reserve market.
* Collect statistics on VAPER and FAPER performance in order to receive appropriate compensation from the retail and whole sale markets respectively.
* Support requisite physical-domain representation in terms of interconnected, scalable spatio-temporal networks.
* Provide multi-scale network forecasting encompassing environmental, human-dynamical, market, and demand-side dynamical aspects.

### 5.5.3 HEB Technology

HEB technology includes the HEB micro-grid, information communication, building automaton, building materials, sensing, distributed generation-storage-resources, grid-friendly appliances, and power electronics accompanying distribution resources. To promote futuristic growth it should:

* Develop cost-effective, energy-efficient, and power-scalable, and durable renewable/alternative energy sources
* Include solid-state (LED) smart lighting technology
* Include wireless communication technologies
* Improve design of sensor/actuation/estimation/control cyber-domain tools
* Develop source-universal, plug-and-play, power-scalable, and modular power-electronic-converter systems that are simultaneously cost effective, efficient, and reliable/robust
* Develop more efficient and cost effective small-scale distributed storage technologies
* Develop cost-effective higher energy-to-mass-ratio battery technology capable of larger number of charge discharge cycles, incorporate in electric vehicles and enable V2G functionality
* Develop a smart interface between PHEV/EV and HEB IIE layer
* Bottom-up, plug-and-play, adaptive, and distributed control (supported with distributed sensing and estimation) over information network under capacity constraints

### 5.5.4 Specific Load Characteristics and Associated Demand Response Potential

OEM at the HEB level is important and so is the existence of cost reflective markets. However, the characteristics of various loads require investigation since the associated degrees of freedom provide the allowable set of OEM actions. Moreover, demand response should be broadly construed and classified in terms of its equivalency to capacity reserves with different dynamic capabilities. Indeed, just as generating units provide primary, secondary, and tertiary reserves, appropriate demand control should be able to provide equivalent services. An abundant supply of reserve services is crucial particularly for the economically sustainable adoption of large quantities of cost-effective but intermittent wind generation.

It is not surprising that a Pacific Northwest National Laboratory study of demand response and utility needs in the Olympic peninsula [14] has concluded that utilities value demand response on the basis of their ramping, duration/storage, and frequency characteristics that are available when HEB occupants authorize the control of load-specific degrees of freedom. Different loads such as PHEV battery charging, HVAC, electric water heating, electric drying, and different resources such as distributed storage, can provide different quantities of primary, secondary, and tertiary reserve equivalencies. Moreover, autonomously responding grid-friendly appliances with FAPER/VAPER type controllers may be designed to provide services that are equivalent to primary and secondary reserves [Ref Kirschen].

Understanding and influencing potential demand-response dynamical behavior is a key research challenge in HEB demand control. The value of such reserve services to the wholesale power market is related to the opportunity cost of providing them on the generation side. In addition to wholesale market opportunity costs, local/retail/distribution costs and congestion (*e.g*., feeder line/transformer overloading), should be reflected in the pricing of demand-control reserves.

### 5.5.5 Distribution/Retail Market Design and Market Clearing Algorithms

Since HEB loads are connected to the distribution grid, participation of HEB demand control in the wholesale market must necessarily pass through a non-existent but probably “soon-to-emerge” retail market.

Designing the rules of this “soon-to-emerge” retail market will depend on a good understanding of (i) the key cost components (*e.g.,* spatio-temporally varying marginal line losses, voltage support and other quality issues, and finally equipment (feeders, transformers) capacity constraints, and (ii) the requisite distribution grid state information). Detailed modeling of real and reactive power flows over distribution lines and transformers will be a crucial tool in understanding (i) and (ii) above.

Given the desired distribution grid state information, the proper deployment of the sensor and communication equipment must be optimized, taking into account costs of deployment and maintenance and the nature of the information required.

Besides the numerous technical issues discussed above, policy and regulatory considerations may prove crucial. Distribution/retail market design must also address electricity tariff structure re-design.

# 

# Cyber-Enabled Smart Distribution Systems and Smart Grids

## 6.1 Introduction

The new cyber-enabled distribution system will be a two-way network connecting “consumers” to a diversified set of energy resources inclusive of new distributed generators (DGs), whereby one-time consumers are also co-generators, transforming the hitherto passive to an active network. Achieving this will require new (two-way) communication that interconnects smart nodes via a *smart* grid and transports necessary sensory data for achieving important network-wide objectives (stability, efficiency, reliability). In effect, the ‘*smart*’ grid will critically rely on embedding new hardware and intelligence at various points in the emergent distribution network to support the above broad goals while empowering individual consumers via a combination of appropriate network architectures, operational strategies, and management policies.

## 6.2 Challenges

Significant changes to the distribution grid are anticipated both in terms of topology as well as operational intelligence in response to inclusion of DGs (*e.g*., wind and solar) that are notoriously intermittent. Operating a network reliably in such conditions will require frequent (dynamic) estimation of network states in support of control actions (voltage and frequency stability). Further, the distribution grid will change from the legacy radial (tree-like) topology to one that is more synergistically integrated (*i.e*., multiple paths between two distribution points for enhanced reliability as well as power flow capacity).

Further, the desire to allow autonomous operation, *e.g*., micro-grid in ‘island’ mode, suggests a need for levels of operational reconfigurability well beyond current practice. Accordingly, the new Smart Distribution Grid will present major new challenges operationally from the following perspectives:

* New temporal complexities: variations at time scales ranging from microseconds to hours (load behavior and intermittency of renewable sources due to environmental conditions)
* New topological complexities: resulting from system changes due to micro-grid operations and “mesh” structure
* New operational complexities: multiple (and often conflicting) objectives (economic, environmental, *etc*.). Similarly, a hybrid of various communication technologies along with new protocol stack definitions will likely emerge in support of the above functions.

Notably, new dynamic estimation/control theoretic formulations for the new grid will be critical. Many more new sensors (akin to PMUs in the transmission grid) will be required in the distribution grid to generate local data that support state estimation for regular operation (improved power quality, voltage stability) as well as decision intelligence for incipient events (fault detection and restoration).

## 6.3 Enabling Technologies

The emergent network architectures for the future distribution grid will consist of a mix of existing heterogeneous (wired and wireless) communication technologies. Selecting from among the multiple possibilities will involve the interplay between potential network architectures, data transport needs, and application constraints and most critically, laying the foundations for inter-operability as well as meeting new efficiency and robustness criteria. At the time of writing, such efforts have been initiated, but their fruition appears to be in the distant future.

Clearly, developing value for all stakeholders- the end users, utilities, and 3rd party vendors - must be a cornerstone of any successful transition. This will necessitate economic incentives and market driven policies, in addition to technological innovation. Further, the training and professional development of a new generation of researchers and industry professionals who are inclusively trained in the core underlying technical areas must be a high concomitant priority. This requires sustained funding for growth in existing academic power-systems education and research programs as well as promoting new modes of interactions with industry (particularly in the leading-edge new technology areas) as well as government labs and standards-setting organizations.

Currently, much remains to be done, but hope lies in these enabling technologies on the horizon:

* Energy storage is essential for counteracting intermittency of renewable sources as the penetration level increases; plug-in electric hybrid vehicle would play an important role
* Power electronics and control enables integration of distributed resources, active load management, energy flow control, and efficient energy utilization
* New diagnosis techniques and automated protection
* Mobile power-systems technologies on:
  + Electric ships
  + More electric aircraft
  + Vehicles
* Test-bed and pilot programs, and demonstration projects

# 

# Towards a Trustworthy Future Power Grid

## 7.1 Introduction

Critical infrastructures are complex physical and cyber-based systems that form the lifeline of modern society. Their reliable, secure, and safe operations are of paramount importance to national security and economic vitality. The electric-power grid, one of the key critical infrastructures, is a highly automated network that uses a variety of sensors, information/control systems, and communication networks (e.g., SCADA, EMS, Wide Area Monitoring (WAMS), DMS) for the purpose of real-time monitoring and control of the generation, transmission, and distribution functions, and also for efficient planning and market functions of the grid. These information and communication systems are collectively known as cybersystems.

Since the 1970s, the power grid control framework has gradually evolved from a closed monolithic structure to a more open networked environment. With the recent trend of using standardized protocols, more utilities are moving toward an Internet Protocol (IP) based system for wide-area communication. The compatibility of standards has also leveraged the cost of system deployment among the vendors to improve system upgradeability. However, a tighter integration may also result in new vulnerabilities. The security concern over information exchange between various power entities is more challenging as the potential of cyber threats grow. The increasing dependence upon SCADA communications over the Internet has added to the significance and magnitude of the problem. Moreover, the deployment of smart sensors (*e.g*., Advanced Metering Infrastructures (AMI)) and associated information systems, and communication networks increases the exposure of power grid to cyber-attacks. Security awareness and personnel training concerning supervisory control systems have become crucially important.

Security threats against utility assets have been recognized for decades. In the aftermath of the terrorist attacks on September 11, 2001, great attention has been paid to the security of critical infrastructures. Insecure computer systems could lead to catastrophic disruptions, disclosure of sensitive information, and fraud. The findings in a report titled “Critical Infrastructure Protection”, Government Accountability Office (GAO), 2004 [1], highlights the extensive plans of the terrorist organizations to disrupt U.S. critical infrastructures, which is highly disturbing; and subsequent GAO reports on this topic stress the urgency of securing these systems against cyber-attacks originating from many groups that include terrorists, criminals, hackers, spammers, malware authors, botnet operators, organization insiders, and hostile nations. A potential for cyber-attacks on the power grid and its growing trend is also well recognized in many industry reports (*e.g*., McAfee commissioned an industry survey report) [9]. Therefore, cybersecurity and trustworthiness of the power grid are pressing issues for today’s electric power grid and in the emerging smart grid.

There are many research, education, and industry tasks that are performed well today. However, they are done either in the cyber domain or in the power-system domain, but not in an integrated CPS domain that is required for future power grid. The CPS research focus is critically important to understand and analyze the reliance of power grid on the cyber system (and *vice-versa*) and to empower the future power grid with resiliency and trustworthy properties through suitable designs and upgrades.

## 7.2 Barriers

The ever increasing power of the Internet coupled with its connectivity to SCADA networks increases the possibility of simultaneous coordinated cyber-attacks compromising multiple critical cyber assets of the power grid. A potentially high-impact attack would involve one or more intruders gaining access into the supervisory control system of one or more interconnected control areas of the grid and simultaneously launching wrong control actions. This could result in maximum damage to the system in terms of generation/transmission loss, thus further resulting in huge un-served loads, equipment damage, or even cascading outages. Another primary concern has been the possibility of massive Denial of Service (DoS) attacks on the SCADA control system to the extent that the real-time operation of the SCADA is affected, with resulting consequences on the overall performance and stability of the power grid.

Defending against cyber-attacks on SCADA networks is a challenging task, given the wide range of attack mechanisms, the decentralized nature of the control, and the lack of coordination among various entities in the electric grid brought about by deregulation. Currently the electric power control system does not have adequate measures to guarantee protection against malicious physical or cyber-attacks. Various cyber incidents in the recent past have indicated the extent to which these SCADA systems are vulnerable and the urgent need to protect them against electronic intrusions. NERC critical-infrastructure-protection (CIP) compliance is mandatory: utilities are required to undertake cybersecurity vulnerability assessment and to take corrective measures where necessary. To secure the power grid against cyber-attacks and make it robust and trustworthy, there have been new policy initiatives from the Federal Government (DoE, DHS), R&D and education undertaken by National Labs and academic institutions, and development and deployments undertaken by industries. All these efforts will continue for the foreseeable future as the level of automation is likely to increase in the power grid (especially in the smart grid). This in turn will introduce more vulnerability, and thus, will increase the cybersecurity risk.

The following are some of the major barriers today to achieving trustworthiness in the energy grid.

### 7.2.1 System Complexity

* The power grid is inherently a complex system with tight coupling between physical and cyber components of the system.
* It is a massively scaled infrastructure that spans the continent with multiple levels of administrative controls that have a huge number of components, devices, and pieces of equipment that exhibit a high degree of heterogeneity in their functionality, reliability, and security.
* It exhibits multi-scale interactions among components, subsystems, and control areas -- both spatially and temporally.
* The level of interdependency in the power grid and potentials for cascading failure mean that the grid's resilience to cyber-attack may be based on the least secure assets. If one utility is very secure, an attacker may be able to attack a nearby utility and create the same impact.
* The modern grid operates with a data glut, which can be exacerbated in the face of real-time constraints.

### 7.2.2 System Models & Architectural

* Lack of compositional modeling frameworks that integrate cyber as well physical aspects of the system.
* Lack of adequate cybersecurity models (trust models) and architecture for control system that captures real-time characteristics and dynamics of the power system.
* Lack of a realistic risk- modeling framework that systematically computes the likelihood of cyber-attacks on the critical cyber assets and the resulting impacts (or consequences) on the operational, planning, and market aspects of the power grid in terms of load loss, equipment damage, system stability violations, and/or economic loss due to malicious cyber events in the power system.
* Lack of comprehensive CPS security frameworks that incorporate risk modeling and robust countermeasures encompassing capabilities for real-time monitoring of malicious cyber events, attack prevention, attack detection, attack mitigation, and attack tolerance.
* Lack of realistic benchmark data sets for model validation and lack of cyber-physical simulation and test-bed environments for security evaluation, conducting attack-defense exercises, and testing new countermeasures measures in a controlled environment.

### 7.2.3 Legacy Systems & Certification

* Legacy nature of the SCADA control system that is inherently insecure when connected to the internet.
* Engendering trust of legacy system operators - what is the role of human operators?
* Inadequate interoperability standards
* Inadequate understanding of incremental deployment of security on legacy systems.
* Lack of "verifiable" certification metrics and path to certification beyond NERC CIP compliance.

Legacy software is expensive to upgrade. Upgrading security SCADA software will require substantial investments by both vendors and utilities. There's a current lack of evaluation and validation of SCADA systems. Software does not undergo a formal review process and does not receive accreditation for achieving known security baselines. Some current SCADA software may not be able to meet the existing NERC CIP mandate. Current compliance (NERC CIP) is not as sophisticated as other compliance standards such as NIST 800-53: Recommended Security Controls for Federal Information Systems [10]. Security is emphasized as a goal instead of a continuing process.

### 7.2.4 Social/Educational/Training

The panel identified several non-technical barriers to achieving and maintaining the needed level of cybersecurity on the power grid. These are

* Not thinking beyond “security through obscurity” mindset.
* Power system vs. software system vs. system science - lack of common vocabulary and reluctance to interact among disciplines.
* Apathy towards security by legacy control-system engineers working in the power industry
* Inadequate funding for research, education, training, and workforce development
* Inadequate amount of interactions among academia, national labs, and industry on the cybersecurity of critical infrastructure systems
* Inadequate awareness and understanding of control-system security issues and often thinking that IT security solutions will solve the control-systems security problems
* Inadequate understanding of safety aspects associated with critical infrastructure systems ,such as the power grid
* Inadequate new educational programs, conferences, and training and outreach programs on cybersecurity of cyber-physical critical infrastructure systems
* The power industry generally does not understand the level of sophistication that an attacker may have, as attacks may be more advanced than, *e.g.,* Operation Aurora.

# Challenges

### 7.3.1 Defining Trustworthiness

The term "trusted/trustworthy" has different connotations depending on the stakeholder. The DoD would define “trusted” as formally verifiable, while much of the computing industry interprets this as cryptographically signed code execution. Having a consistent view of trustworthiness and defining trust models is the first step toward achieving a trustworthy energy infrastructure. Trustworthiness has multiple viewpoints depending on the level of abstraction and the type of stakeholders:

* High-level view: Does it operate “correctly”?
* Low-level view: There are many dimensions to trust, including secure, Quality of Service (QoS), functional, robust performance, dependable, survivable, efficient, fair, *etc*.
* Stakeholder viewpoints:
  + Consumer: “press button - power is on”
  + System operator: “no surprises” - “works as expected"
  + Market players: fair and secure

The stakeholders include utilities, consumers (residential, commercial, industrial), generation assets, transmission and distribution assets, regulatory agencies, local/federal government.

### 7.3.2 Information Systems Security vs. Control Systems Security

It is often misunderstood that control system security is the same as information security. The control system’s security properties need to be clearly identified, specific to the given application and be an integral part of the trust model.

* Control systems security properties are more comprehensive than those of information assurance in IT systems, which include confidentiality, integrity, availability, authorization control, and non-repudiation.
* Control systems security properties typically include information assurance properties and physical system properties (*e.g.,* system dynamics, system stability, cascading failures, feedback control, real-time performance, and safety. In some cases, control systems are heavily skewed towards availability and integrity, while information systems have traditionally focused on integrity and confidentiality. Thus a clear definition of a control system’s security properties and their relevance in specific applications of power grid need to be defined.

### 7.3.3 Building Trustworthy Systems

The design, analysis, and deployment of trustworthy systems require addressing some of the following research issues:

* Defining threat models for the control system
* Defining trust models for the control system
* Developing control system security architectures, secure algorithms and applications, and secure protocols
* Developing a set of security and trust policies that can be verified and certified
* Incorporating built-in security in future energy systems
* Developing methods to deploy security solutions to existing legacy systems
* Building trustworthy systems using untrustworthy components. There is a need to understand the critical requirements necessary to provide an adequate level of security adequate for a system to mitigate inherent risks.

### 7.3.4 Robustness Against All Forms of Cyber/Electronic Attacks

Cyber attacks can come in many forms that include:

* Intrusion-based attacks
* Botnet-based DoS attacks
* Communication-protocol-based attacks
* Wireless communication attacks
* Malware, phishing, and spear-phishing attacks
* Drive-by-download attacks
* Social-engineering-based attacks
* Man-in-the-middle attacks in the form of denying/delaying/modifying/replaying of sensing signals or control signals that are part of the SCADA and other feedback control system operation
* Spam attacks

In particular, a new form of DoS attack, known as Denial of Control, is very specific to a control system and could be waged through man-in-the-middle attacks or by Botnet-based attacks. This attack typically involves compromising the integrity and/or timeliness of the sensing/control signals to affect real-time dynamics of the system.

Based on the number of attackers and their sophistication, the attacks can be classified into four categories:

* Isolated brute-force attacks
* Isolated intelligent attacks
* Coordinated brute-force attacks
* Coordinated intelligent attacks

The attacker in an intelligent attack has knowledge about the operation of the power system and leverages that knowledge to create maximum impactful control actions for a given system exploit. The coordinated intelligent attack is the most lethal to the system and therefore must be prevented, or mitigated and withstood by the system. Insider threats potentially constitute a coordinated intelligent attack. The access to critical cyber assets and associated control actions should be protected through appropriate role-based access-control mechanisms and associated verification.

### 7.3.5 System Resiliency

Achieving system resiliency is more comprehensive than achieving system security. In particular, a massive DoS attack has the potential to bring down or slow communication networks, control servers, or other critical cyber assets through resource exhaustion (in terms of consuming CPU cycles, communication bandwidth and buffers, *etc*.) even if these are well secured. Such DoS attacks can have severe impacts on the real-time operation of the power grid and hence its stability. Therefore, the goal of achieving a resilient power grid must address both security and dependability issues together, presenting a significant design challenge.

### 7.3.6 Communication Network Security

Standard protocols are probably more secure than proprietary protocols, but the risk is inherited from utilizing the Internet. A massive-scale deployment of WAM (wide-area measurement system) technologies (e.g., smart sensors, smart meters, PMUs, and Phasor Gateways) exposes the power grid to potential cyber-attacks if the devices are not properly secured. Potential intrusion into control network through the corporate network or substation automation system should be prevented. Generally, key management is a significant problem when trying to create secure communication and is probably not well understood in control systems. Smart grid/AMI (advanced metering infrastructure) will be heavily based on wireless technology and have a substantial need for secure communications, but the difficult of key generation/management has not yet been addressed, and hence a significant research effort is needed in this direction.

### 7.3.7 Information Assurance vs. Infrastructure Security

Information assurance consists of achieving confidentiality, integrity, availability, authentication, non-repudiation, and access-control properties of control systems. Infrastructure security is defined as protecting infrastructure elements of the control systems (*e.g*., digital devices, communication networks, WAM devices, such as PMUs, SCADA servers, and substation- automation systems). While information- security violations have impacts on the consumers of that information, infrastructure security attacks have impacts on the functioning of the components/subsystems that are attacked, and hence, impact all the associated information/communication they are associated with. Therefore in most cases, infrastructure attacks are much more impactful on power-grid operation than mere information-assurance attacks on a given communication between two entities.

### 7.3.8 Security at Multiple Levels

It is important to understand and manage risk at each level so that security can be added appropriately. This involves:

* Security at substations, control centers, generation, transmission, and distribution systems
* Last-mile security
* Wired-network security
* Wireless-network security
* It will be necessary to deploy defense in depth whereby multiple levels of defense are established through electronic security perimeters covering critical cyber assets

### 7.3.9 Fundamental Design Tradeoffs

There is a general risk-versus-benefit tradeoff whenever a new cyber system is introduced into an environment. Tradeoffs involve trust or security with other system properties, which, depending on the specific system scenario, must be carefully captured through suitable system models and balanced through the use of adaptive algorithms so as to improve the overall trustworthiness of the power system. The tradeoffs include:

* Trust vs. performance
* Security vs. performance
* Security vs. usability
* Security vs. emergency response
* Security vs. distributed decision making
* Security vs. dependability

# Research Strategies

### 7.4.1 Leveraging Information Security

Information security includes the development of algorithms that achieve information assurance properties (*e.g.,* intrusion prevention, detection, tolerance algorithms)

* Secure protocols
* Encryption algorithms and public key infrastructures (PKI) and other relevant security architectures and protocols
* Real-time monitoring technologies
* Threat models
* Trust models
* Multi-level security models and algorithms.

Solutions, other than PKI, need to be developed for large-scale key management. In addition, more diverse authentication and access control mechanisms, large-scale identity management, and advanced auditing/forensic capability are needed in the emerging smart grid environment. Moreover, further research is needed to provide security solutions to ensure high availability.

### 7.4.2 Cyber-Physical-Systems Security Models, Framework, and Analysis

The development of accurate and flexible power and cyber models is required before CPS analysis can become meaningful. The following must be developed in order to achieve this goal:

* CPS security models - trust models, attack models, risk models, emergent-behavior models
* Quantitative risk modeling framework that takes into account threats, vulnerability, and impacts, (in terms of one or more of loss of load, equipment damage, economic loss, cascading outages, stability violations, safety violations, or psychological impacts)
* Component-based formal-modeling framework for CPS that includes security and trustworthiness properties
* Formal verification methods for control system security properties of SCADA control system
* Model-based decision-and-control framework for energy cyber-physical systems that enables the development of large-scale systems that are correctly constructed and whose properties can be verified
* Scalable model that provides the capability to define and analyze the power system beyond NERC's “*N-1* contingency” criteria, in particular, investigation of suitable reliability standards to deal with coordinated cyber-attacks, and developing system architectures and operational algorithms to achieve the new criteria
* Privacy-preserving human-activity models and algorithms to support demand-side management

### 7.4.3 Cyber-Physical Systems Security Algorithms

There is a basic need for the development of security algorithms and tools that directly address the specific needs of the power grid. Specific algorithms include:

* Real-time monitoring algorithms that include domain-specific intrusion detection and anomaly detection and software tools incorporating ideas such as machine learning. Intrusion detection algorithms and software tools should be power-system/SCADA aware.
* Risk-mitigation algorithms, working in conjunction with a risk-modeling framework, that include a combination of cyber-system mitigations (*e.g*., traffic filtering/rerouting and throttling) and power-system mitigations (*e.g*., load shedding, generation shift, and controlled islanding)
* Secure SCADA communication protocols that meet security and real-time performance requirements
* Distributed control-and-decision algorithms to achieve system robustness and trustworthiness in a scalable manner in the face of natural and man-made fault or malicious events in the system
* Multi-agent-based adaptive algorithms for distributed trust management
* Cost-benefit analysis quantifying the economic and other benefits obtained through security investments

### 7.4.4. Resilient Power Grid

To withstand massive "resource exhaustion attacks" (through Botnet-based DoS or other forms of DoS) on the SCADA servers, wide area control networks, or LAN, sufficient amount of redundancy must be built into the system so that alternative servers or communication paths can be activated as part of the attack-mitigation plan. It should be noted that secure protocols and algorithms do not necessarily prevent or mitigate resource-exhaustion attacks. Therefore, "system resilience" must be kept in mind while designing a smart grid and upgrading the power grid with trustworthy features. In particular, the use of dependable design concepts such as information-system redundancy, distributed fault diagnosis, and self-healing of information systems and networks must be integral parts of the future power grid.

### 7.4.5 Security of Wide Area Monitoring (WAM)

WAM technologies using PMUs are being widely deployed in today's power grid for real-time monitoring of system parameters to achieve improved state estimation, system control, and operational decision making. The network of PMUs, called the North American SynchroPhasor Initiative Network (NASPInet) [6], is poised to become an integral part of the future smart grid. The security and resiliency of NASPInet is a very important aspect of the smart grid, which includes the security and fault-tolerance of PMU devices and Phasor Gateways, and the security and resiliency of the "data bus,” the communication interface among Phasor Gateways.

### 7.4.6 CPS Simulation and Testbed Environments:

The environment should seamlessly integrate industry-grade cyber system (*e.g.,* SCADA and EMS servers, SCADA communication protocols, substation automation systems, security devices and protocols, market simulators), and power system components (*e.g*., generation, loads, relays, WAM technologies, real-time digital simulators) of the power grid so CPS security, robustness, and trustworthiness properties can be studied, analyzed, and validated. In particular, cyber-attack-defense exercises should be conducted to study the effectiveness of defense mechanisms. In addition, the platform should provide capabilities for hardware-in-the-loop system-level simulation/emulation studies. The testbed platform should provide insights into power-system components with both cyber and physical controls to prevent malicious manipulations. The platform should be programmable, reconfigurable, and scalable so new power-system configurations (with cyber elements) can be easily defined and studied. Research evaluations, product testing, and developers of new control systems are potential uses of the testbed.

### 7.4.7 Benchmark Topologies and Datasets for Validation

There is a significant need for the creation of benchmark CPS topologies (including SCADA configurations) and realistic data sets for security evaluations. The topologies should identify the physical and cyber-system parameters including security features. The benchmark topologies and data sets should be made available in the public domain so that they are widely available to researchers. In addition, the topologies and data sets should be constantly evolving to be up-to-date with new system configurations, vulnerabilities, and reported incidents.

### 7.4.8 Synergistic Partnership Among Stakeholders

The research activities, simulations, and testbed development described here will be undertaken through synergistic partnerships between universities, national labs, and industries with the help of Federal funding. In particular, National SCADA Testbed [7] resources could be leveraged to create this open testbed platform. The testbed and simulation environments should be made available to academic researchers, national laboratories, and industry researchers, similar to PlanetLab [13], for experimenting with internet protocols. The testbed should be open-sourced so that researchers can contribute to its growth and sustainability. Also, strong collaboration is needed to create benchmark data suites and to validate the analytical and simulation models using realistic datasets and benchmarks.

Appropriate cyber security standards for the power grid must be developed through partnerships with NERC, DoE, NIST, and DHS, leveraging expertise from IEEE technical societies such as the Power and Energy Society [8]. Collaboration among Federal agencies is required to support the development and management of the CPS testbed, develop control-systems cybersecurity standards, and share best practices.

### 7.4.9 Education, Research, and Training

To meet the growing needs of skilled manpower in the emerging area of CPS security, new educational programs must be developed both at the graduate level and the undergraduate level. A model curriculum in CPS security must be developed. The body of knowledge should include fundamental topics from cyber systems (*e.g.,* computer networks, network security, real-time and fault-tolerant systems, and discrete mathematics and algorithms) and from power systems (*e.g.,* power-systems steady-state analysis, power-system dynamics, control systems, systems engineering), and emerging topics *(e.g*., the smart grid). The breadth and depth of the program depends on the level at which it is administered – graduate-level or undergraduate-level, minor degree or major degree. In addition to degree programs, certificate programs (through continuing education) must be developed to enable industry engineers to acquire skills in this new area. In addition, industry short courses and tutorials sponsored through IEEE forums should be encouraged so that the knowledge is widely disseminated to industry and academic audiences.

## 7.5 Roadmap

Following are some of the key research and educational tasks that should be undertaken in the next 5-10 years:

### 7.5.1 Five-Year Roadmap

* Quantitative trust models and risk models with associated cyber-physical analysis frameworks and algorithms
* Resilient system architectures and algorithms accounting for system security and dependability for a future power grid
* Multi-agent framework with distributed sensing-and-decision algorithms to ensure trustworthiness and robustness in the power grid
* Multi-agent architecture and algorithms for distributed trust management
* Algorithms for identity management and for auditing/forensic analysis in smart-grid environment
* Real-time algorithms for attack monitoring, mitigation, and resistance on the power grid
* Scientific foundation for building trustworthy systems from untrustworthy components and subsystems
* Open CPS security testbed environment and benchmark datasets for security evaluations and model validations
* Scientific methodology for incremental deployment of security and trustworthiness properties into legacy power systems and associated verification, validation, and certification processes
* CPS security program at graduate and undergraduate levels

### 7.5.2 Ten-Year Roadmap

* Smart-grid trustworthiness, resiliency, and sustainability against impairments due to natural and man-made faults, malicious events, and errors
* Mature models and methodology for building trustworthy cyber-physical systems from untrustworthy components and subsystems, and field demonstrations
* CPS security standards and pathways to certification
* CPS security testbed enhancements
* Cyber-based integration of interdependent critical infrastructure systems ,such as, (*e.g.,* the power grid, transportation systems, water distribution systems, oil and natural gas pipeline infrastructure) and associated CPS security models, algorithms, and analysis tools
* Demonstration of provably correct Energy-Cyber-Physical Systems

### 7.5.3 Initiatives

To accomplish the above roadmaps, the following initiatives must be undertaken:

* Synergistic partnerships between university, industry, and national labs
* Coordination among smart-grid initiatives (*e.g.,* NIST Smart Grid Security [4] and DoE NASPInet) [5] initiatives
* Centers of Academic Excellence in CPS security, research, and education
* Industry-University Research Centers (IU/CRC) in CPS security
* Federal graduate-fellowship programs in CPS security
* Cyber-defense competitions (college-level) focusing on a control system’s security.
* Industry short-courses on control system’s security focusing on the energy sector and expanding it to other critical infrastructures
* Implementation of model curriculum in CPS security in major universities
* Establishing Engineering Research Centers (ERC) in the area of critical infrastructure, resiliency, and sustainability

## 7.6 Conclusion

The vision of realizing a “trustworthy future power grid” involves addressing several fundamental challenges that are technical, social, and multidisciplinary in nature. This requires significant investment from Federal and industry stakeholders and synergistic research collaborations between universities, national labs, and industries to create fundamental science and engineering in this area and transform them into technologies that can be deployed in practice in the modern smart grid. In addition, significant efforts are needed to create new interdisciplinary educational programs through university-industry partnerships to train highly skilled engineers for the modern workforce.

## 7.7 Related Sources

* [1] GAO 04-354, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems", March 2004. <http://www.gao.gov/new.items/d04354.pdf>
* [2] NERC CIP Standards. <http://www.nerc.com>
* [3] DHS Control Systems Security Program (CSSP). <http://www.us-cert.gov/control_systems/>
* [4] NIST IR 7628: Smart Grid Cybersecurity Strategy and Requirements. <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>
* [5] North American SynchroPhasor Initiative. <http://www.naspi.org/>
* [6] Power Systems Engineering Research Center (PSERC). <http://www.pserc.wisc.edu/home/index.aspx>
* [7] National SCADA Testbed Program. <http://www.inl.gov/scada/>
* [8] IEEE Power & Energy Society. <http://www.ieee-pes.org/>
* [9] “In the Crossfire - Critical Infrastructure in the Age of Cyber War”, McAfee Report, 2010. <http://newsroom.mcafee.com/>
* [10] “NIST 800-53: Recommended Security Controls for Federal Information Systems”, Dec. 2007.
* [11] DETERlab Testbed: Cyber-DEfense Technology Experimental Research laboratory Testbed. <http://www.isi.edu/deter/>
* [12] ISEAGE: Internet Scale Attack Event and Attack Generation Environment. <http://www.iac.iastate.edu/iseage/>
* [13] PLANETLAB: An Open Platform for developing, deploying, and accessing planetary-scale services. <http://www.planet-lab.org/>
* [14] P.A. Boyd, G.B. Parker, D.D. Hatley, “Load Reduction, Demand Response, and Energy Efficient Technologies and Strategies,” Pacific Northwest National Laboratory, PNNL-18111, November 2008, http://www.pnl.gov/main/publications/external/technical\_reports/PNNL-18111.pdf

# 8. **Appendix**

## 8.1. Workshop Working Groups

## 8.1.1 Structural Features of Future Energy Systems: Implications on New Modeling and Control Needs

#### 8.1.1.1 Participants

* Ali Abur (NEU)
* Alejandro Dominguez-Garcia (University of Illinois at Urbana-Champaign) -Moderator
* Joshua Edmison (BBN Technologies)
* Ian Hiskens (University of Michigan) -Moderator
* Ali Keyhani (Ohio State University)
* Johann Kolar (ETH)
* Farshad Khorrami (Polytechnic University)
* Dagmar Niebur (NSF) -Observer
* Ahmed Saber (Missouri University S&T)
* Mohammad Shahidehpour (IIT)
* Dick O’Neill (FERC)
* Michael Walker (General Atomics)
* Le Xie (Texas A&M)
* SudipMazumder (University of Illinois, Chicago)

### 8.1.1.2 Writing Team

### Alejandro Dominguez-Garcia (University of Illinois at Urbana-Champaign) (Lead)

# 8.1.2 Toward a Formal Framework for Designing Energy-CPS

## 8.1.2.1 Participants

* Sohrab Asgarpoor (University of Nebraska - Lincoln)
* Guy Al Lee (Intel Corporation)
* Steven Eisenbarth (Baylor University)
* Franjo Ivancic (NEC Laboratories America)
* Vincenzo Liberatore (Case Western Reserve University)
* Kumar Venayagamoorthy (Missouri University of Science & Technology)
* Lei Wang (University of Connecticut)
* Seyed Zekavat (Michigan Technological University)
* Frank Mueller (North Carolina State University) – Moderator
* Eugenio Schuster (Lehigh University) – Moderator
* Michael Branicky (NSF) – Observer

## 8.1.2.2 Writing Team

* Michael Branicky (Former NSF, now Case Western University)
* Vincenzo Liberatore (Case Western Reserve University)
* Bruce M. McMillin (Missouri University of Science and Technology) (Lead)
* Eugenio Schuster (Lehigh University)

# 8.1.3 High Efficiency Building Technologies and Demand Control

## 8.13.1 Participants

* Joseph Bentsman (University of Illinois, Urbana-Champaign)
* Joe Bockhorst (University of Wisconsin-Milwaukee)
* Morteza Daneshdoost (Southern Illinois University Carbondale)
* Baikun Li (University of Connecticut) - Moderator
* Sudip K. Mazumder (University of Illinois, Chicago) - Reporter
* Karen Miu (Drexel University)
* PravinVaraiya (University of California, Berkeley)
* Hamid Zareipour (University of Calgary)
* Michael Caramanis (Boston University)

## 8.1.3.2 Writing Team

* Michael Caramanis (Boston University) (Lead)
* Pravin Varaiya (University of California, Berkeley)
* Randy Katz (University of California, Berkeley)
* Prabir Barooah (University of Florida)

# 8.1.4 Cyber-Enabled Smart Distribution Systems and Smart Grids

## 8.1.4.1 Participants

* Michael Caramanis (Boston University)
* Scott Coombe (ONR)
* Craig Eldershaw (Palo Alto Research Center)
* Rajesh Gupta (University of California at San Diego)
* Herb Hess (University of Idaho)
* Lan Li (ABB)
* Bipul Luitel (Missouri University of S&T)
* Monica Mallini (IEEE)
* Darrell Massie (IPERC)
* Bruce McMillin (Missouri University of S&T)
* Sirisha Medidi (Missouri University of S&T)
* Joydeep Mitra (Michigan State University)
* Zhihua Qu (University of Central Florida)
* Sumit Roy (University Washington)
* Jian Sun (Rensselaer Polytechnic Institute)
* Sid Suryanrayanan (Colorado School of Mines)
* Subrahmanuam Venkata (University Washington)
* Sally Wood (National Science Foundation)

## 8.1.4.2 Writing Team

* Jian Sun (Rensselaer Polytechnic Institute)
* Sumit Roy (University Washington) (Lead)
* Sid Suryanrayanan (Colorado State University)
* Sally Wood (Former National Science Foundation, now University of Santa Clara)
* Michael Caramanis (Boston University)
* Bruce McMillin (Missouri University of Science and Technology)

# 8.1.5 Towards a Trustworthy Future Power Grid

## 8.1.5.1 Participants

* Mark Anderson (Teledyne)
* Anneliese Andrews (University of Denver)
* Azad Azadmanesh (University of Nebraska - Omaha)
* Ryan Bradetich (Schweitzer Laboratories) - Participant & Report Reviewer
* Manimaran Govindarasu (Iowa State University) - Moderator & Chair
* Cameron Johnson (Missouri S&T)
* Michael Lemmon (University of Notre Dame) - Moderator
* Franxing Li (Universityof Tennessee)
* Thomas Morris (Mississippi State University)
* Dave Naumann (Stevens Institute of Technology)
* Thomas Ortmeyer (Clarkson University) - Participant & Report Reviewer
* Orest Pilskalns (Washington State University)
* Rick Schantz (BBN)
* Serdar Uckun (PARC)

## 8.1.5.2 Writing Team

* Manimaran Govindarasu (Iowa State University) (Co-Lead)
* Thomas Ortmeyer (Clarkson University) (Co-Lead)
* Ryan Bradetich (Schweitzer Laboratories )

# 8.2 Organizers

* Co-Chairs
  + Marija Ilic (Carnegie Mellon University)
  + Clas Jacobson (United Technologies Research Center)
* Program Committee
  + Michael Caramanis (Boston University)
  + Dian Deepak (GA Tech)
  + Alejandro Dominguezs-Garcia (University of Illinois at Urbana-Champaign)
  + Steven Fernandez (Oak Ridge National Lab)
  + Christoforos Hadjicostas (University of Illinois at Urbana-Champaign)
  + Ian Hiskens (University of Michigan)
  + Eric Hsieh (National Electricity Manufacturers Association (NEMA)
  + Bruce Krogh (Carnegie Mellon University)
  + Eugene Litvinov (ISO-NE)
  + Sudip Mazumder (University of Illinois, Chicago)
  + Bruce McMillin (Missouri University of Science and Technology)
  + Sirisha Medidi (Boise State University)
  + John-Francis Mergen (BBN)
  + Jose M.F. Moura (Carnegie Mellon University)
  + Euginio Schuster (Lehigh University)
  + Aleksandar Stankovic (Northeastern University)
  + Siddharth Suryanarayanan (Colorado School of Mines)
  + Pravin Varaiya (University of Science and Technology)
  + G.K. Venayagamoorthy (Missouri University of Science and Technology)
* Government Points of Contact
  + Sushil Birla (Nuclear Regulatory Commission
  + Michael Branicky (Case Western Reserve University)
  + Harold Coombe (Office of Naval Research)
  + Helen Gill ( National Science Foundation)
  + Henry Kenchington (Department of Energy)
  + Brad Martin (National Security Agency)
  + John Pazik (Office of Naval Research)
  + Al Wavering (National Institute of Standards and Technology
* Sponsor Agencies
  + National Institute of Standards and Technology
  + National Security Agency
  + National Science Foundation

# 8.3 Acronyms and Definitions

* AMI Advanced Metering Infrastructures
* ANSI American National Standards Institute
* BACnet building automation and control system
* CG Coordinating Group
* CIP Critical Infrastructure Protection
* COTS Commercial- off-the-shelf
* CPS cyber physical systems
* CPU Central Processing Unit
* CR Cognitive Radio
* DGs distributed generators
* DHS United States Department of Homeland Security
* DMS Distribution Management System
* DOE United States Department of Energy
* DoS Denial of Service
* ECPS Energy Cyber-Physical System
* EMS Energy Management System
* ERC Engineering Research Centers
* EV Electric vehicles
* FACtS Flexible AC Transmission Systems
* FAPER Frequency Adaptive Power Energy Regulator
* FIDVR fault-induced delayed voltage recovery
* GAO United States Government Accountability Office
* GE General Electric
* GFA Grid Friendly Appliances
* HCSS High Confidence Software and Systems
* HEB High Efficiency Building
* HVAC heating, ventilation, and air-conditioning
* IEEE Institute of Electrical and Electronics Engineers
* IEEE 1547 Standard for interconnecting distributed resources
* IIE Intelligent Information and Execution
* IU/CRC Industry-University Research Centers
* IP Internet Protocol
* IT Information Technology
* LED light-emitting diode
* MIT Massachusetts Institute of Technology
* NAE National Academy of Engineering
* NASPInet North American Synchro Phasor Initiative Network
* NERC CIP North American Electric Reliability Corporation Critical Infrastructure Protection
* NIST National Institute of Standards and Technology
* NITRD Networking and Information Technology Research and Development
* NSF National Science Foundation
* OEM Optimal Energy Management
* PeV plug-in electric vehicle
* PHEV Plug-in hybrid electrical vehicle
* PNNL Pacific Northwest National Laboratory
* PMU Phasor measurement unit
* PKI public key infrastructures
* PV Photo Voltaic
* R&D Research and Development
* RF Radio Frequency
* SBN smart-building/neighborhood
* SCADA Supervisory control and data acquisition
* SDR Software Defined Radio
* SOS systems of systems
* V2G vehicle-to-grid
* VAPER voltage adaptive power energy regulators
* VAR Volt-Amp reactive
* WAMS Wide Area Monitoring
* WiFi Wireless Local Area Network
* ZigBee specification for a suite of high level communication protocols used to create personal area networks built from small, low-power digital radios

# 8.4 Workshop Program

**National Workshop on Research Directions for**

**Future Cyber-Physical Energy Systems**

**Sheraton City Center Hotel, Baltimore, Maryland**

**June 3-4, 2009**

**Program Agenda**

**Wednesday, June 3**

*7:00 A.M. – 8:00 A.M.* **Continental Breakfast (Liberty A, Lobby Level)**

*7:00 A.M. – 8:00 A.M.* **Registration (Liberty Foyer, Lobby Level)**

**General Session (Liberty B, Lobby Level)**

*8:00 A.M. – 8:15 A.M.* **Opening Remarks, Goals, and Terms of Reference for**

**Workshop**

*Marija Ilic, Carnegie Mellon University (CMU) and Workshop Co-Chair*

*Clas Jacobson, United Technologies Research Center (UTRC) and*

*Workshop Co-Chair*

*8:15 A.M. – 8:30 A.M.* **NCO/NITRD Introduction**

*Chris Greer, National Coordination Office for Networking and*

*Information Technology R&D (NCO/NITRD)*

*8:30 A.M. – 8:45 A.M.* **High Confidence Software and Systems Initiatives**

*Helen Gill, National Science Foundation (NSF)*

*8:45 A.M. – 9:00 A.M.* **The Challenge of Moving Forward**

*Marija Ilic (CMU and Workshop Co-Chair)*

*9:00 A.M. – 10:00 A.M.* **Government Agency Interests**

*Richard O’Neill, Federal Energy Regulatory Commission (FERC)*

*Helen Gill (NSF), Dagmar Niebur (NSF)*

*H. Scott Coombe, Office of Naval Research (ONR)*

*Al Wavering, National Institute of Standards and Technology (NIST)*

*10:00 A.M. – 10:15 A.M.* **Break (Liberty Foyer, Lobby Level)**

*10:15 A.M. – 10:45 A.M.* **Invited Talk: CPS Community View and Synergies with the**

**Beyond SCADA HCSS Workshop**

*Speaker: Bruce Krogh (CMU* **)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

*10:45 A.M. – 11:30 A.M.* **Keynote: Risk-Limiting Dispatch of the Smart Grid: A Research Agenda**

*Keynote Speaker: Pravin Varaiya (University of California-Berkeley)*

*11:30 A.M. – 11:45 A.M.* **Invited Talk: Structural Features of Future Energy Systems --Implications on New Modeling, Wide-Area Monitoring, and**

**Control**

*Speaker: Ian Hiskens (University of Michigan)*

*11:45 A.M. –12:00 P.M.* **Invited Talk: Galvin Electricity Initiative**

*Speaker: Mohammad Shahidehpour (Illinois Institute of Technology)*

*12:00 P.M. – 1:00 P.M.* **Working Lunch: Position Paper Madness Session (Liberty A,**

**Lobby Level)**

*Moderator: Ron Harley (Georgia Tech)*

*1:00 P.M. – 1:30 P.M.* **Invited Talk: Toward Formal Framework for Designing Energy-CPS: Principles of Future CPSs**

*Speaker: Guy AlLee (Intel Corporation)*

*1:30 P.M. – 2:00 P.M.* **Invited Talk: High Efficiency Building Technologies and**

**Demand Control**

*Speaker: Phillip Price, Lawrence Berkeley National Laboratory (LBNL)*

*2:00 P.M. – 2:30 P.M.* **Invited Talk: Cyber-Enabled Smart Distribution Systems and Micro Grids**

*Speaker: Bruce McMillin (Missouri University of S&T )*

*2:30 P.M. – 3:00 P.M.* **Invited Talk: Towards a Trustworthy Future Power Grid**

*Speaker: Rajit Gadh, University of California-Los Angeles (UCLA)*

*3:00 P.M. – 3:15 P.M.* **Instructions for Breakout Sessions**

*(Workshop Co-Chairs)*

*3:15 P.M. – 3:30 P.M.* **Break (Liberty Foyer, Lobby Level)**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

*3:30 P.M. - 5:30 P.M.* **Breakout Session I: Group I**: **Structural Features of Future Energy Systems: Implications on New Modeling and Control Nee**ds **(Liberty B, Lobby Level)**

*Moderators: Alex Stankovic (Northeastern University) and AlejandroDominguez-Garcia (UIUC)*

**Group II: Toward Formal Framework for Designing Energy-CPS (McKeldin, Cabana Level South)**

*Moderators: Frank Mueller, North Carolina State University (NCSU) and Eugenio Schuster (LeHigh University)*

*3:30 P.M. – 5:30 P.M.***. Breakout Session I Continued:**

**Group III: High Efficiency Building Technologies and Demand Control (Calhoun, Cabana Level South)** *Moderators: Baikun Li (University of Connecticut) and Sudip Mazumder (University of Illinois-Chicago)*

**Group IV: Cyber-Enabled Smart Distribution Systems and**

**Micro Grids** *(***Schaefer, Cabana Level South)**

*Moderators: Rajesh Gupta, University of California-San Diego (UCSD) and Jian Sun, Rensselaer Polytechnic Institute (RPI)*

**Group V: Towards a Trustworthy Future Power Grid (Preston, Cabana Level South)**

*Moderators: Serdar Uckun (Palo Alto Research Institute) and Michael D.*

*Lemmon (University of Notre Dame)*

*5:30 P.M. – 7:30 P.M.* **Working Reception (Liberty A-Lobby Level)**

**Birds of a Feather: Education and Workforce Challenges for**

**CPS**

**Education for CPS:** *Speaker: Sally L. Wood (NSF)*

Power and Energy Engineering Workforce Collaborative

- Outcomes of an NSF/IEEE/PSERC/NERC Workshop

*Speaker: Dagmar Niebur (NSF)*

*Q&A Session*

*Moderators: Workshop*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

**Thursday, June 4**

*7:30 A.M. – 8:30 A.M.* **Continental Breakfast (Liberty A, Lobby Level)**

*7:30 A.M. – 8:30 A.M.* **Registration (Liberty Foyer, Lobby Level)**

**General Session (Liberty B, Lobby Level)**

*8:30 A.M. – 8:45 A.M.* **Opening Remarks**

*(Workshop Co-Chairs)*

*8:45 A.M. – 9:15 A.M.* **Next Generation Future Energy Systems – DOE’s Vision**

*Henry Kenchington, Department of Energy (DOE)*

*9:15 A.M. – 9:45 A.M.* **Invited Industry Talk: Reliability in Smart Grids—Challenges and Opportunities**

*Speaker: Mark Lauby, North American Electric Reliability Corporation (NERC)*

*9:45 A.M. – 10:45 A.M.* **Industry and Academic Panel: Cyber-Physical Energy Systems Challenges**

*Coordinator: Karen Miu (Drexel University)*

*Darrell Massie, Intelligent Power & Energy Research Corporation (IPERC)*

*Alex Huang (NCSU)*

*John-Francis Mergen (BBN Technologies)*

*Steve Leeb (MIT)*

*Ganesh Kumar Venayagamoorthy (Missouri University of S&T)*

*Christopher DeMarco (University of Wisconsin)*

*10:45 A.M. – 11:00 A.M.* **Break (Liberty Foyer, Lobby Level)**

*11:00 A.M. – 12:00 P.M.* **Report Outs of Breakout Session I Summaries:**

**Group I: Structural Features of Future Energy Systems: Implications on New Modeling and Control Needs (Liberty B, Lobby Level)**

*Moderators: Alex Stankovic (Northeastern University) and Alejandro Dominguez-Garcia (UIUC)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

**Group II: Toward Formal Framework for Designing Energy- CPS (McKeldin, Cabana Level South)**

*Moderators: Frank Mueller (NCSU) and Eugenio Schuster (LeHigh University)*

**Group III: High Efficiency Building Technologies and Demand Control (Calhoun, Cabana Level South)**

*Moderators: Baikun Li (University of Connecticut) and Sudip Mazumder (University of Illinois-Chicago)*

*11:00 A.M. – 12:00 P.M.* **Report Outs of Breakout Session I Summaries Continued:**

**Group IV: Cyber-Enabled Smart Distribution Systems and MicroGrids (Schaefer, Cabana Level South)**

*Moderators: Rajesh Gupta, University of California-San Diego (UCSD) and Jian Sun, Rensselaer Polytechnic Institute (RPI)*

**Group V: Towards a Trustworthy Future Power Grid (Preston, Cabana Level South)**

*Moderators: Serdar Uckun (Palo Alto Research Institute) and Michael D. Lemmon (University of Notre Dame)*

*12:00 P.M. – 1:00 P.M.*  **Working Lunch: Position Paper Madness Session (Liberty A, Lobby Level)**

*Moderator: Michael Caramanis (Boston University)*

*1:00 P.M. – 3:00 P.M.* **Breakout Session II: Group I: Structural Features of Future Energy Systems: Implications on New Modeling and Control Needs (Liberty B, Lobby Level)**

*Moderators: Ali Abur (Northeastern University) and Bruce McMillin (Missouri University of S&T)*

**Group II**: **Toward Formal Framework for Designing Energy-CPS (McKeldin, Cabana Level South)**

*Moderators: Sudip Mazumder (UIUC) and Natasha Neogi*

**Group III: High Efficiency Building Technologies and Demand Control (Calhoun, Cabana Level South)**

*Moderators: Subrahmanyam Venkata (University of Washington) and Karen Miu (Drexel University)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

**Group IV: Cyber-Enabled Smart Distribution Systems and Micro Grids (Schaefer, Cabana Level South**)

*Moderators: Michael Caramanis (Boston University) and Sirisha Medidi (Boise State University)*

**Group V: Towards a Trustworthy Future Power Grid (Preston, Cabana Level South)**

*Moderators: Govindarasu Manimaran (Iowa State University) and Fangxing “Fran” Li (University of Tennessee-Knoxville)*

*3:00 P.M. – 3:15 P.M.* **Break (Liberty Foyer, Lobby Level)**

*3:15 P.M. – 4:15 P.M.* **Final Report Outs of Breakout Session Summaries (Liberty B, Lobby Level)**

*(Co-Moderators of Breakout Session II)*

*4:15 P.M. – 4:30 P.M.* **Q&A Session**

*4:30 P.M. – 5:00 P.M.* **Next Steps and Closing Remarks**

*Clas Jacobson (UTRC and Workshop Co-*Chair)

*5:00 P.M.* **Workshop Adjourned**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

National Workshop on Research Directions for Future Cyber-Physical Energy Systems

Sheraton City Center Hotel, Baltimore, Maryland

June 3-4, 2009

8.5 Acknowledgments

The sponsors would like to thank the Cyber-Physical Systems Virtual Organization (CPS-VO) Team at Vanderbilt University’s Institute for Software Integrated Systems (VU-ISIS) and the National Coordination Office for Networking and Information Technology R&D (NCO/NITRD) staff for their valuable contributions to preparing this report.

BLANK PAGE

1. The High Confidence Software and Systems (HCSS) Coordinating Group (CG) is one of eight program component areas of the Networking and Information Technology Research and Development (NITRD) Program. The NITRD Program is part of the National Science and Technology Council, Executive Office of the President. [↑](#footnote-ref-1)
2. Cyber-Physical Systems incorporate sensing and computation into the control of systems that operate in real time and in the real world, *e.g*., the electrical power grid. [↑](#footnote-ref-2)
3. This is a generic term for Supervisory Control and Data Acquisition. [↑](#footnote-ref-3)