Critical National Need Idea

Critical National Need Title:

Smart is Not Enough: Resilience and Securing the Power Grid

Submitting Organization: Idaho National Laboratory

Supporting Organization: Center for Advanced Energy Studies

INL Contact: Craig G. Rieger, Ph.D., PE, Distinctive Signature Lead
Instrumentation, Controls and Intelligent Systems (ICIS)
Idaho National Laboratory
PO Box 1625
Idaho Falls, ID 83415
Office: 208 526 4136
Fax: 208 526 5647
Email: craig.rieger@inl.gov

CAES Contact: Raymond R. Grosshans, Ph.D., Program Coordinator
Center for Advanced Energy Studies
995 University Blvd.
Idaho Falls, ID 83415
Office: 208 526 8389
Fax: 208 526 8076
Email: Raymond.grosshans@inl.gov

Key Words: resilience, complex systems, resilience engineering, smart grid, control systems

Critical National Need Idea

Resilience and Securing the Power Grid

Introduction: Complexity and Resilience

Modern societies depend on complex systems for energy, transportation, sustenance, medical care, emergency response, and security. As we have observed over recent decades in cases of utility and transportation infrastructure failures, natural disasters, and terrorist attacks -- complex systems fail. As the Nation contemplates massive infrastructure investment to address such failures as well as to address a burgeoning economic crisis, we propose that a government, industry, and university consortium focus on system **resilience**. By "resilience" we mean the capacity of a control system to maintain state awareness and to proactively maintain a safe level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature

Systems comprise interconnected parts, nodes and links, which collectively exhibit emergent properties or behaviors beyond those of individual elements. Complexity in a system arises when element interdependencies supersede the importance of individual elements. These dependencies among elements can lead to system rigidity or brittleness which in turn leads to system failure when single elements fail or are intentionally compromised. The problem is characterizing and resolving the interactions with individual elements in such a way that they are not a common source of failure.

There are generally two ways that resilient systems cope with failure and attack: adaption or transformation. Adaptive systems included components designed to function in more than one role, allowing self-modification and leading to emergent properties that counterbalance anomalies while preserving function. Transformable systems have the capacity to reconstitute into fundamentally new systems when external forces render an existing system untenable. Ideally, both adaption and transformability are integrated in resilient systems.

The Idaho National Laboratory (INL) includes unique large-scale infrastructure technology test facilities and a scientific workforce already working on complex system resilience. The INL stands ready to lead a national consortium focused on system resilience and the Smart Grid. In what follows, we lay out the case for such a consortium and describe the attributes of resilience, both in terms of human interaction and system complexity, the research work that will bring this to fruition, and the collaborative environment that is necessary to insure the resiliency of the Nation's complex systems in the face of growing demand and emerging threats.

The Power Grid: Is Smart Enough?

According to the National Academy of Engineering, the single most important engineering achievement of the 20th century was electrification as made possible by the electric grid. This ubiquitous grid, invisible to most consumers, includes over 9,200 electric generating units with more than 1,000,000 megawatts of generating capacity connected to more than 300,000 miles of transmission lines. Always in the background, the grid has powered the Nation's economy for over 100 years, making possible innovations from the assembly line to the internet.

Designed and constructed largely before microprocessors became widely available, the electric grid today – despite its apparent reliability – suffers from underinvestment. The increasing number and duration of "brownouts" and "blackouts" over the past decade is the immediate consequence. Yet, today, the Nation stands poised to demand from the grid even higher levels of performance and reliability.

On the one hand, a growing population will increasingly depend on sensitive microprocessor-based control technologies which, in turn, depend on the ready availability of electricity available in a "steady-state" condition. On the other hand, concern over the Nation's dependence on particular forms of energy from foreign sources and growing concern over the twin threats of environmental degradation and climate change are driving demand for energy production, transmission, and distribution technologies that are not only efficient but are also secure from threats and sustainable. A recent report from the Basic Energy Sciences Advisory Committee of the U.S. Department of Energy suggests that meeting these societal demands will require "new technologies… with performance levels far beyond what is now possible." In this regard, infrastructure investments have been made to produce clean and efficient energy as a means of immediately creating jobs and as a means of transforming the Nation's economy to one that is fueled by science-based innovation.

An intended outcome of this investment strategy is a so-called "Smart Grid," an electric grid that enables two-way digital communications between power producers' and consumers' devices –power plants on one end and hot water heaters on the other, for example. According to the Electricity Advisory Committee of the U.S. Department of Energy in a report entitled: "Smart Grid: Enabler of the New Energy Economy" the nation's electric power grid must be transformed into one that is "more intelligent, resilient, reliable, self-balancing, and interactive" in order to enhance economic growth, foster environmental stewardship, and promote operational efficiencies, energy security, and consumer choice. An Electric Power Research Institute analysis suggests that the use of such a grid would reduce energy consumption by 4.3% itself and enable additional efficiencies using existing technologies to reduce power use by 236 billion kW hours or 22% by 2030.

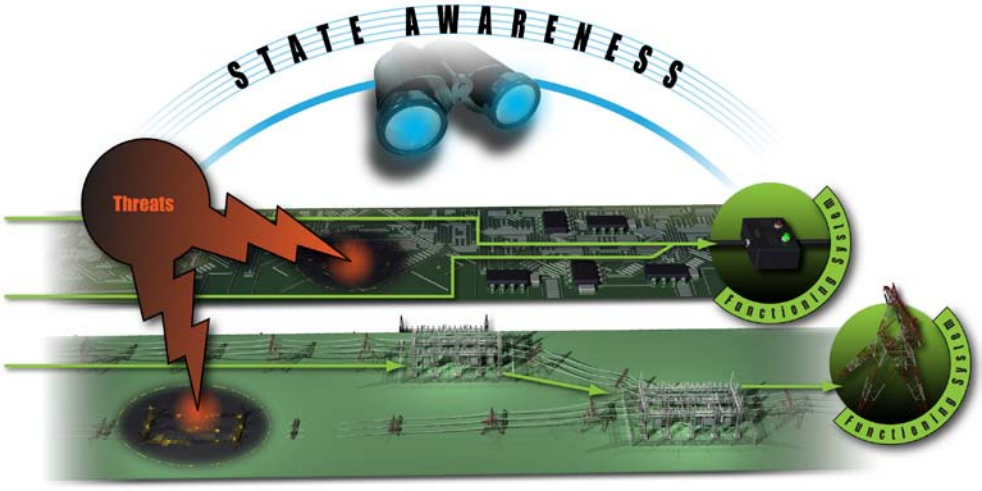
A perhaps more important benefit of Smart Grid deployment is its ability to accommodate energy inputs from renewable sources that are by their nature relatively small scale, geographically distributed, and in the cases of wind and solar – intermittent. In fact, the sine qua non of widespread renewable energy utilization is a grid managed by interoperable communications networks, metering software, and meter data management systems that support bidirectional power flow, looping circuits and transfer of power from substation to substation. Indeed, in anticipation of increased investment by both the federal government and electric producers, efforts are underway to develop the elements of a Smart Grid including hardware (sensors, meters, and communication systems), software (data detection, management, and communication), and protocols and standards to insure the interoperability and security of the national grid.

At this historic juncture, when the Nation is preparing to invest billions in critical infrastructure in order to transform the economy and to secure sustainable energy supplies for future generations, a

consideration not yet elevated to the level of a national challenge is the *resilience* of the soon-to-emerge Smart Grid. Implementing a Smart Grid will entail the deployment of control systems that manage grid inputs from both constant and intermittent sources and manage grid outputs to achieve efficiency and economy by intelligently interacting with end user devices. Given the multiple competing demands with which such a grid must cope, its complexity may well prove to be its Achilles heel. Addressing this fragility will require control system technologies that are resilient by nature and remain resilient in spite of complex interactions. The development of such technologies will underpin the basis for not only the Smart Grid, but also intelligent chemical plants, refineries and nuclear facilities where the prevention of accidents is an even greater concern than the loss of use.

State Awareness and Resilient Design

Given societal dependence on complex systems, particularly the electricity grid, utility operators, regulators, and the government are obliged to ensure efficient operations and commensurate public protections. This obligation hinges on a timely understanding of the status of generating plants as well as transmission and distribution systems. Achieving global "understanding" in this regard involves attending to sensor, communication, analysis, and decision systems, as well as the corresponding human system interfaces necessary to indicate what issues are important and why. We refer to this data-rich understanding of real-time events as "state awareness." For operators, regulators, and the government, their ability to operate the grid efficiently and protect the public depends first and foremost on a high degree of state awareness.



Heretofore, state awareness enabled reaction to anomalous events. In the case of the power grid, such events are difficult to characterize as the grid was not intentionally designed, but rather evolved from the growth and addition of new systems, units, and layers over many years. This has led to a system with sometimes unexpected and unpredictable emergent properties, as the history of recent large-scale blackouts attests. Such events are typically triggered by natural disasters, human error, or mechanical failure. More recently, utility stakeholders are increasingly concerned with expanding their state awareness to also account for malicious actors and actions. While fundamental monitoring and control principles can be applied to achieve a level of success in preventing security events, these techniques are also primarily reactive.

A key design goal for resilient control systems is a high level of state awareness that enables the transformation from reactive to proactive control of power generation, transmission, and distribution systems. The work required to evaluate and verify design resiliency is complex by its nature, involving many disciplines and roles, which in some cases compete in fulfilling their goals and responsibilities. In addition, there are often competing measures by which we determine proper operation or normalcy, which include, process efficiency and stability and compliancy, and cyber and physical security. With power systems, social measures must also be accounted for, as power outages cause immediate concern or outrage from the public and corresponding government pressure on the utilities involved. In such cases agencies as the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the Nuclear Regulatory Commission (NRC) may all play a role.

State awareness then, in addition to enabling proactive grid management, must also provide defense in depth against malicious actors and actions, and support multiple, sometimes overlapping and sometimes competing regulatory agencies. It is our contention that such a state of awareness can be achieved when resiliency is designed into control systems – when resilience is the primary design objective.

Current Research

Current resilience research is focused in two notable areas, organizations and information technology. Organizational resilience considers the ability of an organization to survive in the face of threats, including the prevention or mitigation of unsafe, hazardous or detrimental conditions that threaten its very existence. Information technology resilience considers stability and quality of service in the face of threats to the computing and networking infrastructure. Some might consider control systems that utilize typical information technology components, such as off-the-shelf-computers and IP-based networks, as just a subset of the same. However, control systems provide a whole layer of complexity not adequately encompassed within the performance of the information technology itself. This complexity derives from its interactions with critical infrastructure, where access to information, predictive control actions and automation are required to maintain safe and stable operations. As interactions grow not only in size but also in numbers, as in the power grid which interconnects between generation, transmission, and distribution, dependence on control systems is elevated. As Smart Grid technologies are added to the grid, especially control at the consumer level, not only will the interactions increase, so will the potential fragility caused by increased cyber access for malicious actors and communications latencies to feedback control algorithms. These fragilities will impact grid control systems and ultimately the grid itself unless sufficient resilience is designed in.

It has been suggested by some that “resilient control systems are those that tolerate fluctuations via their structure, design parameters, control structure and control parameters.” While this definition is broad, it does not directly consider the presence and necessity of malicious actors and cyber attack. Another recently proposed definition is “an effective reconstitution of control under attack from intelligent adversaries.” However, this definition appears to focus only on resiliency in response to the intelligent adversary. True resiliency, however, must consider what represents the proper operation of

critical infrastructure grid in the face of many upset conditions, including those attributable to threats from undesirable human interactions. Therefore, we define resilience as the capacity of a control system to maintain state awareness and an accepted level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature.

With this definition in mind, several research areas bear promise regarding control system resilience. These complement the fundamental concept of dependable or reliable computing by characterizing resilience in regard to particular control system concerns, including design considerations that provide levels of state awareness that assure the safe and secure operation of a plant or facility. These areas are presented below with discussion to provide a basis for considering resilience design and to provide a perspective on the interdisciplinary challenge of resilient control systems.

Human Systems (Human Factors Engineers specializing in control systems)

The human ability to quickly understand novel situations, by employing heuristics and analogy, can augment control system resilience. On the other hand there are situations in which we may have a general inability to reproducibly predict human behavior. This may be true in situations of fatigue or high stress or decision making under high levels of uncertainty. The literature in human reliability analysis provides an orientation regarding ergonomics, workload, complexity, training, experience, etc., which may be used to characterize and quantify human actions and decisions by Bayesian methods.

Digital technology used in human control system interactions can, from the operators perspective, provide additional clues to resiliency. For example, more information can be presented to the human operator to base a response. However, the response could be completely automated, human manipulated, or a combination of both. The dependencies and rules for these complex interactions, or mixed initiative, are not necessarily well defined or clear. Resiliency results from understanding of this complexity, ensuring through human factor and design an error tolerant control system results that complements perception, fusion, and decision making.

Complex Control Networks (Engineers and Scientists specializing in complex networks)

As control systems become more decentralized, the ability to characterize interactions, performance and security becomes more critical to ensuring resilience. While more decentralization can provide additional reliability due to implicit redundancy and diversity, it may also provide more avenues or vectors for cyber attack. Therefore, the design of complex control networks must consider all factors that influence resilience, and optimize them for multiple considerations.

Global stability is often perceived as something that can be achieved by local minimization of all process unit operations. However, there is no assurance that global stability can be achieved in this manner and, in addition, this view promotes a reactionary control paradigm by its nature.

However, considering the latencies in digital control systems, there is a tendency as well as a desire to provide faster responses when the feedback and response occur close to the point of interaction with the application. Therefore, it is suggested that a true global optimization coupled with a local interaction can achieve both the assurance of a global minima, and an acceptable response when designing control system architecture.

Cyber Awareness (Computer Scientists and Engineers specializing in cyber research)

Because of the human element of a malicious actor, traditional methods of achieving reliability cannot be used to characterize cyber awareness and resilience. The intellectual level and background of the adversary makes stochastic methods unusable due to the randomness of both the objective and the motives. However, the strength of the adversary is increased because the existing control system architecture is not random, and response characteristics are reproducible. Therefore, a resilient design can find strength in similar fashion by becoming atypical of normal control system architectural design, and appearing random in response and characteristics to the adversary.

Characterization of health or wellness from a cyber perspective is purely empirical, as prediction of the future is based on past events. While there are barriers in place to exclude known types of adversarial communication, state awareness cannot be assured because of the limited availability of diverse sensing. Determination of the actual cause of an abnormal event can only occur only after forensics is completed. Patterns or routines are analyzed and are used to provide comparisons to understand anomalies. However, while this understanding provides an interesting perspective, it may be very limited in predicting future behavior of the adversary.

Data Fusion (Engineers specializing in signal processing)

The nature of the various data types associated with proper operation or performance of critical infrastructure, including cyber and physical security, process efficiency and stability, and process compliancy is diverse. How these data are consumed to generate information will help determine whether appropriate judgments are made, whether by automated and/or human mechanisms. There are several issues that are addressed by data fusion, including the following ones:

- Reduction - The reduction of data to provide only that information necessary for the human or automation scheme to provide the appropriate response, i.e., to prevent a common issue of information overload.
- Identification - Validation and invalidation of causes for events, e.g., a process upset is due to a failed valve and not a cyber attack.

- Improved characterization and knowledge - Development of new information that helps to better characterize the process application, e.g., mining of process temperatures along with process flows provides a better interpretation of stability.

While many of the techniques required to perform data fusion are well known, their application to the diverse types of data represented within the measures of performance provide a distinct challenge. This is nowhere more evident than the fusion of cyber and process data to not only indicate whether an event is cyber specific, whether due to an adversary or network problem, or actually represents a process upset. The effort to address this situation could be split into two parts: i) developing the appropriate data to characterize the cyber threat, and ii) combining the spatial and temporal aspects of both process and cyber data to confirm the cause of the process upset.

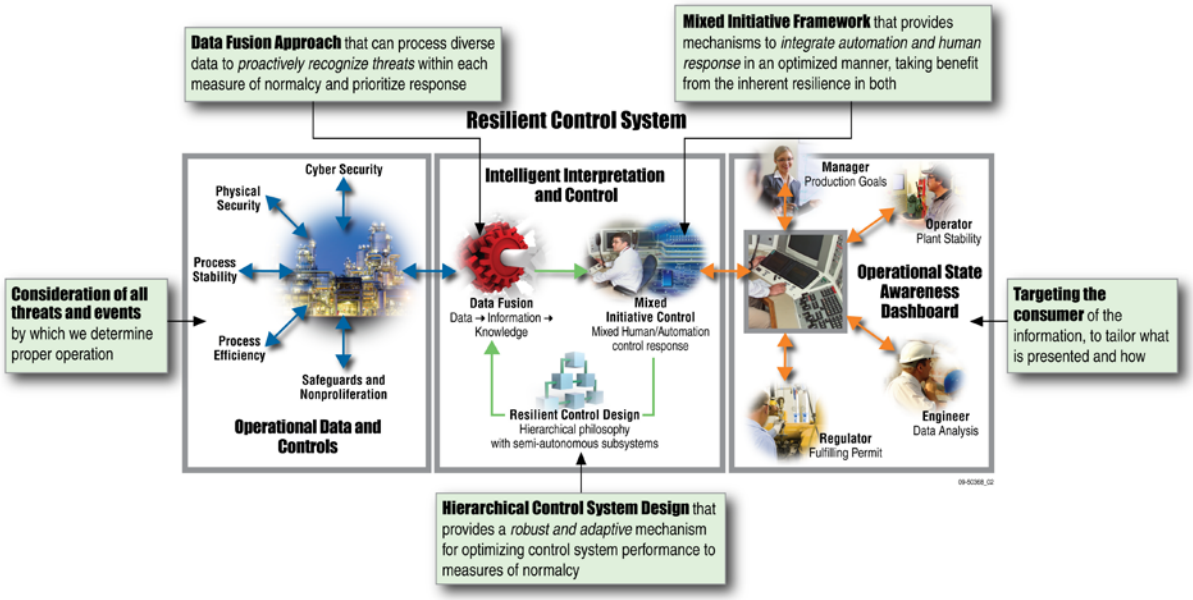
Proposed Research Areas

In considering resilience above, we discussed the importance of state awareness and the role of resilient design in achieving it. Without state awareness of the grid and its complex interactions, there can be no hope of ensuring that any problem or fault is recognized and responded to efficiently and effectively. Software failures, such as those blamed for the August 2003 northeast power outage, are unacceptable to the public, and what's more, will not promote the trust necessary to implement Smart Grid technologies. Without designed in resilience, control system architecture must reflect that of a decentralized system. Such systems would not provide adequate state awareness but would cause unnecessary delays that would also undermine trust of the Smart Grid by both consumers and power vendors alike. A clarification of these research areas follows.

State awareness

In defining state awareness, one must reflect on the fundamental reasons for installing a control system in the first place. From a monitoring standpoint, these control systems are expected to provide a sufficient knowledge of operating parameters that represent a basis for decisions. However, there are a number of measures that are based on the uses of the data, which also provide the basis for establishing performance requirements. From the smallest to the largest control system, maintaining a state awareness of everything that can affect its normalcy must be performed. These measures have previously been identified as cyber and physical security, process efficiency and stability, and process compliancy.

However, gaining state awareness is more than having all the appropriate sources of data. What the consumer of the data really requires is the information necessary to maintain the normalcy of the control system, within the limits of authority that have been provided to him. This requires focusing and prioritizing information based upon an intelligent fusion of data. Intelligent fusion not only reduces the level of information provided to the consumer, but also generates data better characterizing the awareness state space via observers and predictors.



Resilient design

Resilient control system design complements traditional considerations of reliability and dependable computing, which are well established research areas. However, while reliability design brings with it the fundamental considerations of platform operations and communications with no particular focus on the use of the platform, resilient design must consider the attributes that are particular to control systems. Resilient design provides a paradigm shift on how we look at control system design, where traditional redundancy would have been implemented based on a particular vendor's perspective on reliability design. These designs find their basis in the characterization of reproducible and understood events, and while applied to control systems, similar concepts could equally be applied to many types of microprocessor-based applications.

The concepts of safety instrumented systems have taken a step toward considering elements of control system design that are unique to the process application. For example, the control system and its function to prevent unsafe conditions in the process application are considered when determining probability of failure. In a traditional sense, component failure alone was the concern. However, to be resilient, there are notional ideas that come from the areas of resilience already discussed. In human systems, the unpredictability of human performance threatens resilience, while the innate ability to adapt reinforces resilience. Similarly with cyber awareness, the unpredictability of the attacker threatens resilience; however, in this case the ability to adapt is also an added threat. With complex networks, latencies and disruptions in communications may affect the stability of coupled control loops, negatively impacting the resilience. These threats to resilience, considered specifically in regard to desired operation of the process application, form the paradigm under which resilience in the context of this paper and research finds its basis.

In providing monitoring and control capabilities, the basic element of a control system is its underlying feedback control loop, which may be hosted on many communicating platforms, including transmitters, converters, logic solvers, and operator displays. How these elements are build into an integrating architecture can vary, especially when considering next generation resilient designs. In identifying the best method, however, the considerations of complex network design are necessary to build and optimize the interactions of the various elements. When the human elements are considered within this architecture, the purpose of data fusion can be realized. Data fusion is normally considered a method to concentrate or combine data to yield information and knowledge, which in this case provides state awareness and the basis for decisions. However, while the principles of data fusion as described provide a more focused perspective to provide more resilience to the friendly human, by their nature these principles can also be "reversed," so to speak, to provide the contrary results. It is this perspective that is needed to counteract the negative impact on resilience brought by the malicious actor trying to undermine a control system. Therefore, it is desired to increase, not decrease, the confusion of the malicious actor by undermining his understanding of the control system.

The Need for Collaborative Research

Considering resilience from both interdisciplinary and research maturity perspectives, the magnitude of this task is clear. While resilience-related research is underway, a formal interdisciplinary research strategy is needed. In this regard, an annual IEEE symposium on resilient control systems was initiated several years ago, including stakeholders from government, academia and industry, as a forum to discuss collaborative strategies. Our discussions suggested that from a cost perspective, the control system industry will be hesitant to risk capital to design resilience into control systems. Even worse, if an individual company were to make the investment, the results would likely be proprietary and considered a market differentiator from its competitors. A new government-industry-academic collaboration is therefore suggested, where many will ultimately share in the knowledge learned and distributed through standards, design specifications and prototypes.

The national laboratory system is intentionally designed to integrate research and technology and to build the collaborations necessary for shared deployment. Through such programs as the National Supervisory Control and Data Acquisition Test Bed (NSTB) of the Department of Energy (DOE), teaming has proven possible and productive. This and similar programs under the Department of Homeland Security (DHS) have been primarily focused on mitigating current vulnerabilities, while limited research under the National Science Foundation (NSF), DOE, and DHS has been proposed or funded to look at new control system architectures. This research will provide the underlying technology to enable a Smart Grid, and produce the next generation of control systems that will be required to safely and securely control our transportation systems, chemical plants, nuclear power stations and other critical infrastructures.

Establishing Resilience

For proper life cycle development and implementation of resilient control system technologies in the power grid and other critical infrastructure, a guiding body of stakeholders and a representative test bed are required. As we noted above, a consortium of industry, government and university is proposed to guide research and establish standards for acceptance. Universities could support basic resilience research and underpin both evolutionary and revolutionary advances. Industry includes two distinctive, but important elements, the asset owner (day-to-day operational requirements) and final recipient of such technologies and the vendors of equipment. The owners provide a critical perspective on the needs for operation, both the concerns and expectations. The vendors provide a perspective on where current system technology is and the final implementation of the resulting technologies. Government provides two distinct functions. Citizens turn to the government to ensure that their best interests are served and that the critical infrastructure is safeguarded against loss of service, or in the case of a hazardous facility, catastrophic events. The second government function entails the need for integration of not just technologies, but also the development of methods that assure benefit and confirm quality.

The development of resilient control system designs provides the opportunity to develop technologies that are of direct benefit to current designs. These next generation designs will require interdisciplinary research and development, as well as integrated testing on both a pilot and full scale basis to demonstrate solutions. This integrated approach ensures the development of resilience from a practical standpoint, and insures the interoperability of infrastructure components, a common complaint when renewable generating sources are added to the current power grid. Decomposing the elements of resilience, the human aspect, both benign performance issues and malicious action, and complex interdependency aspects, both characterized by a need to fuse diverse data into information and model the interactions, suggest the interdisciplinary makeup for the team necessary to address this challenge. Recognizing this need, INL has an established research programs targeted specifically toward addressing resilience solutions in tightly coupled environments with hybrid energy systems to allow for unique approaches to powering the grid. However, a significant commitment on the part of the government to ensuring grid resilience and the development of renewable technologies in a fashion that allows efficient grid integration will speed the emergence of the Smart Grid.

Sources:

Available upon request.