# Form Follows Function

IMAGE LICENSED BY INGRAM PUBLISHING

**By Miles H.F. Wen and Victor O.K. Li**

## Designing Smart Grid Communication Systems Using a Framework Approach

*Digital Object Identifier 10.1109/MPE.2014.2301536*
*Date of publication: 17 April 2014*

IN THE TRADITIONAL ELECTRICITY GRID, THERE are four major components: power generation, power transmission, power distribution, and grid operation. Power generation usually consists of numerous types of generation plants, such as fossil-fuel power plants and nuclear power plants. The generated electricity is fed into the transmission network, which primarily consists of high-voltage (HV) or extra-high-voltage (EHV) transmission lines and transmission substations and delivers power over long distances. When the electricity arrives at locations in close proximity to utility customers, it is handed over to the distribution subsystem and then dispatched to the customers. Power operation monitors and controls the flow of electricity and all grid components and is essential to the proper functioning and efficiency of the grid.


1540-7977/14/$31.00©2014IEEE

After having served us for more than a century, existing electricity grids have been found incapable of satisfying our desire for greater system reliability and for increased usage of renewable energy sources so as to reduce emissions of the greenhouse gases that cause global warming. It has been observed that the U.S. electricity grid has become increasingly unreliable over the past few decades, with sharp increases in both the number of outages per year and the severity of the consequences of those outages. And due to the nature of electricity, the amount of generation and consumption should be exactly matched at any given instant in time. Otherwise, either the excess amount of electricity generated is wasted or power outages will occur due to insufficient energy supply. In the existing electricity grid, numerous schemes have been developed to balance generation and consumption. Because of the stochastic nature of renewable energy generation, however, none of the existing schemes will be adequate when there is a high percentage of renewable energy generation in the grid. Studies have shown that no more than 10% of renewable energy can be tolerated by most existing electricity grids. In addition, there is a desire to involve customers in grid operations, for example by letting them schedule their electricity consumption based on differential pricing or even generate electricity and sell excess generation to the grid. As a result, there is an urgent need to upgrade the existing grid. The future electricity grid that will result has been dubbed the "smart grid." This future smart grid will be capable of:

- ✔ accommodating a high percentage of renewable energy generation
- ✔ providing high-quality and highly reliable electricity services to customers
- ✔ actively involving consumers in grid operations.

To successfully complete the upgrade to a smart grid, advanced communication technologies are essential. The benefits offered by these technologies include more accurate and timely dissemination of state information about the grid, which lets grid operation programs carry out precise and efficient real-time scheduling to alleviate the problems brought about by the volatility of renewable generation and fluctuations in customer demand.

This article aims to give an introduction to the smart grid from the perspective of a communication engineer; it describes a communication-oriented smart grid framework originally proposed by the authors in 2011. The article also aims to provide readers with a comprehensive understanding of the communications issues surrounding the smart grid so that they may use the framework discussed to properly design a smart grid communication system.

After familiarizing readers with the fundamentals of electricity grid and smart grid, we introduce a three-entity, high-level, communication-oriented framework for the smart grid. Then we give readers a closer look at each entity and discuss possible communication issues. Before concluding, we provide an illustration of how the framework can be used to design smart grid communication systems.

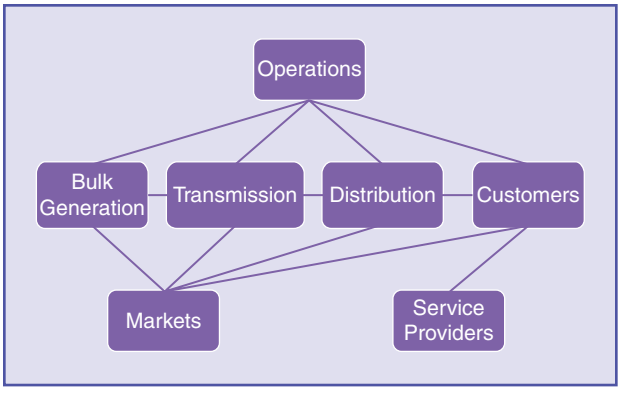


**figure 1.** The seven-entity smart grid framework proposed in 2010 by NIST.

## A Smart Grid Framework

In January 2010, the U.S. National Institute of Standards and Technologies (NIST) issued a document that addresses the interoperable framework for smart grid. As shown in Figure 1, the proposed framework consisted of seven entities: operations, bulk generation, transmission, distribution, customers, markets, and service providers. The idea was that with the help of properly designed communication networks, these seven entities could communicate and interact with each other. After careful investigation, however, we have concluded that although this framework serves as a good reference to help engineers with a background in power systems understand numerous smart grid issues, it does not include enough details about the communication aspects of the problem. We have therefore proposed a three-entity smart grid communication framework.

As shown in Figure 2, the smart grid communication framework consists of three entities: the operation network, the business network, and the consumer network. Each of the three represents a different set of communication networks serving different functions. The operation network is primarily used by power companies to help maintain grid functionality. The business network is used by participants in the electricity market to efficiently regulate the market as well as to provide electricity services to consumers. The consumer network is used by each consumer for home energy management so as to enhance the electricity usage experience.

Readers can interpret *operation network* to mean the backbone network of the smart grid communication system. Its design requires a deep understanding of the existing power system and will very likely involve collaboration with power system and communication engineers. The business network can be regarded as the connection between the operation network and the consumer network; it aims to maximize the efficiency of the electricity market. The business network's design requires knowledge of economics and government policies. The consumer network can be seen as

serving the end users so as to exploit the advantages conferred by the other two entities.

One of the important merits of this three-entity framework is that it clearly captures the major differences between the communication systems used in traditional electricity grids and in smart grids. In particular, if we were to use this framework to represent the communication system typically used by traditional electricity grids, only the operation and business networks would be necessary.

## Communications Within and Between Entities

In this section, we describe the internal structures of each entity in our proposed framework. We discuss the communication issues within each entity and between entities.

### *Communications in the Operation Network*

As shown in Figure 3, the operation network consists of seven major components: the business network gateway (BNG), consumer network gateway (CNG), control centers (CCs), generation station (GS), substation (SS), transmission facilities (TFs), and wide-area monitoring and control network (WAMCN).

The BNG and CNG are the communication bridges connecting the operation network with the other two entities. Since each of the three entities is used by different parties and serves different purposes in the smart grid, when interentity communications are needed, the BNG and CNG serve as firewalls that protect the operation network from external, malicious attacks. Designing the BNG and CNG so that an adequate level of security can be provided without incurring too much communication delay remains an unsolved problem, however. Furthermore, it has not yet been decided who should maintain and operate the gateways.

CCs are the smart grid's central control units. The monitoring and control database (MCDB), the database storing all grid operation information, is accessed by CCs and maintained by database managers. In the traditional electricity grid, CCs follow a strict hierarchical design, with each grid area controlled by a single CC that in turn is controlled by upper-level CCs. A distributed CC design, however, has strong advantages over the centralized one in increasing service availability. The distributed CC design is therefore taken as the future of control in the smart grid. The distributed design introduces many challenging problems, however. One such problem is the additional communication latency brought about by distributed CCs, especially when software techniques, such as middleware, are used. Since CCs must sometimes process urgent messages from GSs, TFs, or SSs and respond promptly, minimizing the extra communication delay is critical. Another problem is security. Since multiple CCs will be monitoring and controlling the same area in the distributed scenario, if an intruder manages to hack into any one of them, he may be able to gain access to all the electrical components in the area. For this reason, the "multiple points of attack" issue must be carefully addressed. In addition, it is worth noting that when a distributed CC design is adopted, the MCDB should also adopt a distributed design. If a distributed design is not used and the MCDB remains centralized while CCs are distributed, the MCDB will become the system performance bottleneck and a single point of failure.

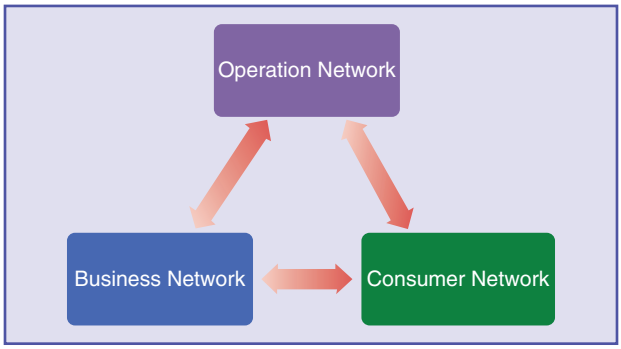


**figure 2.** A three-entity smart grid communication framework proposed in 2011 by Wen et al.

The GS component usually consists of a collection of large power generation stations, each of which may contain many sensors and actuators connected by a local-area network (LAN) and controlled by a local control unit. The local control unit in each GS communicates with CCs via the WAMCN, through a gateway. This second gateway, which complements the CNG and BNG, is used to prevent insider attacks initiated by someone who has managed to get into the WAMCN. Since many different protocols for GS-CC communications have been developed during the past decades, a protocol translator is needed to make the smart grid compatible with legacy technologies. Designing an efficient and effective protocol translator remains an unsolved problem, however. Designing the LAN inside a GS is also challenging because this LAN must be capable of:

- ✔ providing a level of communication quality of service (QoS) compatible with IEEE Standard 1646–2004
- ✔ functioning partially independently of local power generation, i.e., functioning for certain time periods even if the generators at the GS are down
- ✔ functioning with strong resilience against extreme physical working conditions, such as high temperature, strong vibration, and so on.

The SS component is the collection of transmission and electricity distribution substations. It typically has a communication structure similar to that found in the GS component. Since distribution substations sit close to consumers and are sometimes configured so as to have access to consumer data via the CNG, the privacy of those data must be carefully protected. Other than that, the communication requirements inside the SS and GS components are mostly the same.

The TF component consists of the assets involved in long-distance electricity transmission. Although these

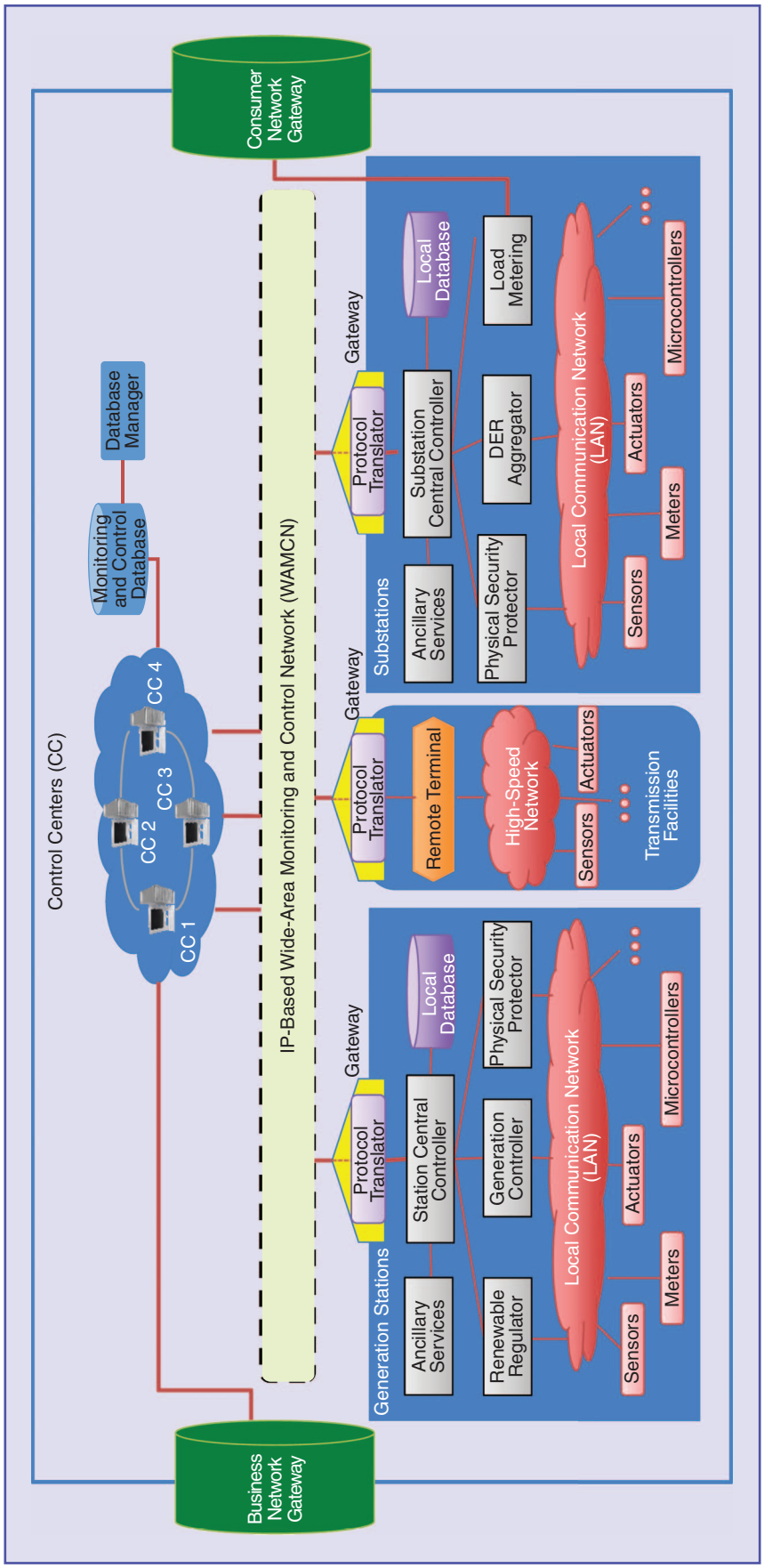


**figure 3.** The operation network (courtesy of Wen et al.).

assets actually include transmission towers (called electricity pylons in the United Kingdom) and underground cables, from the viewpoint of communication, the TF component merely consists of some remote control terminals and a huge number of sensors and actuators located across a wide area. These terminals, sensors, and actuators are connected via a wide-area, high-speed network. Usually, data gathered by the TF component are concentrated by remote control terminals to avoid network congestion before being sent into the WAMCN and delivered as needed. Sometimes, it is also desirable to have the remote control terminals encrypt the TF data to ensure security. As a result, it is challenging to design the concentration and encryption algorithms for the TF component such that satisfactory services can be provided without creating too much computation overhead. Moreover, designing the high-speed network for the TF component is another problem.

Last but not least, the WAMCN is the backbone of the operation network and is used to transfer huge volumes of data among the GS, TF, SS, and CC components. In designing the WAMCN, the following requirements must be met:

- ✔ **High availability:** Since the unavailability of the WAMCN means the loss of most communication services, it is crucial that backup schemes for this network be properly provisioned.
- ✔ **High security:** Although gateways such as the CNG and BNG are installed in the operation network, the routers and switches inside the WAMCN still need to be able to resist insider attacks.
- ✔ **QoS:** Since different types of data are needed by different parties and different applications, the WAMCN

needs to be able to prioritize data transmissions according to needs.

- ✔ **Compatibility:** During the process of upgrading the existing grid to the smart grid, it is possible that multiple legacy protocols that are incompatible with each other will be used simultaneously in the operation network. As mentioned earlier, protocol translators in the GS, TF, and SS components can help alleviate such problems. The WAMCN must employ a globally accepted protocol such as the Internet Protocol (IP) to truly accommodate such compatibility requirements, however.

### *Communications in the Consumer Network*

As shown in Figure 4, the consumer network is made up of six major components: the BNG and operation network gateway (ONG), the smart meter (SM) component, the home electronics (HE) component, local energy management (LEM), a smart controller (SC), and a LAN.

Like the BNG and CNG in the operation network, the BNG and ONG here serve as the primary protectors of the information inside the consumer network against intrusions by outsiders. Since data protection requirements at the consumer end are usually less stringent than those in the operation and business networks, designing these two gateways is a simpler task, and the only major concern is the protection of consumer privacy. In other words, the BNG and ONG in the consumer network should be designed in such a way that consumers are aware of the types of information being requested by other parties and are capable of deciding whether or not the requested information should be released.

The SM is the electricity meter, with a built-in communications module and processor. It receives real-time electricity price data from the business network and sends consumer consumption profile data to the operation network. The price information the SM receives is used by other components in the consumer network to perform various functions, and the consumption profile data the SM sends out are used by applications in the operation network as feedback data. As a result, it is important to design the communication protocols used by the SM to facilitate communication with other entities. One of the best known of these is the draft standard on an application-layer SM communication protocol published by IEEE in March 2012 (IEEE P1377/D11).

The HE component consists of the collection of electrical appliances, such as washers and air conditioners, controllable by the SC. Based on the current electricity price, consumer requirements, and the environmental data collected by the sensors on those appliances, the power level of these appliances may be automatically adjusted to reduce overall electricity costs. An extra gateway is proposed to control access to the HE component, for security reasons. This gateway provides security functions, such as an authenticity check, to protect the appliances from being controlled by unauthorized parties. The design of this new gateway is a critical area for future research. More important, the communication protocol to be used between the HE and SC components is awaiting development and standardization.

LEM is present on the consumer network to accommodate distributed energy generation, such as small-scale wind generation or solar panels, and/or larger energy storage devices, such as electric vehicles, at a consumer's premises. With these distributed generation and storage assets, a consumer can actively participate in the electricity market by selling stored electricity when the price is high and purchasing extra electricity when the price is low. LEM is under the control of the SC, and the decision is made largely based on the current electricity price shown by the SM, which is in turn based on the current electricity demand-supply relationship in the market and the operational status of the grid.

The SC is the central controller on the consumer network and is therefore considered its most important component. Since the functionality of the SC relies heavily on the LAN, the LAN is seen as essential to the consumer network. The design of this LAN remains an unsolved problem. Two of its most important general communication requirements can be summarized as follows:

- ✔ **Authenticity:** Since consumers' premises usually sit close to each other, undesirable consequences may be caused if a command issued by the SC in one consumer's home is accepted by the appliances inside another consumer's home. As a result, it is necessary that the LAN in the consumer network be able to encrypt messages in such a way that only authenticated devices

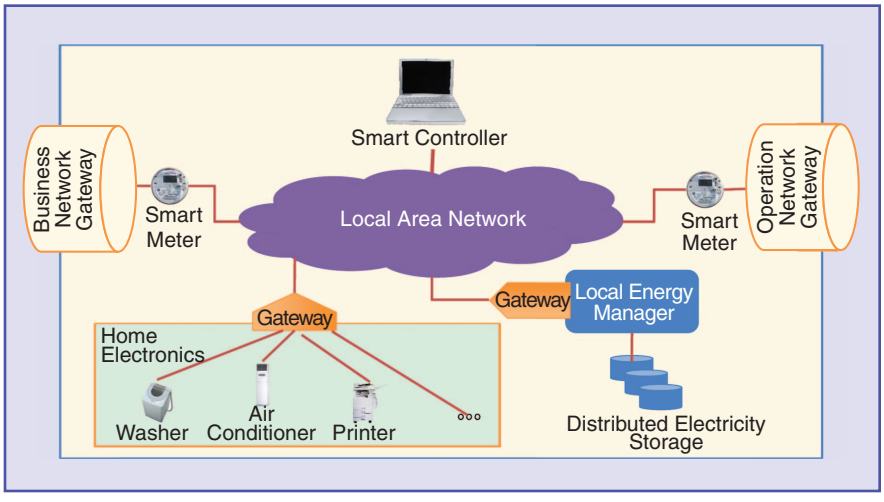


**figure 4.** The consumer network.

can decrypt the contents and only authenticated commands are executed. This functionality may be aided by the HE gateway.

- ✔ **Integrity:** Although the LAN in this context does not require high reliability or low latency, one must ensure that the integrity of messages is strictly guaranteed. For instance, it must be ensured that the HE component will only execute commands issued by the SC if they are guaranteed to have been correctly received.

### *Communications in the Business Network*

Unlike the other two entities, the business network does not possess a dedicated communication architecture. Instead, it includes numerous new participants and players in the electricity market that communicate with each other using an IP-based virtual private network (VPN). As shown in Figure 5, the electricity market regulator, smart meter service provider, demand responder, and electricity market participants are the major players in the business network. There are also parties that communicate with the consumer and operation networks to obtain smart meter data and smart grid operation data via the CNG and ONG, respectively.

Communications within the business network are mostly for commercial use, and hence economy and security are of the utmost concern. This will not be a big issue once an IP-based network is used, however. Since IP has been under development for decades, players in the business network will not have much difficulty finding their desired applications and services from the market.

## Interentity Communications

Interentity communications are very important for the proper functioning of the entire communication system in the smart grid. We will briefly introduce the requirements for such communications here; for more detailed information, see "For Further Reading."

Communications between the operation and business networks require high reliability and security. Those between the operation and consumer networks require high security but relatively lower reliability. For communications between the business and consumer networks, however, only moderate levels of reliability, data availability, and security are required.

## The Way to the Smart Grid

Having introduced the three-entity framework as well as some of the potential communication issues inside each entity and between entities, we now illustrate how this framework can be utilized to help engineers design smart grid communication systems.

After acquiring a fundamental knowledge of smart grid communication systems, engineers should first decide how many of the three entities shown in Figure 2 are relevant to their design project. This will help them clearly understand the following two critical issues before starting their project:

- ✔ **Expertise required:** Generally speaking, designing the communication systems inside the operation network requires expert knowledge of the power system. This means that if a communication engineer works on the operation network, he or she will probably need to collaborate with engineers with power system backgrounds.
- ✔ **Nature of work:** In designing the communication systems within the operation network, compatibility with existing technologies is of the utmost concern, while designing the consumer and business networks requires innovation to enhance the user experience but carries limited compatibility restrictions. For instance, in the traditional electricity grid, the most important communication system is supervisory control and data acquisition (SCADA), used by system operators to monitor the operational status of the entire system and to issue commands to particular components remotely. Recent studies have found that SCADA may be too slow to respond properly to urgent events, however. As a result, a high-speed system offering similar functionalities called a wide-area measurement system (WAMS) has been proposed for use in the smart grid. But since SCADA has been in existence for decades, it is neither economic nor feasible to simply throw it out and use new technologies. As a result, the coexistence of SCADA and new advanced systems such as WAMS is seen as the true future in smart grid communications.

Let us continue the illustration with the assumption that the operation network is relevant. Based on Figure 3, a sequence of design issues for the operation network may be identified by scanning the figure from bottom to top. One such issue discovery process is illustrated by the following steps:

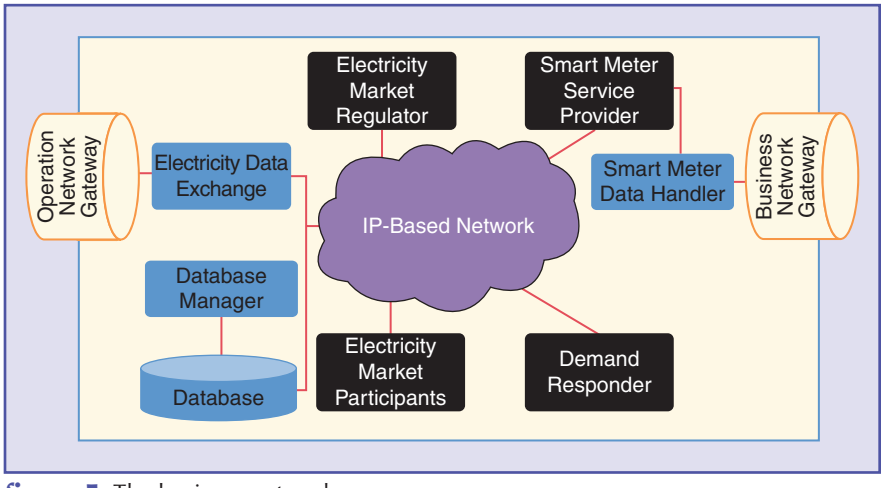


**figure 5.** The business network.

The article aims to provide readers with a comprehensive understanding of the communications issues surrounding the smart grid.

1) Numerous devices, including sensors, actuators, and microcontrollers, are used for controlling and monitoring the GS component. In the design process, the engineers have to deal with numerous design issues by answering the following questions: Which types of devices are needed? How many of each are needed to achieve optimal performance? How should they be placed in a particular GS? With these questions answered, the engineer should look at the LAN connecting the devices and determine its structure and the protocols that could be used based on the communication requirements for this LAN (discussed above).
2) On the boundary of the GS component, there is a gateway and a protocol translator. It is critical for the design engineers to answer these questions: How should the gateway be built and configured so that an optimal trade-off between security and processing delay can be achieved? How should the protocol translator be designed for optimal performance? Since compatibility is a critical issue in designing the operation network, the engineer must also take care in deciding which protocols the protocol translator should support.
3) By repeating the first two procedures starting from the bottom of the TF and SS components, respectively, numerous design issues can easily be identified by engineers. With those issues addressed, the WAMCN can be designed in such a way that the communication requirements discussed in earlier sections are satisfied.
4) CCs lie above the WAMCN. As has been discussed above, when CCs become distributed, intercommunications among different CCs are critical. In designing this part of the operation network, engineers must answer the following questions: Will middleware technologies be good for CC? If the answer is yes, which types of middleware will be needed? If not, then what are the other options? Will the existing intercontrol center communications protocol work well enough in a distributed CC scenario?
5) The CNG and BNG can be spotted at the boundary of GS. In addition to addressing how the two gateways should be designed, an engineer also needs to carefully investigate whether the communication protocols used inside and outside the operation network are the same. If not, then protocol translators may be needed. A second issue is how these two gateways transmit data between the operation and consumer networks and between the operation and business networks, respectively. Should they be directly connected to the WAMCN? Or should they be allowed to communicate with specific components inside the operation network only, as indicated in Figure 3?

After completing the process described above, a sequence of design issues will be clearly identified. The design issues for the business network, consumer network, and interentity communication systems can be identified in a similar manner. With the design issues appropriately identified and addressed according to customer requirements, engineers may find it easier to design communication systems for the smart grid.

## Acknowledgment

This work was supported in part by the Collaborative Research Fund of the Research Grants Council, Hong Kong Special Administrative Region, China, under Grant HKU10/CRF/10.

## For Further Reading

M. H. F. Wen, K.-C. Leung, and V. O. K. Li, "Communication-oriented smart grid framework," in *Proc. IEEE SmartGridComm 2011*, Brussels, Belgium, Oct. 2011, pp. 61–66.

*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, National Institute of Standards and Technology (NIST), Jan. 2010.

F. F. Wu, K. Hoslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, Nov. 2005.

C. H. Hauser, D. E. Bakken, and A. Bose, "A failure to communicate: Next-generation communication requirements, technologies, and architecture for the electric power grid," *IEEE Power Energy Mag.*, vol. 3, no. 2, pp. 47–55, Mar./Apr. 2005.

*IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation*, IEEE Standard 1646-2004, Mar. 2005.

*IEEE Draft Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables)*, IEEE P1377/D11, Mar. 2012.

## Biographies

***Miles H.F. Wen*** is with the University of Hong Kong, China.

***Victor O.K. Li*** is with the University of Hong Kong, China.