BULK POWER SYSTEM INTEGRATION OF SMART GRID RELIABILITY CONSIDERATIONS

MARK G. LAUBY, *SENIOR MEMBER, IEEE*
ERIC ROLLISON, *MEMBER, IEEE*

Abstract—**The deployment of automation, or 'smart grid', on the bulk power system continues to grow. 'Smart' technologies have been implemented for some time at the substations (in the form of SCADA, or supervisory control and data acquisition) and more recently, a small penetration in directly on transmission circuits. Some examples of this include automated reconfiguration capabilities, Dynamic Thermal Circuit Rating (DTCR), phasor measurement units (PMUs), and Flexible AC Transmission Systems (FACTS.**

***Index Terms*—Smart Grids, Transmission, Distribution Reliability, Climate Change, Global Warming, Renewable Energy, Sustainability, Bulk Power System.**

I. INTRODUCTION

Today, the bulk power system is designed to meet customer demand in real time – meaning supply and demand must be constantly and precisely balanced. As electricity cannot be presently stored on a large scale, changes in customer demand throughout the day and over the seasons are met by controlling conventional generation, using stored fuels to generate electricity when needed. Even with climate change initiatives and the potential for changes in fuel mix and technologies, this continuous balancing of resources and demand will be required to maintain the reliability of the bulk power system.

A significant challenge is to reliably integrate smart grid technologies while maintaining reliability. Three fundamental characteristics of the smart grid infrastructure, besides the availability of smart grid technologies, are interoperability, communications and IT systems. However, much of the control systems have little designed security being designed for local control and not resilient to errors from unintentional miscommunications or IT errors or intentional attacks.

First, the strength of interoperability design of smart grids, unless carefully planned and operated, can provide a vehicle for intentional cyber attack or unintentional errors impacting bulk power system reliability, through a variety of entrance and exit points. These control systems must be improved to provide robust protection from IT and communication vulnerabilities.

Second, new tools and analysis techniques will be required to design and manage the deployment of broad-scale smart control systems across the bulk power system. As it is a large non-linear system, the ramifications and design of smart grid on control systems must be modeled, simulated and designed to ensure that the expected performance improvements will be realized. This integration must not increase the vulnerability of the bulk power system to significant reliability concerns, such as transient and long-term stability, small signal stability, voltage stability and component design issues such as short circuit considerations.

As a definition of Smart Grid, we propose:

Smart Grid — The integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in ***a secure, reliable****, and efficient electric power system, from generation source to end-user.*

Smart grid is an important component of the bulk power system of the future. Two perspectives are discussed: Transmission and Distribution.

II. "SMART" TRANSMISSION

The United States Department of Energy lists five fundamental technologies that will drive smart grid for transmission:

- Integrated communications, connecting components for real-time information and control
- Sensing and measurement technologies, to support faster and more accurate response
- Advanced components (e.g. storage, power electronics and diagnostics)
- Advanced controls, to monitor components and enable rapid diagnosis and solutions
- Improved interfaces and decision support

Mark G. Lauby and Eric Rollison are with the North American Electric Reliability Corporation, 08540 USA (e-mail: mark.lauby@nerc.net)

In the U.S., the Federal Energy Regulatory Commission (FERC) issued a Policy Statement identifying six priority areas of smart grid development [1]:

1. System Security
2. Communication and Coordination Across Inter-System Interfaces
3. Wide-Area Situational Awareness
4. Demand Response
5. Electric Storage
6. Electric Vehicles

Further, the U.S. National Institute of Standards and Testing (NIST) is currently developing interoperability standards for equipment. [2]

The deployment of automation, or 'smart' technologies, on the bulk power system has continued to grow and evolve. The goals for these deployments has been to better match energy supply with demand and serves as an important example of how new technologies are gradually diffused within the power industry. In summary, 'smart' technologies have been implemented at the substation (in the form of SCADA, or supervisory control and data acquisition) and more recently, a small penetration in directly on transmission circuits. Some examples of this include automated reconfiguration capabilities, Dynamic Thermal Circuit Rating (DTCR), phasor measurement units (PMUs), and Flexible AC Transmission Systems (FACTS).

Today, the transmission grid has a high-level of observability and some basic remote control. The basic transmission parameters – voltage, frequency and current – are well monitored and understood. The potential of the deployment of 'smart' transmission technology is to gain a better understanding of the real-time operation parameters (e.g., the relative angle of the voltage) of the grid and consequentially increase the control, response and a more precise view of the transmission system. This increase visibility into the system will allow operators for effectively manage the bulk power system, moving from capacity to energy parameters.

III. STATUS OF "SMART TRANSMISSION" IMPLEMENTATION

The smart grid integration enables the coordinated and system-wide ability to deploy automation and smart technologies on the bulk power system. Unlike today, where islands of automation are created without the ability to interoperate across their boundaries, smart grid provides the ability to create an overarching, coordinated and hierarchical approach to automation, control and effectiveness. The goal for these deployments has been to better match energy supply with demand, improving asset management and increasing reliability.

Current deployments of smart grid technologies serves as an important example of how new technologies are gradually diffused within the power industry. These technologies have been localized in their implementation for some time at substations (in the form of SCADA, or supervisory control, intelligent electronic devices (IED) and data acquisition) and, more recently, directly on the bulk transmission system. Some examples of this include automated reconfiguration capabilities, Dynamic Thermal Circuit Rating (DTCR), phasor measurement units (PMUs), and Flexible AC Transmission Systems (FACTS).

Today, the transfer capability can be increased addition of equipment, by raising the operating voltage and reconfiguring conductors into a more compact arrangement. However, for more advanced technologies, such as DTCR, PMUs and FACTS, the deployment is in early stages. These technologies enable the operator to gain intelligence and visibility on the status of the transmission grid on a real-time basis to use the existing transmission capacity and energy carrying capability. Increasing the effectiveness of the bulk transmission system enables delivery of desired resources to demand. Therefore, transmission is vital to ensure climate change goals are met, while maintaining bulk power system reliability.

From a bulk system perspective, data and information are gathered from multiple locations from energy users, distribution systems, transmission and generation. Every second, the bulk power system can adjust to accommodate dynamic changes in energy user's behavior and the status of countless numbers of system equipment. However, many of the systems implemented using existing smart grid technologies have been designed for control functionality and are not resilient to errors resulting from misuse, miscommunications or IT system failures[3]. In fact, unlike most modern IT and communication systems, these control systems have little built-in security. Therefore, security on these control systems can be intentionally defeated or unintentionally corrupted, etc., which can lead to unexpected results and system failures. For example, attackers can upload encrypted code to the Programmable Logic Controllers (PLCs) that control the automation of smart grid devices/systems, which can be accessed through Microsoft Windows PCs. An attacker could remotely control a number of functions, like download files, execute processes, and delete files. In addition, an attacker could also interfere with critical operations of smart grid devices/systems to do things

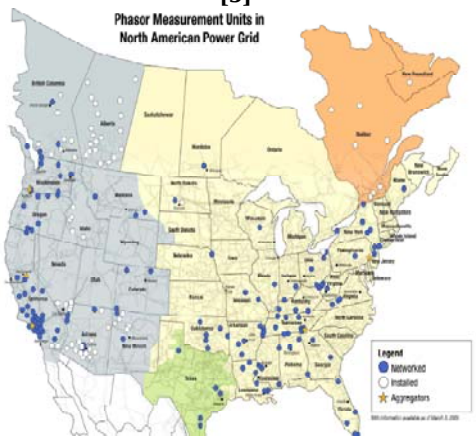
like shut down customer demand, trip lines, not alarm for heavily loaded equipment, etc. The integration of commercial IT systems and communications with existing control systems/PLCs can create two significant reliability considerations.

The implementation of PMUs throughout systems in North America has been gradual due to a number of factors:

- Reliability benefits of PMUs for planning and operations require industry awareness
- Physical and cyber security considerations must be addressed prior to deployment
- Regulatory uncertainty with respect to cost recovery and data access
- Development of tools required to use of the information both for operations and planning

As of early 2009, there were approximately one-hundred-and-fifty networked PMUs in the field (Figure 1). Networked means they are connected to and are supplying data-to-data concentrators at TVA or CAISO. An additional one-hundred operational PMUs are in the field that are collecting data, but are not networked to the data concentration sites. In addition, there are hundreds of digital relays, which can perform PMU-like functions if activated. The North American SynchroPhasor Initiative (NASPI) estimates that 1,200 PMUs are required to provide the needed level of wide area visibility of the four interconnections North America. Additional PMUs would provide detailed visibility of local conditions and eventually, more automated control of the bulk power system. Current plans by the NASPI call for the deployment of PMUs by 2014 at major transmission interconnections, substations 500kV and above, near major load centers, and at large wind, solar, or storage facilities. [4]

Figure 1: PMUs in the North American Power Grid [5]



DTCR is being demonstrated on a number of transmission systems, and, in some cases, deferred planned line upgrades. FACTS technologies are a commercial technology that has seen a slow implementation due to its relative cost compared to alternatives.

IV. "SMART" TRANSMISSION RELIABILITY CONSIDERATIONS

Phasor measurement units (PMU) produce data useful to improve planning and operations for the purpose of disturbance monitoring, stability model validation, data retention and disturbance analysis — enabling more efficient transmission system use by dynamic rating and the advent of new special protection systems, significantly improving operating reliability.

Additionally, the deployment of Dynamic Thermal Circuit Ratings (DTCR) will be used to increase the thermal loading capacity of individual transmission lines and substation equipment. Present limits are both static and often conservative, based on worst-case weather conditions. DTCR uses real-time information about weather, load, temperature, line tension, and/or line sag to estimate actual thermal limits, thus allowing higher thermal capacity of transmission lines and substation equipment. Additionally, Flexible Alternating Current Transmission Systems (FACTS), coupled with storage devices, will increase the power transfer capability of individual transmission lines or a transmission corridor and improve overall system reliability by reacting almost instantaneously to disturbances — allowing lines to be loaded closer to their inherent thermal limits. Specifically, the deployment of Unified Power Flow Controller (UPFC) and the Convertible Static Compensator (CSC) will increase the ability to control both real and reactive power flows among transmission corridors and maintain the stability of transmission voltage.

Two significant reliability considerations must be addressed. First, the strength of interoperability design of smart grids, however, unless carefully planned and operated this interoperability can provide a vehicle for cyber attack on the bulk power system, through a variety of entrance and exit points. Further, the physical assets that support smart grids will require protection as the dependence grows on their functionality.

Second, new tools and analysis techniques will be required to design and manage the deployment of broad-scale smart control systems across the bulk power system. As it is a large system with non-linear characteristics, the ramifications and design of smart grid controls must be modeled, simulated and designed

to ensure that the expected performance improvements will be realized, without increasing the vulnerability of the bulk power system to significant reliability considerations.

V. "SMART" DISTRIBUTION

'Smart' distribution technologies have advanced and become more cost-effective during the last decade. Smart Grid, in this context, is considered as distribution automation technologies that include remote monitoring and control devices; fault detection, isolation, and restoration capabilities; and load and phase measurement and balancing devices (e.g. synchrophasors). There are two main drivers for implementing devices like these:

- **Reduce line losses —** As electricity is carried over long distances, electrical energy gradually dissipates in the form of heat. In the United States, 5–12 percent of all the power generated is lost, and 60 percent is directly attributable to the distribution system. Distribution system line losses depend on the magnitude of the electric current (load density). While there are technical limitations to how much line losses can be reduced, 'smart' distribution system technologies can optimize the performance of the electrical grid by controlling the flow of electricity. Some of these technologies include remotely monitored and controlled devices like capacitors throughout the grid and phase balancing equipment that moves load between the three phases of electricity to balance load on each phase.

- **Improve outage management processes —** Electricity providers are concerned with improving distribution system reliability. Key metrics measuring distribution reliability include the System Average Interruption Frequency Index (SAIFI), or the number of sustained outage events experienced by a customer, and the Customer Average Interruption Duration Index (CAIDI), or the average length of a customer outage. 'Smart' grid distribution technologies address these metrics by expanding fault detection and offering fault isolation and restoration capabilities where a faulted section of a feeder can be de-energized while the remainder of the line is reconfigured to minimize the number of minutes most customers are without power.

The prevalence of 'smart' technologies on the distribution network can also improve the reliability of the bulk power system. For example, by reducing line losses, system peak loads can be reduced thereby reducing strain on the bulk power system. By reducing the frequency and duration of outages, the impact of these disturbances on the bulk power system is reduced.

However, fundamental changes in distribution system operations, such as two-way flow of energy, can, in aggregate, impact the reliability of the bulk power system. Therefore, system planners, designers and operators will need to change their approach and processes to integrate large amounts of smart distribution technologies.

VI. STATUS OF "SMART DISTRIBUTION" IMPLEMENTATION

Smart grid demonstrations on the distribution system are increasing in number throughout North America. For the most part, they seek to demonstrate key 'smart' capabilities on a small scale (usually a medium sized city). These demonstrations also normally are part of a broader initiative that could include advanced meters, home area networks, distributed renewable generation installations, and testing for plug-in hybrid electric vehicles.

For example, Xcel Energy is heading one of the most advanced Smart Grid pilot projects, investing around $100 million to build a Smart Grid City in Boulder, Colorado. Other pending or announced projects include a Smart Grid Corridor project proposed by Dayton Power & Light in Ohio and a Smart Grid pilot by National Grid (approximately 15,000 customers) in Worchester, MA. Finally, the Ontario Energy Board in Ontario, Canada has worked to define smart grid technology and develop the regulatory framework for its implementation. The Government of Ontario set a target of deploying smart meters to 800,000 homes and small businesses (i.e. small "general service" customers under 50 kW demand) by the end of 2007, which was surpassed, and throughout the province by the end of 2010. The Independent Electricity Service Operator of Ontario (IESO) released a report outlining their view of future opportunities in smart grid applications. [6]

With the deployment of demonstrations, and the overarching characteristic of inter-operability, industry experts have recognized the need for deeper and broader cyber-security, in order to manage reliable deployment of the next generation of smart-grid technologies. NERC's Critical Infrastructure Protection (CIP) Standards continue to be modified and improved to ensure grid modernization evolution will have reduced cyber vulnerability. [7]

VII. "Smart" Distribution Reliability Considerations

The increase in the amount and type of generation, or generation-like resources (i.e. hybrid vehicles), on the distribution system essentially makes the distribution system look more like the transmission system, as both generation and demand are connected and power can flow both in the distribution system and onto the bulk power system. Operating the evolving distribution system and assessing its impact on bulk system reliability will likely require significant changes in planning and operating practices. The range of impacts on the bulk power system from the deployment of 'smart' distribution system options in response to climate change initiatives represents fundamental changes in the supply/demand and control processes needed to maintain the bulk power system reliably. Increased dependence on distributed generation, demand-side resources and distribution system applications increases the potential exposure to cyber vulnerability. All of these changes, in aggregate, and their potential impacts must be carefully considered to effectively plan, design and operate the bulk power system reliably.

The priorities for the development of cyber security in the bulk power systems -- especially with the smart grid deployments -- need to focus on prevention, detection and response, and recovery. Furthermore, bulk power system controls should be designed in a way which assumes the failure of control room systems, or loss of control room communications (regardless of cause), and enables the next series of predictable control room actions to be carried out autonomously, or at least automatically, by grid actuators. To be effective, these priorities must be incorporated in the development of the smart grid, and affects all aspects of grid planning and operations.

VIII. Conclusions

In order to maintain bulk power system reliability, planning and operations will need to evolve with the integration of large amounts of 'smart' grid distribution technologies and applications. While a smarter grid can improve the reliability of the bulk power system, with the integration of smart grid technologies on the distribution system, new models and tools will be required to develop reliable designs needed to ensure the reliability of the bulk power system. Though not insurmountable, these challenges must be studied and technologies developed to ensure that the resulting system achieves greater levels of security and remains reliable.

Cyber security is vital for the safe operation of the bulk power system. The introduction of critical infrastructure on the distribution grid that can be remotely controlled poses a threat to bulk power system reliability. In other words, many smart grid devices will operate on assets not considered part of the bulk power system. However, these assets may require cyber protection to mitigate vulnerability of the bulk power system. Therefore, reliability standards must all be compatible. Ultimately, a cyber-secure and reliable grid will ensure smart grid technologies operate effectively and leveraged to their full potential.

IX. References

1. Federal Energy Regulatory Commission, Policy Statement on Smart Grid, http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf, July 2009
2. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, and NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements
3. U.S. DOE and Department of Homeland Security, *Roadmap to Secure Control Systems in the Energy Sector*, January 2006, www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf
4. *Synchrophasor Technology Roadmap*, North American Synchrophasor Initiative (NASPI), March 13, 2009
5. North American Synchrophasor Initiative Phasor Applications Update NERC OC Briefing, March 17, 2009
6. http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report.pdf
7. http://www.nerc.com/files/Reliability_Standards_Complete_Set_2009May20.pdf

X. BIOGRAPHIES

Mark G. Lauby is the Director of Reliability Assessments and Performance Analysis joining the North American Electric Reliability Corporation (NERC) in January 2007. Reliability assessments encompass the electric reliability organization's efforts to independently assess and report on the overall reliability, adequacy, and associated risks to the existing and projected interconnected North American bulk power system. Performance analysis includes the development of reliability metrics and benchmarking establishing an industry-wide set of baseline measurements for determining the reliability. Prior to joining NERC, Mr. Lauby worked since 1987 for the Electric Power Research Institute (EPRI) where he held a number of senior positions, including: Director, Power Delivery & Markets; Managing Director, Asia, EPRI International; and Manager, Power System Engineering in the Power System Planning and Operations Program. Mr. Lauby started his career in the electric industry at the Mid-Continent Area Power Pool (MAPP), in Minneapolis, Minnesota in 1979. Mr. Lauby earned both his Bachelor of Electrical Engineering in 1980 and his Master of Science in Electrical Engineering in 1989 from the University of Minnesota.

He is the author of numerous papers on the subjects of power system reliability, expert systems, transmission system planning, and power system numerical analysis techniques. Mr. Lauby has served as Chair and is a life member of the International Electricity Research Exchange (IERE), is a Senior Member of the Institute of Electrical and Electronic Engineers (IEEE), and served as Chairman of a number of IEEE working groups. Mr. Lauby has been recognized for his technical achievements in many technical associations, including the 1992 IEEE Walter Fee Young Engineer of the Year Award.

Eric Rollison is the Engineer of Reliability Assessments at the North American Electric Reliability Corporation. Eric began working at NERC in April 2009 and joined the Reliability Assessments and Performance Metrics Group in July 2010. He previously was an Engineer in the Compliance Enforcement group within NERC. Eric is currently a member of Institute of Electrical and Electronics Engineers (IEEE) and the American Society of Mechanical Engineers (ASME). Prior to joining NERC, Eric worked for five years as both an Engineer and Project Manager in the Aerospace Industry working on sensor manufacturing and development for a mid-sized manufacturing firm that worked directly with General Electric and Pratt & Whitney on Civil and Defense Aviation projects.

Eric holds a Master's of Science in Finance from Temple University, which he received in January 2009, and he holds a Bachelors of Science in Mechanical Engineering degree from Villanova University, which he received in 2001.