Communication Requirements for Risk-Limiting Dispatch in Smart Grid

Victor O. K. Li, *Fellow, IEEE*, Felix F. Wu, *Fellow, IEEE*, and Jin Zhong, *Member, IEEE*

Department of Electrical and Electronic Engineering,

The University of Hong Kong, Pokfulam, Hong Kong, China

(e-mails: vli@eee.hku.hk, ffwu@eee.hku.hk, jzhong@eee.hku.hk)

Abstract — **The existing power grid infrastructures in many countries are primarily based on technologies that have been developed as centralized systems in which power is generated at major power plants and distributed to consumers through transmission and distribution lines. In the recent decade, with the increasing penetration of renewable energy sources such as solar and wind power, and smart electrical appliances, the centralized model may no longer hold, and the supply and demand for electricity become more dynamic. Moreover, the latest developed information and communication technologies (ICT) and power electronic technologies could enhance the efficiency and performance of power system operations. Recently, concerns with global warming have prompted many countries to announce research programs on smart grid, which is the transformation of the traditional electric power grid into an energy-efficient and environmentally friendly grid by the integration of ICT, power electronic, storage and control technologies. With the smart grid, there is an opportunity for a new operating paradigm that recognizes the changing structures of the power grid with renewable generation, and the high-resolution data, high speed communications, and high performance computation available with the advanced information infrastructure. A new operating paradigm, namely, risk-limiting dispatch, is proposed for the smart grid in this paper. In addition, we have identified the requirements of a communication infrastructure to support this new operating paradigm.**

Keywords – Communication architecture, risk-limiting dispatch, smart grid.

I. INTRODUCTION

Concerns with global warming prompted governments throughout the world to pursue policies aiming at the reduction of greenhouse gases, mostly carbon dioxide. Government policies to achieve carbon reduction in electric energy systems include increasing renewable energy penetration to reduce fossil fuels, and introducing smart grid to facilitate the integration of renewables into the system.

However, increased renewable energy generation in the power grid negatively impacts power system operations. Due to the intermittent characteristics of wind and solar, the outputs of wind farm and solar energy are difficult to forecast. A sudden change in wind conditions could result in very large changes in power output. It is a challenge for a system with large renewable generation capacities to implement real-time power balance. Hence, renewable energy may cause instability in the power grid. To accommodate high penetration of renewable energy sources, efficient real-time control and communication technologies are needed.

The small-scale distributed renewable energy generators installed at customer premises open up the possibility of users selling electricity to the grid. Coordinating distributed generators with storage (e.g., in electrical vehicles) has the effects of peak shaving and load shifting, hence implementing demand side response. Real-time two-way communications and smart meters are the basic platform for demand side response and demand management.

The smart grid brings information and communication technologies (ICT) to bear on the electric grid to accommodate renewable energy sources and, at the same time, to ensure its reliability on which the society depends.

The objectives of the smart grid include (1) accommodating all generation, including renewable resources, and storage options; (2) enabling active participation by consumers in demand response; (3) optimizing assets and operating efficiency; (4) providing good power quality for electricity supply; (5) self-healing capability from power disturbance events; (6) operating resiliency against physical and cyber attack; and (7) enabling new products, services, and markets [1].

The European Union initiated the smart grid project in 2003 [2]. The Electric Power Research Institute of the USA started the IntelliGrid project around the same time [3]. US DOE had a Grid 2030 project [4]. Under the Energy Independence and Security Act of 2007, the National Institute of Standards and Technology (NIST) is responsible for coordinating the development of a framework for information management to achieve interoperability of smart grid devices. Currently, there is an urgent need to establish protocols and standards for the smart grid. The NIST report (Phase I) provides a conceptual reference model for the smart grid [5].

Some argue that the electric power grid with modern energy management system (EMS), consisting of hundreds of remote terminal units (RTU) sending real-time data from substations

This work was supported by the Strategic Research Theme and the University Development Fund (Initiative on Clean Energy & Environment) of the University of Hong Kong.

978-1-4244-6826-3/10/$26.00 ©2010 IEEE

spread all over the system every two seconds to the computer control center via supervisory control and data acquisition (SCADA) system and the advanced application software in the control center processing the data through state estimation, optimal power flow, etc. to ensure economic and reliable operation, is a smart grid already. For an introduction to SCAD and EMS, interested readers are referred to [6]. However, the computer and communication technologies employed by EMS and SCADA systems lag behind the rapidly developing state of the art ICT technologies. Moreover, most power systems do not have real-time monitoring and control capability in the lower voltage distribution system from substation down. The push for smart grid is to modernize the whole electric power grid to merge it with the latest, as well as the emerging, information and communication technologies. Recent progress in Phasor Measurement Unit (PMU), which provides GPS time-stamped measurements in milliseconds opens up opportunity to upgrade EMS to serve a smarter transmission grid. The time has come for a unified smart grid for all kinds of generation, namely, conventional centralized large fossil-fuel generators to small distributed renewable generators, transmission and distribution networks, all the way to the consumers.

Immediate efforts in smart grid have largely focused on the Advanced Metering Infrastructure (AMI) that installs smart meters on consumer premises for demand response and the communication systems to connect the meters to distribution control centers. The work is mostly implementation of available technology. The next step will be the design of seamless integration of AMI with EMS.

Simply building hardware for the renewable generators and the smart grid, but still using the same operating paradigm of the grid will result in limited achievement of the ultimate goal. Once the information infrastructure is in place, opportunity is ripe for a new operating paradigm that recognizes the changing structures of the power grid with renewable generation, and the high-resolution data, high speed communication, and high-performance computing provided by a unified smart grid. A new operating paradigm *Risk-limiting Dispatch* is proposed for the smart grid in this paper. The fundamental transformation in risk-limiting dispatch is from the traditional worst-case control strategy to risk-based control; from deterministic control to stochastic control; from preventive control to predictive control; from centralized control to distributed control. This new paradigm will be discussed in detail in Section II. In Section III, we shall identify the requirements of the communication architecture to support risk-limiting dispatch. We conclude in Section IV.

II. RISK-LIMITING DISPATCH

The traditional worst-case dispatch of power system, though inefficient, works well for systems whose primary uncertainty in operation is the outage of generators and transmission equipments (i.e., discrete probability). However, with the introduction of stochastic and intermittent nature of renewable generation of wind and solar, it is imperative to adopt the probabilistic approach in power system operation. The resource wastage in under-dispatch of and over-reserve for wind and solar generation is not acceptable for the goal of reducing carbon emission to curb global warming. A visionary new approach that is compatible with the new reality of the future (large penetration of renewable sources and highly effective smart grid) is needed. The proposed new paradigm - risk-limiting dispatch - is based on the belief that a probabilistic approach provides more efficient operation of power systems [7] [8]. But a risk-based probabilistic approach with predictive control is not viable without an effective information infrastructure of a smart grid.

The difficulty of current worst-case dispatch practice is that since (N-1) contingency analysis assumes a 0-1 failure of generator, transmission branch and critical devices, it must treat a renewable generator as an 'equivalent' conventional generator with a reliable capacity. As a result reserve capacity and the associated carbon emissions are not as greatly reduced as expected. The worst-case dispatch is like maintaining a large inventory in order to meet stochastic demands. Other industries have moved away from this paradigm to "just-in-time" supply-chain management using information technology. It is time for the operation (or dispatch) of electric grid to move to "just-in-time" dispatch in the era of smart power grids.

This new operating paradigm uses real-time information about supply (taking into account the stochastic nature of renewable sources) and demand (stochastic nature of demand response), obtained from smart grid hardware. The operational decision-making of the new operating paradigm is based on the criterion of limiting the risk of not meeting the operating constraints.

Power system operation requires that the power must be balanced at all times at all points of the system (power balance constraints) and operating limits, such as line flow limits, voltage limits, stability, etc., must be satisfied (operating limit constraints). Depending on the time-scale of interests, power balance can be expressed by a set of differential equations, algebraic equations or both. For simplicity, we shall use algebraic equations to illustrate the concept here. Thus, the power balance constraints are expressed as $g(x(t),u)=0$ and the operating limit constraints are expressed as $h(x(t),u)\le 0$, where $x(t)$ is the state of the system at time *t*, and *u* is the control taken. Power generated and consumed at time *t* is determined by three decisions: the *scheduling* decision σ taken T_σ time units earlier at $t-T_\sigma$; the *recourse* decision ρ taken T_ρ time units earlier at time $t-T_\rho$; and the *emergency* decision ε taken at time $t-T_\varepsilon$.

Typically, at the scheduling time $t - T_\sigma$ in the day-ahead market, the System Operator or ISO receives offers and bids for power to be supplied and consumed in the next 24 hours at 'real time' *t*. ISO's decision u_σ schedules a subset of these offers and bids that maximizes an objective function $f(x(t),u)$ subject to the operating constraints. For a smart grid, we assume that at each *t*, ISO receives observations y_t so ISO's information at *t* is $Y_t = \{y_s, s \le t\}$. Due to the stochastic nature of supply (due to renewable resources) and demand (due to demand response), a probabilistic approach is necessary.

$$\max\{f(x(t),u_\sigma) \,|\, P\{g(x(t),u_\sigma)=0, h(x(t),u_\sigma)\le 0 \,|\, Y_{t-T_\sigma}\} \ge p^* \qquad (1)$$

where p* is the desired probability, such as 0.995.

One hour before real time *t*, ISO has better information about the availability of generators that were scheduled in the day-ahead market and on demand. This information is used to balance any mismatch in supply and demand. This *recourse* decision is taken at a later time ($t - T_\rho$), for example at the hour-ahead balancing market, to counter violations in constraints incurred by the earlier decision u_σ. Lastly, it may turn out that at real time *t*, or at the outset of cascading outages, $t - T_\sigma$, the scheduled generation is unable to meet the demand, in which case ISO must take an emergency decision to disconnect or shed sufficient load to fit the available generation. Hence,

$$\max\{f_\rho(x(t),u_\rho) \,|\, P\{g(x(t),u_\rho)=0, h(x(t),u_\rho)\le 0 \,|\, Y_{t-T_\rho}\} \ge p^* \qquad (2)$$

$$\max\{f_\varepsilon(x(t),u) \,|\, P\{g(x(t),u_\varepsilon)=0, h(x(t),u_\varepsilon)\le 0 \,|\, Y_{t-T_\varepsilon}\} = 1 \qquad (3)$$

We call the risk-based control of power system operation, formulation in (1) - (3) above, the *risk-limiting dispatch*. It explicit incorporates renewable resource uncertainties, smart grid measurements, and the reliability of power system operation.

Risk-limiting dispatch relies on the ability of the smart grid to provide event prediction and handling capability. In the current power system operation, voltages and currents of most nodes and lines are measured and monitored by the system control center. The voltage and current information are analyzed to estimate the system operation states and to forecast emergency states. When a fault occurs, the power system protection system detects the abnormal voltage and current, calculates the possible location of the fault, and isolates the fault by disconnecting the fault from the rest of the system. The actions of the traditional protection system mostly rely only on voltage and current information measured at different locations. The limited unsynchronized information may result in inaccurate localization of faults. The other issue is that the abnormal voltages and currents are the results of faults. They can be detected only after the occurrences of faults. This means that current protection systems can only detect a fault afterwards, and they focus on minimizing the impacts of the fault to the rest of the system.

To predict fault events and protect power systems in advance, additional information beyond the above power system parameters are required. With the recently developed sensor and communication technologies, some non-electrical information of power systems can be measured and communicated in real time. The information include, for example, winding temperature, insulation oil temperature and composition, transmission line sag, insulation of underground cable, and insulation of high voltage devices, etc. The non-electrical information can help identify the stressed power components in advance, and predict equipment faults beforehand.

III. Communication Architecture For Risk-Limiting Dispatch

It has been advocated [9] that there is a need of an electricity communication superhighway for supporting generation, transmission, substations, consumers, and distribution and delivery controllers. The challenge in creating the power delivery system is the development of a communication infrastructure to support universal connectivity and interconnection-wide real time monitoring. Multiple recipients must be able to receive updates of the system status in real-time but they may have various latency and rate requirements. In particular, our analyses of the requirements of the smart grid and of risk-limiting dispatch reveal the following requirements for the communication infrastructure:

1. Capability to transport large volume of data: To enable risk-limiting dispatch, the time resolution of data is in milliseconds. In addition, there will be a large variety of data generated not only by the power generators, but also by the consumers, and the distribution system. Therefore, the volume of data generated is expected to be many-fold the volume of data generated today.
2. Extensive coverage: The network must cover the whole power generation, distribution, and consumption network, all the way to the customer premises.
3. Quality of Service (QoS) support: The system must satisfy very stringent reliability, delay, and throughput constraints.
4. Cyber security: The system must be protected against cyber attacks.

Supervisory Control and Data Acquisition (SCADA) systems are currently employed as the core of the communication system for monitoring and controlling a wide-area, geographically dispersed power grid. These SCADA systems have fundamental limitations. SCADA is associated

with a star network with point-to-point links connecting substations to control centers. As a control centre polls each substation for control data once every two to four seconds, the power grid can fall behind when it undergoes some disruptive events [10] [11].

To provide reliable data delivery, some projects in the power industry have employed the Transmission Control Protocol (TCP) [12] [13]. Yet, TCP is a best effort, in-order reliable packet delivery transport layer protocol for any two communicating devices. It neither supports multicasting and spatial redundancy, nor offers any real-time quality of service (QoS) guarantees. Hence, TCP is inadequate for many real-time mission-critical applications, such as grid communications, which have very stringent QoS requirements. The Internet Protocol security (IPsec) [14] has been proposed to provide security services for the Internet traffic. IPsec has recently been extended to support multicasting [15], but it only supports a uniform security policy per group. In addition, it does not defend against outsider attacks (such as a denial-of-service attack), and such defense is critical to the vulnerability of the smart grid.

Information architecture for supporting fault-tolerance and scalability requirements of a power system was proposed in [16]. The proposed layered architecture aims to support coarse real-time guarantees (typical deadlines in hours) at the top layer (such as the energy trading system) and fine-grain guarantees (at substations with deadlines in seconds) at the lower layers. Multi-protocol label switching (MPLS)-based virtual private network (VPN) through a firewall is employed for the provision of timely and secure information exchange among communicating devices. Nevertheless, it relies only on the existing network technology so that it is not possible to support any configurable, policy-based QoS guarantees (latency, reliability, and security level) and communication mechanisms.

In [17], GridStat has been proposed as a middleware framework to provide flexible, robust, and secure data communication for the operations in a power grid. It has been designed to be implemented on top of any kinds of networks, such as IP networks and ATM networks. It aims to manage network resources for offering QoS-managed low-latency, reliable multicast delivery of information across the grid. The idea is to employ a publish-subscribe communication model so that a source announces the availability of data to the management plane and publishes data items, which are distributed to destinations as subscribers. The subscribers make requests to the middleware to set up paths for the delivery. This substantially simplifies the application programs. Besides, GridStat makes use of a set of hierarchically arranged QoS brokers and a set of status routers for the provision of scalable policy-based QoS guarantees with proper bandwidth allocation among various applications. Nevertheless, GridStat employs static routing that is more susceptible to network failures (such as device or link failures). Moreover, security and trust requirements have not yet been addressed.

IEC 61850 has been adopted as a standardized communication technology for interoperability among communicating devices, known as intelligent electronic devices (IEDs) for substation automation systems [18]. However, it does not devise any mechanisms for the provision of QoS guarantees or any delivery mechanism for wide-area control of a smart grid.

A secure communication infrastructure is crucial to smart grid operations. In March 2009, some cyber security experts said that some types of smart grid sensors can be hacked easily [19]. On the other hand, worms can easily spread among smart grid sensors according to a journal article released on June 18, 2009 [20]. We have identified several attacks which may be launched on the smart grid:

1. Distributed Denial-of-Service (DDoS) attack: In a DDoS attack, a group of distributed and hacked sensors simultaneously and continuously send a large volume of traffic to a victim sensor or even the central server. As a result, normal data cannot be handled properly. Methodologies should be developed to enable a network node (i.e. the sensor) to identify that the network traffic is authentic, and in case a network node malfunctions, allow other nodes to become aware of this fact.
2. Simultaneous shut-down attack: An attacker (as a malicious server) can send out fake control messages to instruct thousands or even millions of sensors to shut down simultaneously to render the smart grid network ineffective. Therefore, it is important to ensure the confidentiality, integrity, and authenticity protection of the instructions.
3. Fake demand for power: An attacker can intercept or alter messages in the network and then dramatically increase or decrease the demand for power. This disrupts the load balance maintained in the system and can cause a sudden power blackout. Besides, the attacker can also drop some of the messages so as to affect the statistical analysis at the central server. Again, it is important to ensure the confidentiality, integrity, and authenticity protection of the data transmitted.

To summarize, there is a need for a new information architecture that can support policy-based multicast communication services with a vast variety of QoS guarantees (in latency, reliability and fault-tolerance, and security/trust level) as well as the *seamless* interaction and interoperability with existing power system standards (such as IEC 61850) and the underlying communication networks.

IV. CONCLUSION

With the increasing penetration of renewable energy sources such as solar and wind in power systems, and the application of demand response and smart electrical appliances, the supply and demand for electricity become very dynamic. The traditional centralized system operation model may no longer hold. The infrastructure revolution of using modern technologies such as communication, sensor network, power electronics devices and control technologies can facilitate real-time power system operation and improve operation efficiency. Simply building hardware for the renewable generators and the smart grid but still using the existing operating paradigm of the grid will result in limited achievement of the ultimate goal of carbon reduction. A new paradigm for power system dispatch is necessary. A new operating paradigm, namely, risk-limiting dispatch, is proposed for the smart grid. In addition, we have identified the requirements of the communication infrastructure to support the smart grid and risk-limiting dispatch.

REFERENCES

[1] "Smart Grid," available at: http://www.oe.energy.gov/smartgrid.htm.

[2] "European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future," European Commission, Directorate-General for Research, Sustainable Energy Systems, EUR 22040, 2006.

[3] "Intelligrid," available at: http://intelligrid.epri.com/

[4] "Grid 2030: A National Vision for Electricity's Second 100 Years," US Department of Energy, 2003.

[5] "NIST Framework and Roadmap for Smart Grid Interoperability Standards," Release 1.0, NIST Special Publication 1108, Jan. 2010.

[6] F. F. Wu, K. Moslehi, A. Bose, "Power System Control Centers: Past, Present and Future," *Proceedings of the IEEE*, Vol. 93, Issue 11, Nov. 2005, pp. 1890-1908.

[7] F. F. Wu and Y. K. Tsai, "Probabilistic Dynamic Security Assessment of Power Systems, Part I: Basic Model," *IEEE Transactions on Circuits and Systems*, Vol. CAS-30, March 1983, pp. 148-159.

[8] F.F. Wu, Y.K. Tsai, Y.X. Yu, "Probabilistic Steady-state and Dynamic Security Assessment," *IEEE Transactions on Power Systems*, Vol. PWRS-3, February 1988, pp. 1-9.

[9] C. Gellings, "Smart Power Delivery: A Vision for the Future," *EPRI Journal*, 9 June 2003.

[10] D. E. Bakken, C. H. Hauser, H. Gjermundrød, and A. Bose, "Towards More Flexible and Robust Data Delivery for Monitoring and Control of the Electric Power Grid," Technical Report EECS-GS-009, School of Electrical Engineering and Computer Science, Washington State University, 30 May 2007.

[11] J. E. Dagle, "Postmortem Analysis of Power Grid Blackouts," *IEEE Power and Energy Magazine*, Vol. 4, No. 5, September/October 2006, pp. 30-35.

[12] J. Postel, "Transmission Control Protocol," Request for Comments, RFC 793, Protocol Specification, DARPA Internet Program, September 1981.

[13] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control," Request for Comments, RFC 2581, Network Working Group, Internet Engineering Task Force, April 1999.

[14] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," Request for Comments, RFC 4301, Network Working Group, Internet Engineering Task Force, December 2005.

[15] B. Weis, G. Gross, and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol," RFC 5374, Network Working Group, Internet Engineering Task Force, November 2008.

[16] Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An Information Architecture for Future Power Systems and Its Reliability Analysis," *IEEE Transactions on Power Systems*, Vol. 17, No. 3, August 2002, pp. 857-863.

[17] H. Gjermundrød, D. E. Bakken, C. H. Hauser, and A. Bose, "GridStat: A Flexible QoS-Managed Data Dissemination Framework for the Power Grid," *IEEE Transactions on Power Delivery*, Vol. 24, No. 1, January 2009, pp. 136-143.

[18] M. Vadiati, M. A. Ghorbani, A. R. Ebrahimi, and M. Arshia, "Future Trends of Substation Automation System by Applying IEC 61850," Proceedings of the 2008 43rd International Universities Power Engineering Conference (UPEC), Padova, Italy, 1-4 September 2008.

[19] Jeanne Meserve, " 'Smart Grid' May be Vulnerable to Hackers," CNN.com, 21 March 2009. (Available online: http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html).

[20] "The Security Vulnerabilities of Smart Grid," Journal of Energy Security, 18 June 2009. (Available online: http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96).