Wide-area situation awareness in electric power grid

Frank L. Greitzer*
Pacific Northwest National Laboratory, 902 Battelle Blvd., Richland, WA USA 99352-0999

ABSTRACT

Two primary elements of the US energy policy are demand management and efficiency and renewable sources. Major objectives are clean energy transmission and integration, reliable energy transmission, and grid cyber security. Development of the Smart Grid seeks to achieve these goals by lowering energy costs for consumers, achieving energy independence and reducing greenhouse gas emissions. The Smart Grid is expected to enable real time wide-area situation awareness (SA) for operators. Requirements for wide-area SA have been identified among interoperability standards proposed by the Federal Energy Regulatory Commission and the National Institute of Standards and Technology to ensure smart-grid functionality. Wide-area SA and enhanced decision support and visualization tools are key elements in the transformation to the Smart Grid. This paper discusses human factors research to promote SA in the electric power grid and the Smart Grid. Topics that will be discussed include the role of human factors in meeting US energy policy goals, the impact and challenges for Smart Grid development, and cyber security challenges.

Keywords: electric power grid, Smart Grid, situation awareness, wide-area situation awareness, cyber security

1. INTRODUCTION

The Secretary of Energy emphasizes two important elements of US energy policy: demand management and efficiency, and renewable sources.[1] These policy elements can be facilitated by Smart Grid development to "lower energy costs for consumers, achieve energy independence and reduce greenhouse gas emissions."[2] A key element of Smart Grid implementation will be real time information transparency for all operators.[3] In practice, this capability is referred to currently as wide-area situational awareness.[4] Research in this area has been supported by the DOE Office of Electricity Visualization and Controls (V&C) program. The recently published FERC policy statement[4] further delineates specific areas in requiring development of interoperability standards to ensure smart-grid functionality, including wide-area situational awareness (SA). The National Institute of Standards and Technology also identified wide-area SA among eight priorities for Smart Grid interoperality.[5]

This paper discusses human factors research needs to promote SA in the electric power grid and the Smart Grid. Topics that will be discussed include the role of human factors in meeting US energy policy goals, the impact and challenges for Smart Grid development, and cyber security challenges. We describe domains of human factors research needs and approaches to human factors research and development. Critical elements of human factors research in this area include viewing the increasingly complex power grid within a system-of-systems framework; the need for user-centered design of wide-area SA tools rather than a more traditional technology push of adapting visual graphics techniques to displayable parameters; and application of cognitive engineering methods to facilitate effective design and deployment of visualization tools.

1.1 Background

The electric infrastructure in the United States has been called the most complex machine on earth[6], yet it is by most standards antiquated since it was designed over 50 years ago. Despite this, consumers have implicit trust in the technology, even though the failure of the electricity infrastructure would lead to significant disruption of people's lives, industry and commercial activities, and result in massive economic losses. Recent power grid blackouts, such as the west coast blackouts of 1996 and the east coast blackout of 2003, brought significant attention to the reliability of power grids.[7,8] How to predict and prevent or mitigate such blackouts has been a central topic in the area of power system research, and has also become one of the primary focuses of the DOE Office of Electricity Delivery & Energy Reliability (DOE-OE).[9]

*frank.greitzer@pnl.gov; phone 1 509 372-4251; fax 1 509 375-2443; http://www.pnl.gov/cogInformatics

Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, edited by John F. Buford, Gabriel Jakobson, John Erickson, William J. Tolone, William Ribarsky, Proc. of SPIE Vol. 7709, 77090F · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.855674

Because of the complexity, wide geographical coverage, and dynamic/nonlinear behaviors of its numerous network configurations, operation of the electricity infrastructure is an extremely challenging task. This is compounded by a number of external factors including physical attacks, cyber threats, human errors, and natural disasters. To respond effectively to emergency situations, operators must be able to process and understand large amounts of data to gain adequate SA; yet in current practice electricity infrastructure operation is largely based on the operator's experience, with very limited real-time decision support.

Modernizing the country's electrical grid is an urgent national priority. Implementing new Smart Grid technologies will help to revolutionize the production, transmission, and consumption of energy in the United States, and will impact every home and business connected to the electric grid. The Smart Grid uses intelligent transmission and distribution networks to deliver electricity. By providing two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning, the Smart Grid is expected to improve the electric system's reliability, security, and efficiency. Enabling technologies include smart meters, standards, and protocols that will help transform the current centralized, producer-controlled network to a decentralized, consumer-interactive network supported by fine-grained monitoring.[10] For example, consumers react to price signals (that is, supply) with the help of smart meters to achieve active load management. On the monitoring side, smart meters that collect data every minute will replace systems that record metering data hourly or monthly. Similarly, current supervisory control and data acquisition (SCADA) systems collect one data point every 1 to 4 seconds. Some data types may only be collected once per minute, whereas newer technology enables collection via phasor measurement units (PMUs) at rates of 30 to 60 data points per second.[11]

The distributed control and monitoring technologies of the Smart Grid will extend control to consumer equipment such as generators and office or home appliances. This distributed architecture and unprecedented amount of information about devices connected to the network are expected to save energy, reduce costs, and improve reliability of the electric grid, and increased volume and timeliness of information are expected to promote real time information wide-area situation awareness.

Implementing the Smart Grid is expected to make the country's energy system more resilient and prepared to address emergency situations such as hurricanes, ice storms, or terrorist attacks. Today, energy disruptions like blackouts can lead to a cascading series of failures; in contrast, Smart Grid technologies are expected to reinforce security protocols and better detect and isolate power outages and contain rolling outages.

1.2 Critical needs and technical gaps

With these benefits come possible risks and vulnerabilities. The implementation of the Smart Grid may cause information congestion, increase the possibility of cyber attacks and misoperation, and lead to cascading failures propagating from one system to another. More data do not mean more information. Increased volume and complexity of data may exacerbate human performance difficulties and lead to information overload and degraded decision making unless human factors issues are addressed. Two-way communication and interactive functions increase the potential for cyber attacks, loss of consumer security and threats to privacy. Possible consequences include power system blackouts, smart-grid IT infrastructure failures, energy market chaos, damaged consumer devices, endangered human safety, loss of trust in the energy infrastructure, and less severe but more frequent incidents such as smaller-scale outages. These needs and technical gaps are summarized as follows:

- High volume of data yields challenges for human-system integration to ensure design of displays, visualizations, and SA tools that facilitate real time information transparency and SA for all operators.
- Integration of a multitude of end-use devices with various vulnerabilities, data formats, security protocols, etc., poses risks and questions about whether the Smart Grid can resist attacks without causing damage to equipment, infrastructure, or leading to blackouts.
- Two-way communication and visibility into use and status of consumer equipment offers unprecedented opportunities for consumers to gain an awareness of their energy use habits, but it also may afford increased risk of data exploitation, loss of privacy, and opportunities for cyber attacks.

It is crucial to fully engineer the data collection capability provided by the Smart Grid infrastructure to build a trustworthy system that preserves data integrity and privacy and to design display, visualization and decision support systems that promote effective decision making through wide-area SA.

2. CYBERSECURITY CHALLENGES

Vulnerabilities of the power grid have been recognized for many years. The President's Commission on Critical Infrastructure Protection observed in 1997 that the widespread and increasing use of SCADA systems has increased the ability to cause serious damage and disruption by cyber means.[12] Simultaneous attacks on a few critical components of the grid could result in a widespread and extended blackout; and a grid collapse with cascading equipment failures could lead to an even larger, longer-term blackout.[13] Serious concerns have been raised about whether the Smart Grid can resist attacks and heal itself without causing infrastructure and equipment damage or large-scale blackouts.[10] Ensuring cyber security of the Smart Grid is a critical priority, recognized by NIST in its *Framework and Roadmap for Smart Grid Interoperability Standards*.[5] NIST asserts that Smart Grid cyber security requires incorporation of security at the architectural level, and a NIST-led Cyber Security Coordination Task Group[14] is leading the development of a cyber security strategy and cyber security requirements for the Smart Grid. The Task Group aims to identify risks, vulnerabilities, threats and impacts; to develop security architecture; and to document security requirements. Challenges arise with the integration of cyber and physical systems, and with impacts of factors such as human behavior, commercial interests, regulatory policy, and even political elements.

2.1 Cybersecurity vulnerabilities for the Smart Grid

Khurana et al.[10] suggest that cyber security challenges for the Smart Grid will be similar to those of traditional networks, except they will involve more complex interactions. Among the Smart Grid cyber security vulnerabilities that Khurana et al. discuss are the following issues:

Trust. For control systems, trust is reflected in the confidence that, during some specific interval, the appropriate user is accessing accurate data, created by the right device at the expected location at the proper time; communicated using the expected protocol; and that the data has not been modified.

Communications. With the traditional electric grid serial communications giving way to increasing numbers of smart-grid deployments that use less reliable Internet and broadband communication, the communication and control environment becomes less deterministic and secure. This issue is compounded by the rapid deployment of smart-grid systems without adequate security (including physical access controls) and reliability planning. Two-way meters and automatic meter reading (AMR) environments also present potential for data integrity or security vulnerabilities since a customer or an adversary can directly access the meter or home area network.

Privacy. Historically, the electric grid's security objectives have been availability, integrity, and confidentiality. However, as the grid incorporates smart metering and load management, privacy is increasingly becoming an issue. Electricity use patterns could lead to disclosure of not only how much energy customers use but also when they're at home, at work, or traveling. This information could be exploited by compromising either the customer's home area network or the AMR network—not only by criminals planning a break-in, but also by entities interested in gaining "intelligence" about types of appliances and devices that are present.

Scalability. With the Smart Grid, both the volume of data and the number of devices with which a utility communicates will likely increase by several orders of magnitude. This presents challenges for maintenance, trust management, and monitoring of cyber intrusions. Devices currently planned for monitoring and controlling the Smart Grid might not have the processor cycles and memory to support cryptographic computations involved in security authentication. For example, Khurana et al.[10] conclude that for a utility company with 5.5 million smart meters to update each device even as little as once a year would require processing an average of 10 security certificate pairs every minute; this is not possible with current technology, nor is it feasible for the utility company to employ the required number of support staff (in excess of 5000) who would be needed to monitor that many security certificates.

2.2 R&D implications

These challenges pose several R&D needs and implications for cybersecurity technology to support the Smart Grid.

Identifying and characterizing the risk. What data may be collected or created that can reveal information about individuals or activities within specific premises (both residential and commercial)? How might this information be exploited? What policies and practices are needed to identify and mitigate risks? The needs and priorities surrounding issues of confidentiality, data integrity, and availability are typically in competition. For example, making sure power is available whenever it is needed is usually more important to consumers than ensuring confidentiality of power flows.

Data processing capability. The enabling of two-way communication and control networks in power distribution networks, more PMUs in the transmission networks, and the increasing information exchanges among various user groups provides an explosion of information that bears different data formats and time stamps, with or without secured information interchange mechanisms. When considering needs for efficiency and scalability, the electric grid has varying real-time requirements that make efficiency essential—which argue for an R&D priority aimed at increasing throughput and development of predictive analysis to enhance SA and decision making. The increasing number of devices and their interactions point to the requirement for research aimed at addressing scalability.

Cyber security and equipment failure. The massive use of low-cost communication and electronics may leave the network without a complete, secure set of information interchange mechanisms. The Smart Grid needs a supervisory system that can efficiently process a myriad of data to evaluate system status, identify failures, predict threats, and suggest remediation. Research must address the need for adaptive systems that can evolve to meet changing needs in a dynamic cybersecurity environment.

Interoperability. Through digital and information technology, the Smart Grid allows close interaction and interoperation of the transmission and distribution grid, building and house controllers, and distribution generation. These devices must be able to interoperate through reliable and efficient exchange of information. There is a need for research in cybersecurity technology and solutions to improve authentication capability and analysis of data integrity, which ultimately enhances the trustworthiness of the power grid.

3. APPLICATION OF HUMAN FACTORS METHODOLOGIES

The final report on the August 14, 2003 blackout pointed out that SCADA networks to other systems introduced vulnerabilities and systems lacked visibility of operations in surrounding areas. The lack of wide-area SA was a contributing factor for the 2003 blackout.[15,16] This was a "wakeup call" for the power industry that elevated the need to apply human factors methods to improve processes, displays and visualizations that support power grid control and management operations. The current decision making environment for grid operators tends to focus on centralized hierarchical control, involving dispatch control for bringing generation on or off-line. As the load control task changes with development of Smart Grid systems, and the increased linkages of wide-area resources, the concept of "system-of-systems" becomes increasingly important in power systems. In systems-of-systems, traditional human factors concepts and design methods are challenged due to multi-owner/multi-mission considerations, incompatible human-system interfaces, operating modes, operator capabilities, underlying infrastructure, and mission criticality.[17] Decision support in electric grid systems-of-systems will need to address the multiple concerns of grid operators, managers, power marketers, public authorities, and the consuming public.[18] Visualization tools to be developed within this context will require blending systems engineering perspectives with traditional human factors approaches and concerns. Here we describe human factors issues, challenges and methods to address the various needs for secure systems, data integrity, efficient monitoring and control, and privacy/trust for the power grid of the future.

3.1 Transforming data into information

Currently there are hundreds if not thousands of displays to be reckoned with in power grid control operations. Power system operators and decision makers are already overloaded with data; more data will be available in the future, but rather than burdening operators with more data, we must transform the data into information that supports and alleviates the processing load of human decision makers. This implies that information analytics and displays, visualizations and other forms of operator support must be designed to enhance performance of the overall system (or system of systems) that the human must oversee and for which humans are ultimately responsible.

Most displays comprise tabular data, although there are other forms of information presentation such as graphs and more typically, electric grid "wiring diagrams" that show connectivity, voltages, and other status information. Studies of displays and visualizations for power grid operation are continuing to identify possible alternatives to tabular displays that are difficult to use, but as yet there have been few definitive studies or development efforts to introduce or validate prospective solutions for deployment. An ongoing study of a small subset of operational displays in normal and emergency operations (conducted by the author and colleagues at the Pacific Northwest National Laboratory) reveals little commonality in display design and organization of information. Display design and human factors guidelines demand that information displays, aids, and visualizations must support the process flow. Power grid displays provide a loose connection to process flow and make great demands on operators to maintain SA.

Design of effective visualization tools for power-systems operation requires a systematic approach that is focused on facilitating and improving overall performance at multiple system levels, across a range of operational personnel. A structural-operational view of the electricity infrastructure is needed so that the operation of new visualizations can be examined in the larger context, specifically their ability to aid in the achievement of high level goals, i.e., a "top down" approach. By mapping the operations of a visualization tool to the highest level goals, through multiple intermediate steps, it will be possible to examine the interdependencies within the operational environment.

3.2 Applying human factors methods to improve situation awareness

Traditional human factors research informs design and development of user "transactions" with the computer with guidelines for effective user-computer interface designs. In the future, a greater emphasis must be on the design of effective visualizations for normal and emergency operational decision making—techniques that enhance understanding and promote SA. We will have failed to meet future needs for more efficient and effective power grid control if we merely add to the number of displays to be monitored and digested by human operators.

Analyses of blackouts[15,16] indicate that lack of SA is an underlying problem, but it is important to explore this in more detail, both in terms of problem areas and when awareness seems to be functioning properly. This can be approached with the human factors technique of cognitive task analysis, which is an extension of traditional task analysis techniques with an aim to incorporate cognitive constructs.[19] Representation of the information gained from cognitive task analysis can take a variety of forms, including variants of network diagrams, flow charts, operational sequence diagrams, concept graphs and timelines, as well as analysis of communications among distributed decision makers. Cognitive task analysis is often applied to retrospective analysis of activity logs or structured interviews in which researchers request that operators recall and describe specific cases/instances in which they were particularly successful at solving a problem. A taxonomy of approaches to system design, visualization/displays and decision support systems has been described to help organize discussions of R&D needs for future power grid operations and control centers.[20]

The focus of most visualization research that was stimulated by the 2003 blackout has been on developing new and better techniques for displaying data—a "technology push." This general trend has led to a proliferation of techniques and tools, but much less understanding of end-user operational tasks that need to be supported. The result, unfortunately, is a collection of software tools that fail to meet user needs and that are, consequently, underutilized. The North American SynchroPhasor Initiative—after failing to identify any clear benefits of the rapid and voluminous measurements available—stated that the first task in its strategic plan is to identify such benefits and convey them convincingly to utility and reliability coordinator executives.[21]

A human factors framework that appears to offer particular insights into power grid decision making is naturalistic decision making. This perspective on decision-making arose from studying how people use their experience to make decisions in real-world settings. The research focus is on how experienced people identify and assess the situation, make decisions and take action in dynamic, uncertain, and often fast-paced environments.[22] Within this framework, the Recognition Primed Decision Making model proposes that decision makers draw upon their experience and ability to recognize similar situations to develop a single course of action with plans for contingencies.[23] Because much of the decision making process is not observable, cognitive task analysis is used to understand the decision maker's prior knowledge and the thought process used to arrive at a course of action.[19] A relatively new approach to assessment of grid operator performance applies cognitive decision models and naturalistic decision making approaches, using mental models and other cognitive "artifacts" that may be observed or extracted from behaviors or decisions.[24] The processes and principles of Recognition Primed Decision Making and SA were combined into an integrated decision making model, which could be tested using cognitive task analysis methods.

Research conducted within our Laboratory in consultation with stakeholders from the electric utility industry applied human factors and cognitive task analyses to the analysis of dispatcher displays and processes. We worked with operators and stakeholders to select an appropriate "event" to study and we examined the current set of processes, procedures, and associated displays. This human factors analysis produced specific recommendations to improve processes, displays and visualizations that are expected to improve operator SA and efficiency of operations. In follow-on research that is planned, we hope to document and verify expected improvements in the process by estimating time saved in certain parts of the decision process (e.g., identifying the problem, analysis of alternative actions, implementing solution) that may be further extrapolated to identify potential cost savings (e.g., by reducing or avoiding monetary sanctions).

3.3 Development of advanced technology solutions to enhance decision making

Advances in technology that enable increased automation will lead to changes in the responsibilities of humans in the loop. Systems with little or no automation require that the human operator be intimately involved in monitoring and control functions, while also responsible for higher-level decision making tasks that use cognitive processes. High information processing demands on the human operator leave little time for such cognitive/decision making tasks. Automation typically has focused on relieving the human operator of intensive signal processing functions, which allows the operator to devote more time to decision making. The result is to shift the responsibility of the human toward more supervisory functions. In electrical power operations and control, the role of automation is to filter, preprocess and analyze data, while the role of the human operator is increasingly focused on the more cognitive task of *synthesize*, *plan*, and *decide*. Of paramount importance in this advanced information processing environment with the human in the role of supervisor is the need for the human to maintain SA.

Electricity infrastructure operation involves complex computational processes with complicated power grid models. One of the most difficult decision making functions is contingency analysis, which examines "what-if" conditions in anticipation of potential power grid failures. Contingency analysis identifies operational violations if one or more elements fail. Today's commercial tools use tabular displays of the contingency violations, where each violation is represented by a row. Such displays do not show the severity or the geographical context of the violation and the contingency resulting in this violation. While this may be adequate when there are only a few contingencies, tabular displays become overloaded when the system is heavily stressed with significantly more contingency violations. Under such conditions it is impossible for an operator to sift through the large amounts of violation data to gain an understanding of the situation within several seconds or minutes. Automated aids for contingency analysis are being designed to help relieve this heavy cognitive burden on human operators. PNNL has developed a collection of analysis tools and displays/visualizations to improve performance by enhancing SA and understanding of the system state, possible contingencies, and a ranked presentation and visualization of alternative courses of action to address the contingencies.[25,26] PNNL's Graphical Contingency Analysis tool supports contingency analysis by improving SA through analysis and visualization of risk levels; analyzing patterns of impacts to predict future states; and assessing effects of alternative response options through interactive analysis of severity levels and impacts. This real-time decision support reduces the operator's need to review massive amounts of data and presents timely and actionable information on current status, system trends, and alternative actions. Simulation-based studies are currently being designed to evaluate the effectiveness of the decision support and visualizations provided by the Graphical Contingency Analysis tool.

3.4 Maintaining operator skills

Providing reliable electricity is an enormously complex technical challenge, even on the most routine of days. It involves real-time assessment, control and coordination of electricity production at thousands of generators, moving electricity across an interconnected network of transmission lines, and ultimately delivering the electricity to millions of customers by means of a distribution network. To meet the demands and expectations of this industry, effective training and maintenance of a high level of mastery are required of the system operators and decision makers. Prior to the blackout of August 14, 2003, only a small fraction of power system operators had ever trained with realistic operator training simulators. Following the blackout, the North American Electric Reliability Council Emergency Operations Recommendation No. 6 required that all reliability coordinators, control areas, and transmission operators provide at least five days per year (in addition to other training) of training and drills in emergencies, *using realistic simulations*, for each staff person with real-time operation or reliability monitoring responsibilities.[27]

It is also important for the utility community to appreciate the changing demographics of electric grid operators. In the past, operators typically had field experience as linemen and tended to move up in the organization to operational positions as dispatchers and reliability coordinators. This career path provided a level of experience that is not available to more contemporary operators who hire into the organization as power grid operators, lacking field experience. Changing experience and background of operators produces challenges for the industry to facilitate preservation of "corporate knowledge" and to instill both theoretical and practical knowledge through more effective training and on-the-job experiences.

To develop and maintain sharp skills, more effective training approaches are needed across the industry. Traditionally, power system operator learning objectives are specified only at a general level, such as "the operator will demonstrate skills in interpersonal communication protocols in multi-balancing authority coordinated operations." Based on the selected problem area and learning objectives, a training scenario is developed that includes problems that exercise the desired skills. In contrast, when informed by the more specific and rigorous concepts and performance criteria available in cognitive task analysis and naturalistic decision making approaches, a detailed and systematic training plan may be developed to take account of the mental processes that come into play when making critical decisions. Using the naturalistic decision making framework, the approach focuses on the operator's demonstration of understanding (or lack of understanding) of requisite cues, patterns, mental models, action scripts, etc.[24] That is, instead of reacting to relatively gross behavior or outcomes, the trainer has specific guidelines or behavioral/performance indicators that identify possible deficiencies. With this information, the trainer may choose to interrupt the exercise immediately to discuss problems, or note performance gaps and review the incorrect or missing concepts in an after-action debriefing. In this way, training will progress more efficiently, and with an enhanced ability to identify deficiencies and enable greater transfer of training. To facilitate this type of training, high fidelity simulation environments are needed. Simulation is the best training approach for developing and maintaining skills needed to keep the electric grid running reliability.[28] Simulated environments are risk-free, enabling learners to integrate theory and practice without fear of causing system reliability issues. From a cognitive learning point of view, simulation provides a unique modality and environment for experiential learning in an active and immersive learning environment.[29]

4. RESEARCH ROADMAP

The following research priorities may be gleaned from the foregoing discussion:

4.1 Develop a more robust definition of wide-area SA to drive interoperability standards and inform tool and visualization design.

Situation awareness as a concept was borrowed originally from a military context, and migrated into many other areas that engage human operators in dynamic processes. It has typically been studied at the individual level as this is the most tractable for experimentation and measurement. However, the concept of wide-area SA implies more than breadth of information for a single operator; it also implies a "shared representation" of grid functioning among multiple personnel at different locations and organizational levels.

The lack of standardization among energy management systems has much potential for confusing and contradictory representations of grid functioning. The activities envisioned in this analytic area involve developing a much more robust definition of wide-area SA that can be used to drive interoperability standards for software systems. This will include not only what to display, but how to display it, and to whom and under what circumstances. We envision this activity to be an on-going, multi-year process, culminating in FERC guidance for wide-area SA interoperability standards.

4.2 Conduct research to increase our understanding of the "shared representation" aspect of wide-area SA for groups of decision makers.

As observed above, wide-area SA should transcend the boundaries of a single operator. Research on team SA reveals factors that influence performance, including the complexity of the system, distribution of equipment and systems across physical locations, and the number of required concurrent tasks.[30] Additional research, especially simulation studies that may be more tightly controlled, should be performed to examine the ability of team members to exchange information, observe/identify deviations in SA across team members, and the extent to which team members demonstrate awareness of an overall, shared goal. In the fall 2008, PNNL conducted a distributed exercise involving multiple cooperating organizations operating out of four geographically dispersed locations, with operators engaged in a complex simulated "blackstart" scenario that required shared awareness and effective communications.[24] This study, which was run from the PNNL Electricity Infrastructure Operations Center (EIOC), demonstrated not only the capability to perform distributed operational exercises but also the application of human factors methods to analyze communications and infer mental models that could be used to test the extent of shared representations and wide-area SA. More collaborative/distributed exercises of this nature should be conducted.

4.3 Develop effective paradigms and test environments in which to conduct evaluations of selected tools and visualizations

Simulator-based study of SA tools is needed to assess the resilience of decision support and visualization software under more challenging conditions than is possible in typical laboratory experiments. Earlier developmental testing will have demonstrated the ability to enhance SA in scripted conditions; more challenging testing in simulators will be necessary prior to deployment in field demonstrations. The principal issue is to ensure that the tools are not brittle, i.e., only able to function under very constrained conditions, but instead show resilience through the ability support a broad range of simulated operating conditions. It is important that simulation studies focus evaluation both on the individual and team level of performance (team in this case being the wide-area hierarchy of Reliability Coordinator—Balancing Authority interactions). Individual evaluation measures should focus on handling a large information load, accuracy of mental models of the situation, and ability to correctly diagnose and manage off-normal or contingency operations. This type of simulation environment offers a safe setting for researchers to work through the iterative process of developing and refining technology more quickly. It may also be used by the U.S. Department of Energy and government agencies to test solutions and assess the potential benefits of technologies, or by utilities to solve a particular problem. The PNNL EIOC, mentioned above, represents a significant advance in the research strategy of producing a high-fidelity, realistic simulation and test bed environment. The EIOC[31] brings together industry software, real-time grid data and advanced computation within a functional control room that is superbly suited for power grid simulation-based research. The EIOC allows researchers to work with real data—running scenarios to determine how to increase capacity and improve reliability models, and testing new technology, without the cost and risk of disrupting an operational control system.

Beyond the need for sophisticated test beds for evaluation research, there is a need for rigorous and systematic evaluation methods. Evaluation studies are needed to assess the effectiveness of proposed process improvements, user interface design or visualizations, and decision support/automation solutions. Experiments must be designed to compare effectiveness of candidate solutions within realistic simulation environments, and performance metrics are needed to support these experiments. As has been noted earlier, development of performance measures and metrics should focus on measuring performance under high workload, assessing accuracy, accounting for mental models employed by decision makers, efficiency in diagnosing and addressing off-normal or contingency operations, and extent of shared representation among members of distributed teams.

4.4 Research on improving detection and prediction of risks to Smart Grid wide-area SA and security

To produce a trustworthy Smart Grid, it is necessary to reduce the potential for information congestion as well as the risk and cost of cyber attacks or operational failures. We must fully utilize smart grid data collection capability to support analysis of correlations and interdependencies among data sets originating from different sources. Confining analysis of one type of data from one source does not reveal interdependencies; a higher-level, structured reasoning process that examines multiple layers of the grid architecture will enable multi-layer triggering of alerts relating to issues such as data overflow, cyber security breaches, and processing of data redundancy to enable cross-checking for data integrity or abnormal behaviors. Because the same device may be measured for different purposes, and the measurements are sent to operators through different communication networks, cross-checking enforces data authentication and increases the credibility and reliability of decisions.

Ongoing research at PNNL is focusing on predictive analytics and modeling to simulate physical and cyber security threats in the distributed communication and control network that forms the information infrastructure of the smart grid. The research is developing a predictive defense model that identifies threat patterns, predicts the threats, and takes action based on potential impacts on power grid reliability and stability to remove, prevent, or mitigate the threats. The approach involves developing information filters to generate threat patterns, conducting multi-layer reasoning to synthesize information, and generating automated reactions to triggered threat levels. The predictive analysis is conducted by a reasoning system that will help grid operators identify the nature of bad data, outages, and security incidents and assess security threats by cross-checking data collected from SCADA systems, PMUs, smart meters, and other control and communication channels to detect or anticipate data integrity problems and abnormal (suspicious) behaviors.

4.5 Additional research questions

A collection of research and/or engineering questions relate to system architecture decisions, such as the number of smart grid "monitors" (e.g., in-home units, smart-meters, meter data management systems) to deploy and determining the best time interval to be used for sampling data. Scalability challenges may be addressed by distributing to end-devices more hierarchical, intelligent processing functions that will help to reduce the volume of data processing.

Finally, there are questions that need to be addressed in the area of human factors and consumer research from an end-user/consumer perspective. Where are the best places to locate the smart-meters—inside or outside of houses, for example? What are design issues for such devices—how they will work, what level of user experience/capability is assumed? Usability studies are needed to test ease of use and user acceptance. What are implications for system design of public and consumer perceptions of privacy and security surrounding use of smart-meters that will allow unprecedented visibility of consumers' energy use habits? An example of a research project that sought to gain a better understanding of consumer behavior and preferences in this context is the GridWise™ Demonstration project, funded primarily by the Department of Energy and conducted by PNNL in 2006. Through this research, insight was gained into energy consumers' behavior by testing new technologies that gave homeowners more information about their energy use and cost, and by monitoring their energy use to see if this information would modify consumer behavior.[32] Continuing research in this area will help to ensure that Smart Grid technologies will be designed and deployed in ways that will be accepted and used by consumers.

5. CONCLUSIONS

Development of the Smart Grid seeks to achieve US energy goals of clean, reliable, and secure energy generation, transmission, and distribution by lowering energy costs for consumers, achieving energy independence and reducing greenhouse gas emissions. A research roadmap for the electric power industry to facilitate the transformation to the Smart Grid and produce effective and secure operational and decision processes for the Smart Grid involves the following high level research needs:

- Research should focus on developing a more robust definition of wide-area SA to drive interoperability standards and inform tool and visualization design.
- Research is needed on team or group decision making in power grid operations to increase our understanding of the "shared representation" aspect of wide-area SA for groups of decision makers.
- Research should focus on development of effective paradigms and test environments in which to conduct evaluations of selected tools and visualizations.
- Research in human factors and consumer behavior should focus on issues of system effectiveness and usability from the consumer's perspective to ensure that smart-meters and other consumer devices are easy to use and acceptable from a security and privacy standpoint.
- Research in the area of predictive analytics should focus on improving detection and prediction of risks to Smart Grid wide-area SA and security.

The Smart Grid is expected to enable real time wide-area SA for grid operators. Wide area SA and enhanced decision support and visualization tools are key elements in the transformation to the Smart Grid. This paper has discussed human factors research needs to facilitate the US energy goals by enhancing SA and decision making performance in the electric power grid and the Smart Grid. We described domains of human factors research needs and approaches to human factors research and development. Viewed fundamentally within a system-of-systems framework, the increasingly complex power grid requires research and tool development that addresses the linkages between high-level federal policy goals for the electric grid and the enabling capability provided by software. A research and development approach is needed that involves analysis, design and evaluation activities that proceed iteratively and in parallel, in order to better determine user needs at multiple organizational levels. We believe it is critical to understand and address user needs at multiple organizational levels so that the pitfalls of "technology push" can be avoided. It is recommended that R&D programs adopt user-centered design and application of cognitive engineering methods to facilitate effective design and deployment of decision support and visualization tools in the electric power industry.

ACKNOWLEDGMENTS

This work was supported in part by the Information and Infrastructure Integrity Initiative of the Pacific Northwest National Laboratory. The Pacific Northwest National Laboratory is operated by Battelle for the U.S. Depart of Energy under Contract DE-AC06-76RL01830. For their contributions in earlier work that informed this paper and for their insightful comments that improved this work, the author wishes to thank PNNL colleagues Yousu Chen, Jeff Dagle, Mark Hadley, Henry Huang, Ning Lu, Tom Sanquist, and Kevin Schneider. [Report Number PNNL-SA-71224]

REFERENCES

[1] Chu, S., “Secretary Chu Opinion Piece in Times of London.” [US Department of Energy Press Releases], May 27, 2009. http://www.energy.gov/news2009/7429.htm. (2009).

[2] Locke, G., “Locke, Chu Announce Significant Steps in Smart Grid Development.” [US Department of Energy Press Releases], May 18, 2009.http://www.energy.gov/news2009/7408.htm. (2009).

[3] U.S. Department of Energy, Office of Electric Transmission and Distribution, [Grid 2030: A National Vision for Electricity’s Second 100 Years], US Department of Energy, Washington, DC (2003).

[4] Federal Energy Regulatory Commission, [Smart Grid Policy], http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf, July 16, 2009 (2009).

[5] National Institute of Standards and Technology, [NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. NIST Special Publication 1108], Office of the National Coordinator for Smart Grid Interoperability. http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf (2010).

[6] Bush, R., & Wolf, G., “The Bulk Power Grid Seeks Intelligent Operation,” Transmission & Distribution World, (2007).

[7] Kosterev, D.N., Taylor, C.W. & Mittelstadt, W.A., “Model Validation for the August 10, 1996 WSCC System Outage,” IEEE Trans. Power Syst 14(3), 967-979. (1999)

[8] Department of Energy, [U.S.-Canada Power System Outage Task Force: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations], US Department of Energy (2004).

[9] U.S. Congress, [Energy Policy Act of 2005], URL: http://www.doi.gov/iepa/EnergyPolicyActof2005.pdf (2005)

[10] Khurana, H., Hadley, M., Lu, N., & Frincke, D.A., “Building security in: Smart-grid security issues,” IEEE Security & Privacy, 8 (1), 81-85 (2010).

[11] IEEE Power Engineering Society, “IEEE Standard for Synchrophasors for Power Systems,” IEEE Std C37.118 – 2005, IEEE. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1611105&isnumber=33838 (2006)

[12] President’s Commission on Critical Infrastructure Protection, [Critical Foundations: Protecting America’s Infrastructure. The Report of the President’s Commission on Critical Infrastructure Protection]. URL: http://fas.org/sgp/library/pccip.pdf (1997)

[13] Committee on Science and Technology for Countering Terrorism, National Research Council, [Making the Nation Safer: The Role of Science and Technology in Countering Terrorism]. National Academies Press, Washington, D.C., http://www.nap.edu/catalog.php?record_id=10415 (2002).

[14] National Institute of Standards and Technology, [Smart Grid Cyber Security Strategy and Requirements, DRAFT NISTIR 7628], The Cybersecurity Coordination Task Group. URL: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf (2009)

[15] North American Electric Reliability Corporation (NERC), [A Review of System Operations Leading up to the Blackout of August 14, 2003], NERC, Princeton NJ (2004).

[16] North American Electric Reliability Council, [Technical Analysis of the August 14 2003 Blackout: What Happened, Why, and What Did We Learn?], NERC http://www.nerc.com/filez/blackout.html (2004).

[17] National Research Council, Committee on Human-System Design for Changing Technology. [Human-System Integration in the System Development Process], National Academies Press, Washington DC (2007)

[18] Overbye, T.J. and Weber, J.D., “Visualizing the electric grid,” IEEE Spectrum, 52-58 (2001).

[19] Gordon, S. E. & Gill, R. T. “Cognitive Task Analysis” (Chapter 13), in C.E. Zsambok & G. Klein (eds.), [Naturalistic Decision Making]. Lawrence Erlbaum Associates, Mahwah, NJ, 131-140 (1997).

[20] Greitzer, F.L., Schur, A., Paget, R., and Guttromson, R.T., “A sensemaking perspective on situation awareness in power grid operations,” IEEE Power & Energy Society Annual Meeting—Conversion and Delivery of Electrical Energy in the 21st Century (Pittsburgh, PA), IEEE, Piscataway, NJ, pp. 1-6. (2008).

[21] North American Synchrophasor Initiative (NASPI), [Synchrophasor Technology Roadmap], NASPI http://www.naspi.org/ (2009).

[22] Zsambok, C.E. “Naturalistic decision making: Where are we now?” [Naturalistic Decision Making] Zsambok, C. and Klein, G. (Eds). Erlbaum, Mahwah, NJ, 3-16 (1997).

[23] Klein, G. “The recognition-primed decision (RPD) model: Looking back, looking forward.” [Naturalistic Decision Making] Zsambok, C. and Klein, G. (Eds). Erlbaum, Mahwah, NJ, 285-292 (1997).

[24] Greitzer, F.L., Podmore, R., Robinson, M., & Ey, P. “Naturalistic decision making for power system operators,” Naturalistic Decision Making Conference, London, United Kingdom (2009).

[25] Huang Z, Wong, P.C., Mackey, P.S., Chen, Y., Ma, J., Schneider, K.P., & Greitzer, F.L. "Managing complex network operation with predictive analytics," Proc. AAAI Spring Symposium on Technosocial Predictive Analytics, Stanford University, Palo Alto, CA (2009).
[26] Chen, Y., Huang, Z., Wonn, P.C., Mackey, P.S., Allwardt, C., Ma, J., & Greitzer, F.L. "An advanced visual analytic decision support tool for electricity infrastructure operations," Proc. Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (2010)
[27] North American Electric Reliability Council (NERC), [August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts.], Available from http://www.nerc.com/docs/docs/blackout/BOARD_APPROVED_BLACKOUT_RECOMMENDATIONS_021004.pdf [Accessed 1/5/2010] (2004).
[28] Aldrich, C. [Simulations and the future of learning], John Wiley and Sons, San Francisco CA (2004).
[29] Kolb, D. [Experiential learning: Experience as the source of learning and development], Prentice Hall, Englewood Cliffs NJ (1984)
[30] Kaber, D.B. & Endsley, M.R., "Team situation awareness for process control safety and performance," Process Safety Progress 17(1), 43-48. (1998).
[31] For more information about the EIOC, see [EIOC Electricity Infrastructure Operations Center web site], Available from http://eioc.pnl.gov/.
[32] For more information about the GridWise™ program, see "Bringing Power to the People," EIOC Electricity Infrastructure Operations Center web site article, Available from http://eioc.pnl.gov/research/gridwise.stm.