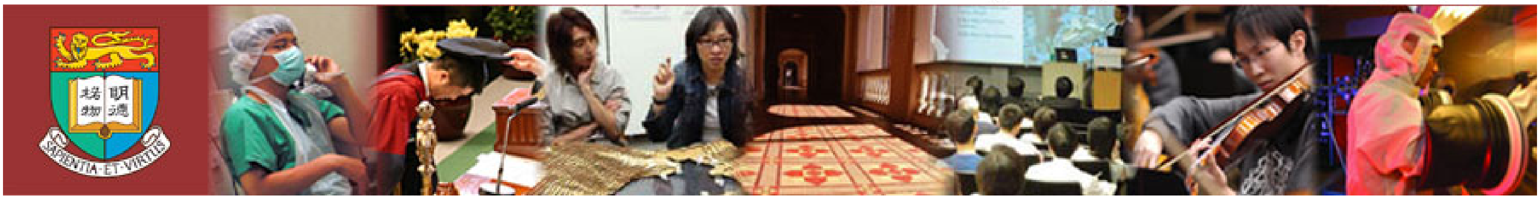

Title	Communication-oriented smart grid framework
Author(s)	Wen, MHF; Leung, KC; Li, VOK
Citation	The 2nd IEEE International Conference on Smart Grid Communications (SmartGridComm 2011), Brussels, Belgium, 17-20 October 2011. In Proceedings of 2nd SmartGridComm, 2011, p. 61-66
Issued Date	2011
URL	http://hdl.handle.net/10722/142812
Rights	Proceedings of the IEEE International Conference on Smart Grid Communications. Copyright © IEEE.

Communication-Oriented Smart Grid Framework

Miles H. F. Wen, Ka-Cheong Leung, and Victor O. K. Li
Department of Electrical and Electronic Engineering
The University of Hong Kong
Pokfulam Road, Hong Kong, China
E-mail: {mileswen, kcleung, vli}@eee.hku.hk

***Abstract*—Upgrading the existing electricity grids into smart grids relies heavily on the development of information and communication technology which supports a highly reliable real-time monitoring and control system as well as coordination of various electricity utilities and market participants. In this upgrading process, smart grid communication is the key to success, and a simple but complete, innovative but compatible high-level communication-oriented smart grid framework is needed. This paper proposes a simple and flexible three-entity framework, so that devices employing the existing technologies are supported and can interoperate with those employing new technologies.**

I. Introduction

The desire to use more renewable energy resources in electricity generation and to achieve more reliable and efficient electricity supplies drives the upgrading of the existing electricity grids into smart grids. In this upgrading process, efficient and effective communication is the key to success.

Due to the stochastic nature of renewable energy resources, maintaining the stability of the power grid as we increase renewable penetration is a major problem. This problem can be alleviated by an advanced high-speed communication network [8]. With the help of such a network, better predictions on renewable energy generations can be realized, allowing utilities to perform real-time scheduling efficiently. Besides, as the traditional large-scale electricity automation systems handle contingencies or faults via their local intelligent facilities and a centralized control centre, the reaction speeds are sometimes very slow, potentially making the system unreliable. To solve such reliability issues, the communication technologies play an essential role, as operators can gain more situational awareness so as to react rapidly and accurately to emergencies [11]. In addition, based on the fact that electricity generation must exactly match the consumption in order to maintain stability of the grid, advanced technologies including generation dispatch and demand-side management are required in smart grids. To achieve full functionalities of such technologies in smart grids, communication plays one of the most fundamental roles.

Therefore, there is an urgent need to design a communication framework for smart grids, on which all smart grid communication technologies can be built. Most of the existing work addressed the communication specifications, but they only focused on some specific parts of the entire smart grid network, rather than gave a complete architectural view. Aggarwal *et al.* [1] presented a communication framework for the distribution network only. In [15], the communication requirements of a smart grid were discussed, but it did not discuss what a framework should look like. Chen *et al.* [3] focused only on the home-area network (HAN). National Institute of Standards and Technologies (NIST) proposed a seven-entity framework for smart grids [12]. As shown in Fig. 1, the framework consists of seven domains or entities, namely, Markets, Service Providers, Bulk Generations, Transmissions, Distribution, Operations, and Customers. Although this high-level framework is complete, it is somewhat too complicated for researchers focusing on the underlying communication networks.

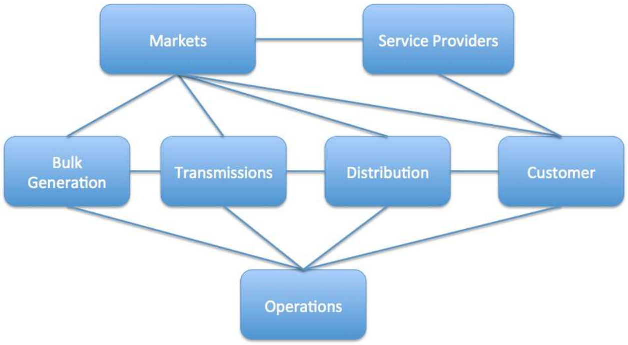

Fig. 1. NIST Seven-Entity Smart Grid Framework.

The purpose of this paper is to introduce a high-level communication framework for smart grids, together with the field-level sub-network architectures. This framework can provide researchers with a better understanding of the entire smart grid communication network, such that better coordination of various technologies can be achieved. After familiarizing readers with the important communication issues in smart grids as well as the significance of our work in Section I, we shall give the reader a brief description on the kind of requirements a communication network must meet so as to support smart grid functionalities in Section II. In Section III, the proposed framework is discussed in details and Section IV concludes this paper.

This research is supported in part by the Collaborative Research Fund of the Research Grants Council of Hong Kong under Grant No. HKU10/CRF/10.

II. Communication Requirements

The fundamental function of smart grids is to deliver stable and reliable electricity services to consumers. To ensure this function, certain specific communication requirements must be met in designing a smart grid network. The essential requirements are summarized as follows.

- *Cyber Security*: According to NIST [16], cyber security refers to all the security issues in automation and communications that affect any functions related to the electricity power systems. Specifically, it involves the concepts of integrity (data cannot be altered undetectably), authenticity (the communication parties involved must be validated as genuine), authorization (only requests and commands from the authorized users can be accepted by the system), and confidentiality (data must not be readable to any unauthenticated users). As one of the most critical assets of a nation, the smart grid network must be robust against any cyber threats. Data integrity, authenticity, and authorization must be maintained at a very high level. Traditionally, the confidentiality issues were not considered important [14], [17]. Even in some SCADA systems used for grid monitoring and remote control, the employed protocols, such as Distributed Network Protocol 3.0 (DNP3) [6], do not support confidentiality. However, we believe that this is no longer true for smart grids. Allowing outsiders to access grid monitoring and control data may potentially allow them to analyze the grid status. If some terrorists have that kind of knowledge, they may possibly launch attacks on these electricity facilities when the system-in-fault signals are detected in the monitoring data, as that will be when the entire grid system becomes weak and vulnerable. Moreover, smart grids extend the scope of the grid system as they are no longer confined within the power systems and electricity utilities, but allow consumers and market entities to get involved actively. Under this situation, confidentiality must be maintained in the communication activities for the consumers and markets.
- *Availability*: In the smart grid network, availability refers to the requirement that any piece of important data, such as the monitoring data and control commands, is guaranteed to reach their destinations successfully within an acceptable time period. The traditional electricity grids tend to deploy proprietary networks with very limited coverage and bandwidth, making local systems unaware of system-wide conditions. This in return causes the grid to fail in some situations [5].
- *Quality of Service (QoS)*: In communication networks, QoS refers to the capabilities of the system to provide different levels of priorities to different applications or users so that each application or user can achieve its required level of performance either deterministically or probablitistically. The performance of an application can be defined in terms of delivery latency, delay jitter, connection bandwidth, and so on. Although different applications in smart grids may have different QoS requirements, it is expected that the QoS requirements for grid operation applications would be stringent. Any fault which cannot be discovered and cleared within a short period of time can potentially cause severe problems, such as power outages or damage to facilities, and hence is unacceptable. The two most important factors of rating the electricity quality, namely, the electricity adequacy and continuity of supply, both depend heavily on the QoS provided by the communication network in a smart grid. On the other hand, the QoS requirements are relatively less stringent for applications dealing with consumers and market participants since these applications are usually not directly related to the operation and maintenance of smart grids.

III. Communication Framework

In this section, a new communication-oriented framework for smart grids is introduced. We first describe the three-entity framework, which is designed to be technology-neutral so that any new technologies suitable for smart grids can be adopted in the proposed framework. Given the simple, complete yet flexible framework, the communication requirements specified in Section II can be accommodated by implementing and deploying existing and new technologies.

A. Three-Entity Framework

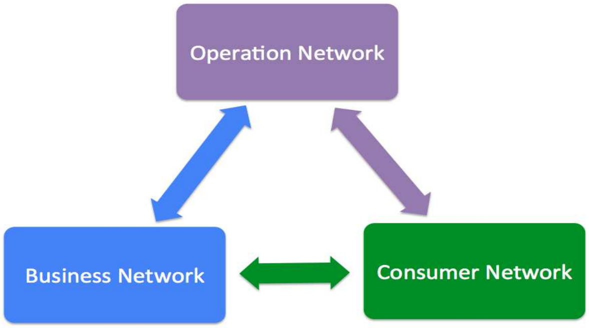

Fig. 2. Three-Entity Framework for Smart Grid Communication.

The proposed smart grid framework consists of three entities, namely, Operation Network, Business Network, and Consumer Network, as depicted in Fig. 2. Operation Network refers to the network for managing electricity generation, transmission, and distribution, typically including automation technologies related to the legacy SCADA systems, Wide-Area Measurement Systems (WAMS), and large-scale Energy Management System (EMS). Business Network refers to the network used by the electricity market participants, such as the metering service providers and government regulators, to coordinate the electricity market, and Internet technologies play a key role. Consumer Network handles the communication for the electricity consumers. It includes a HAN as part of the advanced metering infrastructure (AMI). Details of each entity will be addressed in the subsequent sub-sections.

The design principles for the proposed three-entity framework are shown as follows:

- *Simplicity*: Obviously, as a high-level framework of the entire system, the fewer entities and less inter-entity communication we have, the easier it will be for us to analyze and develop further. As far as we know, this framework is by far the simplest one being proposed for the smart grid communication.
- *Completeness*: This framework represents a simple yet complete picture for the smart grid communication network. The service blocks in the framework represent all possible existing and future applications in smart grids.
- *Compatibility*: The proposed framework is compatible with the one from NIST as exhibited in Fig. 1. Operation Network in our framework includes the domains of Operations, Bulk Generations, Transmissions, and Distribution from the NIST framework. Business Network in our framework contains NIST's domains of Markets and Service Providers. Consumer Network is the same as the domain of Customers. As a result of this compatibility, one can enjoy the nice features of this framework without incurring extra overheads by adopting our proposed framework instead of the NIST framework for smart grid research and development.
- *Ease of deployment*: We have identified three major levels of communication requirements. Those parties at the same level are grouped together into the same entity in our framework. Generally speaking, Operation Network requires the most stringent requirements in cyber security, data availability, and QoS. Business Network requires relatively less stringent in the requirements. Consumer Network has the lowest level of requirements as compared to the other two networks. Hence, it is a good idea to separate them from each other for ease of network deployment and inter-entity communication control.
- *Ease of evolution*: Generally speaking, Operation Network has been in existence for decades as the core of power system automation, for which companies have already made huge investments. Our future research efforts in this area will likely focus on allowing the existing network to evolve and meet the requirements for smart grids. Internet technologies have been proposed for supporting Business Network of smart grids [9]. Research efforts will probably be focusing on designing new applications and electricity market regulation schemes, such as in [9] and [13]. Consumer Network is still at the primitive stage, research efforts will have to be spent on designing new technologies, including smart metering and distributed energy resource (DER) management.
- *Ease of collaboration*: The future electricity system calls for efforts not only by the electrical engineers, but also other stakeholders, such as networking engineers, business experts, and government officials. Hence, in designing a communication-oriented framework, we also need to consider how experts from various fields can collaborate more efficiently.

B. Operation Network

Operation Network is the part of a smart grid that primarily handles electricity generation, transmission, distribution, and services to maintain the stability and efficiency of the entire system.

There are eight major components in the entire operation network. Their detailed descriptions are given as follows.

- *Business network gateway* and *consumer network gateway* are the bridges between Operation Network and Business Network, and between Operation Network and Consumer Network, respectively. In our design, gateways are used for this kind of inter-domain communication primarily for security reasons. Since the business network and consumer network are more exposed to the end users, we must strictly control their connectivities to the grid operations since some malicious users may try to infiltrate or hack into the electricity systems and initiate attacks.
- *Control centres* are where grid operation data are gathered and processed. Different control centres collaborate with each other for controlling the same operation area via a dedicated, secure, high-speed network to manage the various facilities in a smart grid. Traditionally, one single control centre is assigned for one big operation area, as deployed under SCADA. However, distributed control centres have been proposed and deployed for achieving better reliability [18]. Hence, in our architecture, we have a dedicated and separate network for all control centres to coordinate with each other. Such control centre network will have to be highly secured and operate under an extremely fast interconnection speed.
- A *monitoring and control database* is used to store the historical data of the utilities, including the status parameters of the grid during its operation, event logs for operators, and so on. A dedicated manager may be needed for maintaining the database, as the gigantic database used in a smart grid may be geographically dispersed. Such distributed databases must be very well-coordinated in order to function properly.
- A *wide-area monitoring and control network (WAMCN)* is a wide-area network for control centres to acquire data from the remote stations or substations as well as issuing the control commands. Moreover, these remote stations can communicate with each other to gain a better awareness on the neighbouring environment. We believe that an IP-based network will be most suitable for WAMCN in Operation Network for its scalability, ease of deployment, and availability of various applications. Despite the numerous advantages, there are two very important drawbacks of an IP-based network, namely, its lack of security and lack of QoS guarantees. However, there are various alternatives to handle these problems. Internet Protocol Security (IPsec) [10] can be employed, if needed, for providing some of the required security services in WAMCN. Other security services can also be implemented by the specific applications themselves, according to their specific security requirements. Besides, QoS can be supported via some middleware, such as GridStat [4], which can be built on top of an IP-based network to provide the desired QoS guarantees.

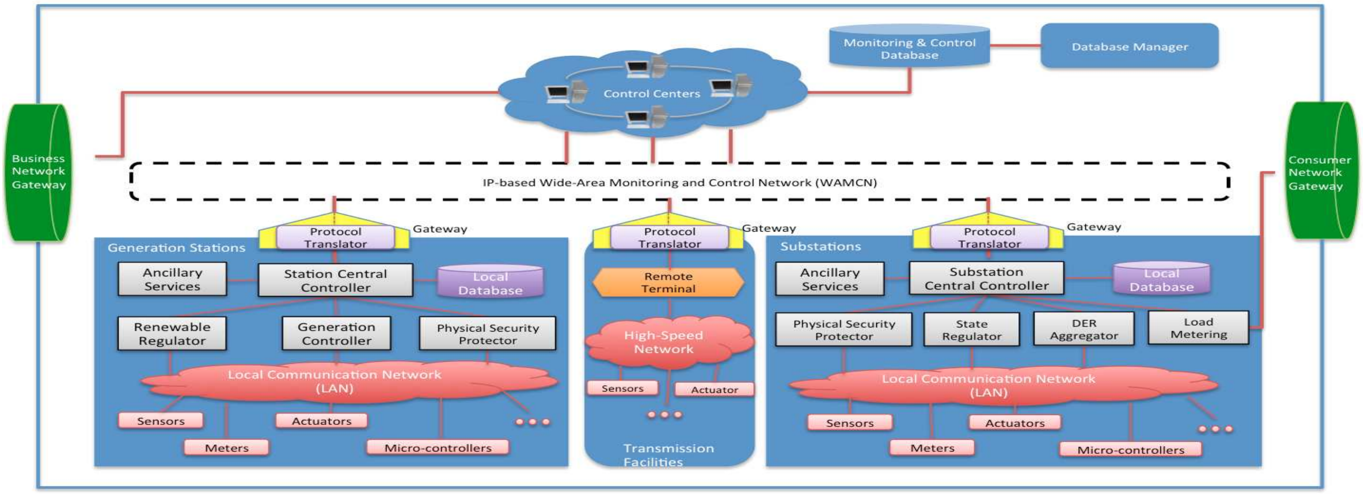

Fig. 3. An Illustration of Operation Network.

- A *generation station* is where a large-scale electricity generation plant resides to generate electricity for the grid. In each generation station, a gateway with a built-in protocol translator is used for connections between the station networks and WAMCN. It is needed primarily because of compatibility and security reasons. Although outsider attacks can be blocked by inter-domain gateways, we need to provide capabilities to the network for preventing insider attacks, which are initiated by attackers inside Operation Network but cannot be effectively defeated by the traditional grid system. Despite the various services provided by different applications in a station, the most important component is a high-speed local area network (LAN), which connects all sensors, actuators, and other devices together with a station controller. The sensors are essential to the grid monitoring system, whereas the actuators play key roles in grid control. The speed of the LAN determines, to a large extent, how quickly contingencies can be detected and how rapidly the system can react to such anomalies.
- *Transmission facilities* are the collection of field devices far away from both power stations and substations. Most of these devices are monitoring devices (such as sensors) and control devices (such as actuators). They need to communicate with the control centres or nearby substations so as to provide status feedbacks of the working facilities. However, as more and more devices are deployed in a distributed manner, WAMCN could fail to scale well if these devices connect to it directly. Hence, they should be grouped according to their locations and connected by the same LAN when they belong to the same group. Data can be gathered and pre-processed by a remote terminal connecting to the LAN. The terminal can then communicate with other components via WAMCN. Due to the concerns about security and compatibility, a gateway installed with a protocol translator acts as a relay between WAMCN and the terminal.
- A *substation* distributes electricity to the consumers. Similar to a generation station, a gateway is needed for a substation to access WAMCN. A high-speed LAN is needed for connecting sensors and actuators within a substation. Since a substation usually reside near the consumers, it can fetch smart meter data from Consumer Network via a consumer network gateway.

C. Business Network

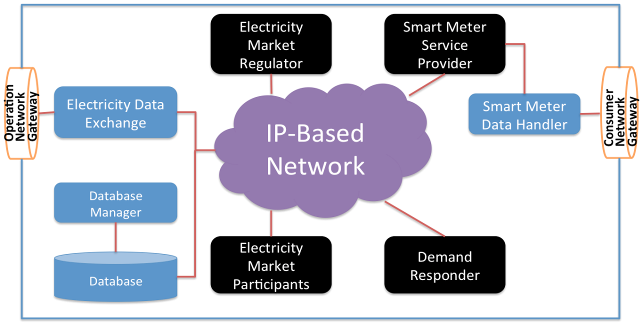
Operation Network Gateway
Electricity Market Regulator
Smart Meter Service Provider
Consumer Network Gateway
Electricity Data Exchange
Smart Meter Data Handler
IP-Based Network
Database Manager
Database
Electricity Market Participants
Demand Responder

Fig. 4. An illustration of Business Network.

The development of smart grids gradually spurs the architectural change in the electricity market, as more services can be offered and the market itself will become more open. Detailed discussions on the changes are beyond the scope of this paper. Instead, we investigate the key players needed in Business Network.

The backbone of Business Network, as depicted in Fig. 4, is an IP-based virtual private network (VPN). The major players in this network are: electricity market regulator, smart meter service provider, demand responder, electricity market participants, and database manager.

- An *electricity market regulator* primarily refers to the government organization which carries out market regulations.

The major duties include the regulation of the electricity rates, which should be maintained at an affordable level.

- *Smart meter service providers* are utilities providing smart metering services to customers. The smart metering services include functions like periodically updating the electricity rate on the smart meters, collecting the electricity consumption profiles from customers, and distributing the available profiles to other authorized utilities in Business Network.
- A *demand responder*, which is different from just providing demand response (matching the electricity generation with power consumption), refers to electricity utility to perform functions by altering the electricity consumptions from the consumers in order to match them with the given or expected power generation. This can be achieved either implicitly by giving incentives to consumers to consume less when the total demand is high, or explicitly by switching on or off some appliances at the consumers dynamically. The former approach can be achieved with the help of smart metering, whereas the latter one can be realized, say, by demand dispatch [2].
- *Electricity market participants* refer to the parties that handle the trading of electricity as well as electricity services to customers. When the electricity market is open and electricity can be traded dynamically, the electricity brokers may match the electricity purchasers with the appropriate sellers. Alternatively, as suggested in [9], consumers can place an electricity order a day in advance online via the Internet. To support such an online electricity purchasing system and the provision of electricity services, some new market participants would emerge in the electricity market.
- A *database manager* is needed for managing the electricity market information in the databases.

D. Consumer Network

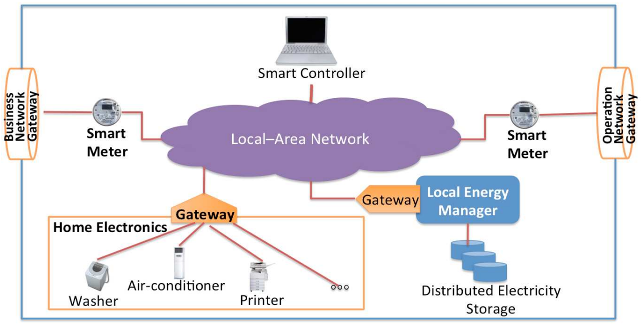

Fig. 5. An illustration of Consumer Network.

As illustrated in Fig. 5, Consumer Network is a LAN on a consumer's premise. This network can be within an apartment or an entire building. The smart metering technology plays an important role in this network.

The communication technology being or to be used in Consumer Network varies, depending on the specific customer requirements. For example, Zigbee [7] can be used in networks where consumers demand high reliability, local mobility, and connectivity. However, whichever technology is selected, the confidentiality among different consumer networks must be guaranteed. In other words, there must be certain levels of segregation among different consumer networks such that any data communication within one network cannot be observed nor affected by those in the neighbouring networks.

Besides the communication technology, the major components in Consumer Network is summarized and discussed as follows:

- A *smart controller* works as the coordinator of the entire home network. Its functionalities include switching on or off loads automatically according to the current grid operating status based on the agreed contracts, analyzing metering data from the smart meters, giving electricity usage suggestions to consumers, managing the local energy storage, and so on. Although there is only one single smart controller depicted in Fig. 5, multiple smart controllers can exist at the same time to improve the reliability of the network.
- A *smart meter*, which connects to Operation Network and Business Network, gathers the electricity usage profile and receives the real-time price data for a consumer. It can support dynamic pricing, which is an electricity pricing scheme to allow utilities to change electricity rates based on the expected consumption levels.
- *Home electronics*, or appliances, mainly refer to electronics, such as washers and air-conditioners, which contribute to the daily electricity consumption of a customer. In Consumer Network, these electronics can be controlled manually by a consumer, or automatically by a smart controller. A proper scheduling for the usage of these electronics can lower the electricity bill of a consumer. It can also help the grid operators maintain load balancing. Since the functionalities of these appliances may directly affect the daily lives of the consumers, we must ensure that, even if hackers can somehow infiltrate into Consumer Network, it will be very difficult for them to take control of these appliances. Hence, we need to maintain a gateway between Consumer Network and the home appliances.
- A *local energy manager*, contrary to the large-scale EMS embedded in Operation Network, handles a relatively small amount of energy generation and storage at the consumer end. With a smart controller, it allows the sale of electricity from a consumer. Similar to the home electronics, a gateway is needed in the energy manager for addressing the aforementioned security issues.

E. Inter-Entity Communications

Communications among different entities are important so as to support communication in the entire smart grid. In this section, we will give some highlights on the basic requirements.

The communication between Operation Network and Business Network requires high reliability and security, as these two entities form the backbone of the entire smart grid network. A typical type of such infrastructure is a point-to-point communication paradigm, which can offer very high levels of security and reliability despite its high deployment cost.

The communication between Operation Network and Consumer Network also requires high security, so as to support strict access controls between these entities. The ease of deployment is also a high-priority concern, due to the huge number of consumers in the system. However, the data from Operation Network to Consumer Network, or vice versa, can also be delivered indirectly through Business Network. It may be necessary to block direct communication between Operation Network and Consumer Network, so as to trade the communication performance with better security.

The communication between Business Network and Consumer Network, on the other hand, requires high data availability and high reliability, but relatively less stringent security. Typically, a mesh wide-area network is most suitable.

IV. Conclusion

There is a need of a communication-oriented framework to support the development of information and communication technology in smart grids. Since there is no such framework available, we have proposed a three-entity framework to address this problem. The three entities in the framework are Operation Network, Business Network, and Consumer Network. Operation Network handles communication activities for the grid operations and coordinations of electricity generation, transmission, and distribution. Business Network is where communication within the electricity market resides. Consumer Network deals with the local communication at the consumer end.

The merits of this three-entity framework, as compared with the smart grid framework proposed by NIST, are as follows. First, it is very simple and communication-oriented since all components which have similar communication requirements are grouped into a single entity in our framework. Second, it provides a high-level flexibility for implementation as all functions in the network are represented by the service blocks. Third, it gives readers a better idea about what collaborations are needed to build a smart grid. Besides such merits, our framework is compatible with the NIST framework, which further makes our design the best choice for researchers as a platform for the development in smart grid communication.

Based on this proposed three-entity framework, our future work includes evaluating the feasibility of the proposed framework by simulating a smart grid communication network, developing an efficient protocol translator to be used in Operation Network for smart grid, and optimizing network configurations for communication within each entity as well as communication among different entities.

References

[1] A. Aggarwal, S. Kunta, and P. K. Verma. A Proposed Communication Infrastructure for the Smart Grid. *Proceedings of IEEE ISGT 2010*, 19-21 January 2010.

[2] A. Brooks, E. Lu, D. Reicher, C. Spirakis, and B. Weihl. Demand Dispatch. *IEEE Power and Energy Magazine*, Vol. 8, No. 3, pp. 20-29, May/June 2010.

[3] K. C. Chen, P. C. Yeh, H. Y. Hsieh, and S. C. Chang. Communication Infrastructure of Smart Grid. *Proceedings of IEEE ISCCSP 2010*, 3-5 March 2010.

[4] H. Gjermundrd, 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, pp. 136-143, January 2009.

[5] 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 and Energy Magazine*, Vol. 3, No. 2, pp. 47-55, March/April 2005.

[6] Institute of Electrical and Electronic Engineering Inc. IEEE Std 1815-2010, IEEE Standards for Electric Power Systems Communications - Distributed Network Protocol (DNP3), 1 July 2010.

[7] Institute of Electrical and Electronic Engineering Inc. IEEE Std 802.14.4-2006, IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANS). New York: IEEE Press, October 2003.

[8] A. Ipakchi and F. Albuyeh. Grid of the Future. *IEEE Power and Energy Magazine*, Vol. 7, No. 2, pp. 52-62, March/April 2009.

[9] T. Jin and M. Mechehoul. Ordering Electricity via Internet and its Potentials for Smart Grid Systems. *IEEE Transactions on Smart Grid*, Vol. 1, No. 3, pp. 302-310, December 2010.

[10] 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.

[11] S. M. Massoud and B. F. WollenBerg. Toward a Smart Grid: Power Delivery for the 21st Century. *IEEE Power and Energy Magazine*, Vol. 3, No. 5, pp. 34-41, September/October 2005.

[12] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.

[13] F. Rahimi and A. Ipakchi. Demand Response as a Market Resource Under the Smart Grid Paradigm. *IEEE Transactions on Smart Grid*, Vol. 1, No. 1, pp. 82-88, June 2010.

[14] T. Sauter and M. Lobashov. End-to-End Communication Architecture for Smart Grids. *IEEE Transactions on Industrial Electronics*, Vol. 58, No. 4, pp. 1218-1228, April 2011.

[15] V. K. Sood, D. Fischer, J. M. Eklund, and T. Brown. Developing a Communication Infrastructure for the Smart Grid. *Proceedings of IEEE EPEC 2009*, 22-23 October 2009.

[16] The Smart Grid Interoperability Panel - Cyber Security Working Group. Guidelines for Smart Grid Cyber Security, NIST IR 7628. National Institute of Science and Technology, Interagency Report, August 2010.

[17] A. Treytl, P. Palensky, T. Sauter. Security Considerations for Energy Automation Networks. *Proceedings of IFAC FeT 2005*, pp. 158-165, 14-15 November 2005.

[18] F. F. Wu, K. Moslehi, and A. Bose. Power System Control Centers: Past, Present, and Future. *Proceedings of IEEE*, Vol. 93, No. 11, pp. 1890-1908, November 2005.