QoS Requirements for the Smart Grid Communications System

Yong-Hee Jeon

Catholic University of Daegu, Gyeongsan, Rep. Of Korea

Summary
A communications infrastructure is necessary in order to integrate numerous devices on the smart grid. Among the key technology areas, the implementation of integrated communications infrastructure needs to be performed with the highest priority to build the smart grid efficiently. To encounter possible disruptions of the grid system, a highly reliable, scalable, secure, robust and cost-effective communications infrastructure which supports QoS (Quality of Service) requirements is absolutely needed. In order to answer the question "What is the QoS requirements in the context of smart grid?", this paper presents a survey result on the QoS requirements of the smart grid communications system .This paper examines the challenges that arise in defining QoS requirements in the smart grid communications system and explores potential solutions for implementing them.

Key words:
Smart grid communications, AMI, QoS requirements, utility communications, power grid

1. Introduction

A smart grid communications infrastructure is needed to integrate numerous devices on the power grid, customer devices such as AMI (Advanced Metering Infrastructure), and distributed power generation and storage facilities [1]. To meet technical requirements for power that is reliable, secure, efficient, economic, and environmentally responsible and to achieve the modern grid, five key technology areas are specified as follows by NETL [2]:

- Integrated communications
- Sensing and measurement
- Advanced components
- Advanced control methods
- Improved interfaces and decision support

In the executive summary of appendix on Integrated communications, NETL provides the following statements: "Of these five key technologies, the implementation of integrated communications is a foundational need, required by the other key technologies and essential to the modern grid. Due to its dependency on data acquisition, protection, and control, the modern grid cannot exist without an effective integrated communications infrastructure. Establishing these communications must be of highest priority since it is the first step in building the modern grid."

The smart grid will ultimately require hundreds of standards, specifications, and requirements. Some are needed more urgently than others. To prioritize its work, NIST chose to focus on eight key functionalities, aspects that are especially critical to ongoing and near-term deployments of smart grid technologies and services. The eight priority areas are as follows [3]:

- Demand response and consumer energy efficiency: Demand response is necessary for optimizing the balance of power supply and demand. The purpose of energy efficiency is to cut energy usage during times of peak demand or when power reliability is at risk.
- Wide-area situational awareness: The goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise.
- Energy storage: The smart grid will need new storage capabilities for distributed storage from generation to end use.
- Electric transportation: This refers primarily to enabling large-scale integration of plug-in electric vehicles (PEVs).
- Advanced metering infrastructure: AMI provides customers real-time (or near real-time) pricing of electricity, and it can help utilities achieve necessary load reductions.
- Distribution grid management: To increase reliability, to reduce peak loads, and to improve capabilities for managing distributed sources of renewable energy, it focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and

Manuscript received March 5, 2011
Manuscript revised March 20, 2011

integrating with transmission systems and customer operations.
- Cyber security: For the management, operation, and protection of the smart grid's energy, information technology, and telecommunications infrastructures, this encompasses measures to ensure the confidentiality, integrity and availability of the electronic information communication systems and the control systems.
- Network communications: In the variety of networking environments of the smart grid system, the identification of performance metrics and core operational requirements of different applications, actors, and domains is critical to the smart grid.

The smart grid communications system requires a high-performance data delivery that enables reliable remote control systems, which have the capability of monitoring the real-time operating conditions and performance of electric systems [4].
However, the communication systems used in the power industry today are too slow and too localized to support the integrated communications necessary for the modern power grid [2]. Thus an open communications architecture that fully support the interoperability based on universally accepted standards is needed. In [2], the present state of communications in the U.S. is specified from the aspects of communication standards, and communication media and technologies.
From the points of communications standards, it describes as follows [2]:

- For communications in the grid to be truly effective, they must exist in a fully integrated system.
- Standards for advanced meter reading (AMR), demand response (DR), and other modern grid features should be adopted.
- Universally adopted standards do not yet exist for most user-side features such as AMR and DR.

It states that although numerous communication standards already exist today, the establishment and adoption of universal standards by users, vendors, and operators is lacking but greatly needed. Therefore, standards development such as IEC 61850 for substation automation (SA) should be performed to attain a modern grid.
It also indicates that SA needs to be fully integrated with other features of a variety of communication media including copper wiring, optical fiber, power line carrier technologies, and wireless technologies, in order to modernize the power grid.
The communication technologies for electric system can be classified into four classes as follows [4]:

- Power Line Communication
- Satellite Communication
- Wireless Communication
- Optical Fiber Communication

To determine the best communication technology appropriate for the smart grid, we have to evaluate its own advantages and disadvantages for the expected situations of the system. A highly reliable, scalable, secure, robust and cost-effective communications infrastructure is very important to encounter possible disruptions of the grid system. Therefore, this paper surveys the QoS (Quality of Service) requirements of the smart grid communications system.
The remainder of this paper consists of as follows. In Section 2, we present a communications architecture of the smart grid system. Section 3 presents the QoS requirements. Then, Section 4 describes the proposed methods to meet the QoS requirements. Finally, we conclude and suggest directions for further research in Section 5.

2. Smart Grid Communications

2.1 NIST conceptual reference model [3]

According to the defined architecture of NIST, a single, all encompassing architecture is not practical. The smart grid is expected to have a composite of many system and subsystem architectures in order to allow maximum flexibility during implementation and to simplify interfacing with other systems. NIST adopted the approach of dividing the smart grid into seven domains, which are customers, markets, service providers, operations, bulk generation, transmission, and distribution.
Each domain and its sub-domains encompass smart grid actors and applications. Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications. Applications, on the other hand, are tasks performed by one or more actors within a domain. Examples of applications and devices in the customer domain include smart meters, energy storage, electric vehicles, and distributed generation. Their examples in the operations domain include SCADA systems.
The information network requirements for the smart grid include:

- network management functionality, network activities, and network devices, including status monitoring, fault detection, isolation, and recovery
- ability to uniquely identify and address elements in the network and devices attached to it

- routing capability to all networks end points
- QoS support for a wide range of applications with different bandwidths and different latency and loss requirements

2.2 Required characteristics

An effective, fully integrated communications infrastructure which support open communication standards and provide appropriate media is an essential component of the smart grid. Open architecture will create a plug-and-play environment that networks the grid components together for talk and interaction. The appropriate media should be deployed to provide the necessary infrastructure to transmit information accurately, securely, reliably, and at the required speed with the required data throughput. The integrated communications infrastructure of the smart grid is expected to have the following characteristics [2]:

- Universality: It is a property that all users can be potential active participants.
- Integrity: The infrastructure should be operated with a high degree of integrity. It is notified only if it ceases to function effectively.
- Ease of use: Appropriate rules and procedures should be set up for the user to utilize the infrastructure without any difficulties.
- Cost effectiveness: The deployment of the smart grid should consider cost effectiveness.
- Standards: The communications architecture should support applicable standards in order to guarantee interoperability between the elements of the infrastructure.
- Openness: The public interfaces of the infrastructure should be available on a required basis.
- Security: The communications infrastructure is critically important to the safe and efficient operation of the smart grid but is vulnerable to security attacks.
- Applicability: The communications infrastructure should have enough bandwidth to support not only current applications but also future applications to be developed.

2.3 End-to-end Communications Architecture and Basic Building Blocks

A smart grid is a form of electricity network using digital communication technology. In order to save energy, reduce costs, and increase reliability and transparency, it delivers electricity from suppliers to consumers using two-way digital communications [5]. The Smart Grid outside the home touches the whole power grid and related infrastructure, from back office (BO) IT systems used for billing and managing the grid to power generation, transmission and distribution, and eventually the connection to the home, as shown in Fig. 1 [6].

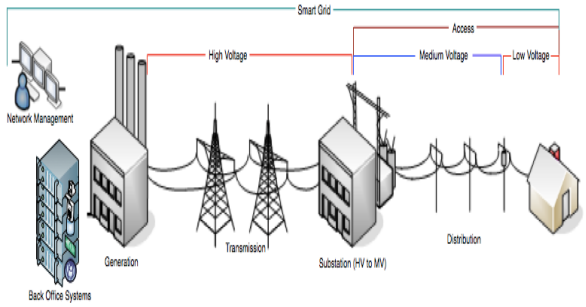

Fig. 1 General model of Smart Grid including Utility Back Office Systems, Power Generation, Transmission, and Distribution [6].

The basic building blocks of the smart grid communications architecture are identified and defined by [7] as shown in Fig. 2.

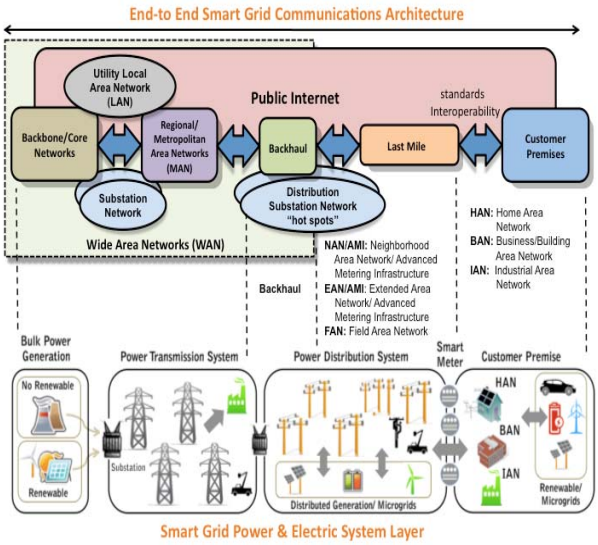

Fig. 2 End-to-end smart grid communications architecture [7]

It defines the smart grid communications architecture framework with its key segments and constituent elements. The figure 2 shows the building blocks of an end-to-end smart grid communications system, including the terminologies used to define the multiple network segments and boundaries for proper interoperability. It also shows SLA (Service Level Agreement) performance metrics compliance at the interface boundaries [7]. It is stated that this segmentation and boundary offers a modular and flexible approach to define interoperable segments, interfaces and elements and ensures that service performance and end-to-end network management is met

all the way across multiple interoperable network segments.
Each element of the smart grid communications architecture is described as follows [7]:

· Wide Area Networks (WAN) – It consist of (i) the core network/backbone, (ii) regional and/or Metropolitan Area Network (MAN).

This part includes a hybrid mix of networks including fiber optics, PLC (Power Line Carrier) systems, copper-wire line, and several wireless technologies. This WAN is needed to support utility applications for the safe and reliable operation of the electric utility infrastructure, which are SCADA/EMS, protective relaying for high voltage lines, generating plant automation, distribution feeder automation and physical security [8].

· Utility Local Area Network (LAN) – To manage operations, control and enterprise processes and services such as billing and automation, meter reading, outage management, demand response, load control, etc, it is comprised of utility operations and enterprise LANs. It interconnects to the WAN through secure wired or wireless communications. It also interconnects to the Internet to exchange customer data to third party providers.

· Backhaul – It is the spur that connects the WAN (major POPs (point-of-presences)) to the last mile network. It aggregates and transport customers' smart grid telemetry data, substations automation critical parameters data, distribution plant intelligent devices data field information, mobile workforce information from/to the utility head end to/from the last mile network.

· Last Mile –The last mile is a two-way wireless or wired communications network overlaid on top of the power distribution system. Depending on the utility network system characteristics, services offered, network topology and demographics and the vendor technology utilized, it is usually named as Neighborhood Area Network (NAN) or Advanced Metering Infrastructure (AMI). The last mile could be an integrated and multi-purpose network technology alternative for AMI (smart meters, Demand Response, etc) services, Distribution Automation (IEDs in the field) and substation automation.

· Customer Premise – It is comprised of the residential or Home Area Network (HAN), Business/building Area Network (BAN), and Industrial Area Network (IAN). These networks are also connected to the ancillary elements outside the customer premises like the Plug-in Vehicle (PEV), solar/wind energy (microgrids) sources and storage devices. It can also be connected to the public Internet network through a "service provider-provided energy management gateways" or Energy Services Interfaces (ESI).

2.4 IP-Based Networks

There is a wide expectation that Internet Protocol (IP)-based networks will serve as a key element for the smart grid networks. IP-based networks enable bandwidth sharing among applications and increased reliability with dynamic routing capabilities [3]. For some applications that have specific QoS requirements, other technologies, such as MPLS (Multi Protocol Label Switching), may be used for the provisioning of dedicated resources.
Figure 3 represents IP communications architecture between the utility enterprise data center (at the head end) and the end Smart Grid devices in ANSI C12.22 standard. This standard provides an application layer standard for network communications, designed to transport data tables in electric metering over any physical medium.

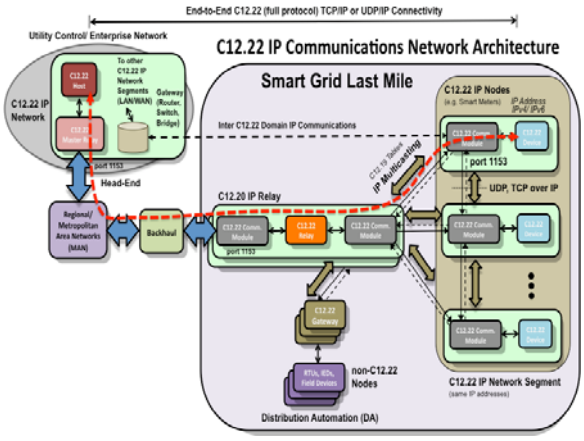

Fig. 3 C12.22 IP Communication Network Architecture

It shows an example of the C12.22 Master Relay connecting to a C12.22 IP Node at the edge of the network. It also shows the multiple network segments (Enterprise Network, MAN/Regional, Backhaul, Last Mile) and C12.22 elements (C12.22 IP Relay) it transverses to connect to the end devices (smart meters and/or DA field devices) and establish the end-to-end IP communications path between them [9].
It points out the QoS provisioning as follows: "Quality of service (QoS) tags can be provided by C12.22, under a configuration parameter, to mark urgent messages, which in turn can be mapped onto IP protocols to enable enhanced levels of message delivery and QoS across an end-to-end Smart Grid IP networking. For instance, the QoS engine could be placed at some point of the last mile network, whenever the Access Points (APs) (C12.22 IP

Relay) require more distributed processing intelligence, to differentiate and prioritize Demand Response (DR) signals from meter reading and other non-critical telemetry applications".

2.5 Communication Requirements

The Smart Grid will generate numerous data points from a variety of system devices and many customers [8]. Those data from meters, appliances, substations, and/or distribution systems need to be integrated and analyzed for the safe and reliable operation of the grid system. Functional information for the operation of the grid system includes load factors, energy usage patterns, equipment condition, and voltage levels.
To determine the architecture of communications infrastructure, the timing and data requirements should be collected first [10]. Five main activities are specified as follows:

- Data gathering: Data collection from many sources on the power grid such as sensors, meters, and voltage detection, in the customer premises such as sensors for high-consuming appliances and from external sources such as weather is necessary. The number of devices, the amount of data and frequency of communications with the devices are also necessary to be determined. Acceptable latency and required bandwidth for every type of data should also be considered.
- Additional data for analysis or forecasting: Some additional data transfer for the analysis of the problem, if occurs, for the operation of grid system should be considered. Different data for forecasting, for engineering or other use may be required.
- Security requirement and security overhead: Smart grid is vulnerable to cyber attacks and security is critically important to the safe and efficient operation of the infrastructure systems. The security system imposes an additional traffic on the network and bandwidth consumption for the security overhead should be considered.
- Monitoring, management, and action: In order for the system operators to initiate appropriate actions, accurate information should be sent on the behavior of the grid. The latency on those actions is influenced by the traffic level on the communications network. Many smart grid applications, including distribution automation, outage alarming and load control signaling, require very low latency, while others, such as metering, are more latency-insensitive.
- The deployment of gird to support bidirectional power flow, looping circuits and transfer of power from substation to substation: This part is noted the most expensive part of the Smart Grid deployment, and will take 20 years or more to complete nationwide. They noted that a communication backbone is the key to achieving the interoperability of smart grid networks.

3. QoS requirements

The communications infrastructure is necessary to make the smart grid observable, controllable, automated, and integrated [11]. Based on their experiences in working with utilities on smart grid designs and implementations, four trends emerging in the way the smart grid will be built, operated, and controlled are specified as follows [11]:

- Shift from centralized to peer-to-peer control: The existing utility communications infrastructure generally has star networks with centralized command and control. As the smart grid communications will be more decentralized with distributed command and control, this will require peer-to-peer communications.
- Shift from centralized generation to distributed energy resources: As the distributed energy resources such as bio-mass generation, solar panels, and wind turbines grow, we need to integrate large numbers of remote devices from those sites.
- Shift from few end points with little intelligence to many end points with large amounts of intelligence: In the smart grid system, new large volumes of data can be generated by new intelligent end point devices, including devices in the customer premises. This presents a trade-off decision problem in terms of bandwidth and latency versus cost between distributed intelligence and telecommunication network in the design of a smart grid.
- Shift from low data volumes, often slow response time requirements to high data volume, low latency requirements: In smart grid communications systems, we must support several different data classes that have different behavioral characteristics. In [11], they categorize data into three classes as follows. The first class of data is operational data. This class of data tends to be constant in volume and timing, and may be the same in terms of bandwidth and latency requirements. The second type of data is non-operational or telemetry-type data. The third type of data is asynchronous event messages generated by smart grid devices in reaction to grid physical events. They note that these messages come in unpredictable bursts and floods that need to be transmitted and processed with very low latency.

According to NASPInet [12], the proposed system architecture shall support a diverse set of QoS classes with wide range of rate, delay, and delay-jitter requirements. NASPInet accommodates five classes of data services for supporting different types of applications as follows:

- Class A: supports the needs of high performance feedback control applications. This class of data should have very low latency and a fast data rate. A high level of data availability is required.
- Class B: supports the needs of feed-forward control applications, such as state estimator enhancement. This class of data is less strict than for Class A data for latency requirement. High availability of the data is also required.
- Class C: supports view-only applications such as visualization by power system operators. This class of data is less stringent than Class B data for the accuracy and latency requirements.
- Class D: supports the needs of post-mortem event analysis and other off-line studies. This service class requires a high degree of data completeness and accuracy. However, it is somewhat delay-tolerant.
- Class E: primarily supports the needs for testing and R&D applications. This class shall be given the lowest priority of all NASPInet data traffic.

The NASPInet architecture is supposed to support a set of predefined QoS, and the application services shall be mapped onto these classes for resource management purposes. The proposed system encompasses a set of algorithms for resource monitoring, QoS mapping, admission control, resource reservation, and resource negotiation. The QoS mapping function shall map application level QoS into system level QoS in terms of bandwidth, delay, jitter, CPU demand, and other such items. The admission control function shall determine if an incoming flow can be admitted into the network without QoS degradation of the already admitted flows.
Table 1 summarizes the attributes for each of the five data service classes identified above.

<Table 1> NASPInet Traffic Attributes [12]

NASPInet Traffic Attribute	Real-time steaming data			Historical data	
	A	B	C	D	E
Low Latency	4	3	2	1	1
Availability	4	2	1	3	1
Accuracy	4	2	1	4	1
Time Alignment	4	4	2	1	1
High message rate	4	2	2	4	1
Path Redundancy	4	4	2	1	1
Key: 4-Critically important, 3-Important, 2-Somewhat important, 1-Not very important					

In the Table 1, five classes of data were grouped into two groups: real-time streaming data and historical data. Real-time streaming data may be real-time control and visualization applications, such as closed-loop voltage control and feed-forward remedial action control. Historical data may be non-real-time applications, such as post-disturbances analysis and off-line studies.
The NASPInet shall implement QoS assurance based on the resource management scheme, including resource condition monitoring, resource usage monitoring, QoS performance monitoring, QoS provisioning, and traffic management. The resource condition monitoring is supposed to detect and report any failure and out-of-service conditions for any of its resources. The resource usage monitoring information shall include but not limited to detailed loading information (instant, peak, and average) of each resource. The NASPInet is supposed to provide a traffic management mechanism for QoS assurance based on the traffic prioritization of different data service classes. Therefore data delivery based on the priority traffic levels should be supported.
Alcatel-Lucent provides the following table listing some of the most important smart grid applications and their qualitative network requirements [13].

<Table 2> Network requirements for smart grid applications [13]

Application	Data Rate/ Volume	Latency Allowance (one-way)	Reliability
Smart metering	Low/ Very Low	High	Medium
Inter-site rapid response	High/ Low	Very low	Very high
SCADA	Medium/ Low	Low	High
Operations data	Medium/ Low	Low	High
Distribution automation	Low/ Low	Low	High
Distributed energy management & control	Medium/ Low	Low	High
Video	High/	Medium	High

surveillance	Medium		
Mobile workforce	Low/ Low	Low	High
Corporate data	Medium/ Low	Medium	Medium
Corporate voice	Low/ Very low	Mow	High

Latency requirements for smart grid and other utility applications are further specified as follows [13]:

- Teleprotection: less than 10 ms
- Synchrophasor applications: about 20 ms
- Most SCADA and VoIP applications: 100 to 200 ms
- Smart metering and others: up to a few seconds

Many smart grid applications, including distribution automation, outage alarming and load control signaling, are described to require very low latency, while others, such as metering, are more latency-tolerant [4]. As noted in the latency requirements above, smart grid networking needs to support end-to-end and device-to-device latencies with units of millisecond and second.

To manage traffic appropriately, networking technology must support message prioritization, allowing critical, latency-intolerant messages primary to other network traffic. Based on examples given in [14], meter-reading acquisition is generally expected only within a time window measured in minutes or hours, while some DA (Distribution Automation) applications require that remote devices talk across the network (without routing through the back office) in less than a second. In the following chapter, we will further examine methodologies presented to meet QoS requirements in the literature.

In [13], Alcatel-Lucent believes that an integrated communications network supporting all applications, with proper implementation of QoS, reliability, security and unified network management tools would be a better, less costly strategy to ensure delivery of critical smart grid application traffic.

4. Methods to meet the QoS requirements

An advanced networking infrastructure is required to efficiently manage the many devices deployed in the smart grid. The right network interconnects smart devices together and allows for real-time command and control of the smart grid.

In [14], the right network infrastructure is stated as one that is functionally capable and cost-effective today, yet will support future requirements. The critical components of the smart grid network are specified as follows:

- Internet protocol (IP)-based networking: Since IP is the networking standard used in managing almost all telecommunications and information technology applications and the IP suite is also proven technologies for addressing, routing, QoS and other related networking functions, a common network infrastructure can be developed with IP to minimize cost and complexity.
- Transport-agnostic network technology: In order to choose the physical transport among a variety of transports, including wired or wireless, the smart grid networks can be deployed by adopting standard, interoperable, IP-based products rather than proprietary, transport-specific ones.
- Multi-application: As new utility and consumer devices are evolved such as remote controllable thermostats, consumer-based energy storage appliances, customer displays, fault indicators, distribution automation applications and others, a smart grid networks should easily incorporate the applications or devices that emerge.
- Standards-based: By choosing a standards-based network with the right performance characteristics, it is expected that new technologies are easily and seamlessly incorporated onto the network.
- Appropriately sized bandwidth: Two critical issues when developing the technical requirements of the smart grid are specified as those of available bandwidth and latency. Although smart grid applications does not generate a large volume of data relative to modern IT systems, a new smart meter, for example, might generate over 10,000 times as much as a manual meter data.
- High security: This means that the move to sophisticated command-and-control applications mandates significantly more proven and robust security across the entire grid.

In [14], they also argue for IP-based networking for implementing the right network for the smart grid. Internet can therefore afford a communications infrastructure for command and control in the smart grid system. However, Internet by itself cannot guarantee QoS requirements for the smart grid because the basic service principle is based on *best-effort service*. Therefore, some QoS capabilities should be added to ensure the prioritization of mission critical or delay sensitive traffic [4]. They state in [4] that wireless communication technologies provide typically lower QoS compared to wired communication networks. Therefore, they say that each level in the communication protocol stack should adapt to wireless link characteristics in an appropriate manner, taking into account the adaptive strategies at the other layers, in order to optimize network communication performance. They also describe the

recent advances in wireless communications which can provide strict QoS requirements of automation applications, including wireless sensor networks, WiMAX and wireless mesh networks.

Conclusively, they propose a hybrid network architecture for electric system automation. The hybrid network architecture consists of various types of networks such as Internet, wireless sensor networks, WiMax and wireless mesh networks. They maintain that electric utilities can fully exploit the advantages of multiple wireless networks with the integration of different networks. Example use of networks are provided as follows: Low power and low range wireless sensor networks can be utilized for urban areas, while WiMax technology can be used for the reliable long distance communication of rural areas.

WiMax supports five levels of QoS to allow different packets to be given different service. Ethernet VLANs, as defined in IEEE 802.1Q, support eight different Class of Service (CoS) markings in the 802.1Q header to carry QoS information [15]. Delay sensitive control traffic should use these mechanisms where appropriate to ensure that it is not delayed by less critical traffic.

In [13], Alcatel-Lucent also believes that the end-to-end network layer technology of choice will be IP. In order to accelerate the deployment of smart grid networks, it is necessary that access to contiguous spectrum allocation should be provided at least 3 to 5 Mbps or greater of wireless throughput per sector.

5. Conclusions

Smart grid is the term generally used to describe the integration of power grid with an information infrastructure in order to provide power to the end-users in a reliable, self-healing, secure, manageable, and efficient manner. Therefore, smart grid is more than just metering. The smart grid is a complex system of systems which include bulk generation, transmission, distribution, markets, operations, service provider, and customer [3]. The smart grid cannot exist without an effective integrated communications infrastructure.

Two critical issues when developing the technical requirements of the smart grid communications infrastructure are QoS and security. In order to avoid possible disruptions in the smart grid system, a high-performance communications infrastructure which supports QoS requirements is absolutely needed.

An IP-based network is considered as a key element to implement open communication architecture of the smart grid. However, IP itself cannot guarantee QoS requirements.

Therefore, this paper addressed QoS requirements for the smart grid communications system.

References

[1] Trilliant White Paper, Wireless WAN for the Smart Grid command and control grid applications that require real-time or near-real-time response, HTTP retrieved on March 2011.

[2] NETL (National Energy Technology Laboratory), Appendix B1: A Systems View of the Modern Grid: Integrated Communications, Feb. 2007.

[3] NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, U.S. Department of Commerce, Jan. 2010.

[4] V. Cagri Gungor and Frank C. Lambert, "A Survey on Communication Networks for Electric System Automation", Computer Networks 50 (2006) 877–897, Elsevier.

[5] Wikipedia, Smart Grid, http://en.wikipedia.org/wiki/Smart_grid.

[6] ITU-T Technical Paper, Series G: Transmission Systems and Media, Digital Systems and Networks, Applications of ITU-T G.9960, ITU-T G.9961 transceivers for Smart Grid Applications: Advanced metering infrastructure, energy management in the home and electric vehicles, June 2010.

[7] NIST PAP 01, The Role of IP in AMI Networks for Smart Grid, 2009, Oct. 24.

[8] James G. Cupp and Mike E. Beehler, Implementing Smart Grid Communications, Burns & McDonnell, TechBriefs, pp. 5-8, 2008, No.4.

[9] ANSI C12.22-2008, American National Standard Protocol Specification For Interfacing to Data Communication Networks, Nov. 2008.

[10] Meir Shargal and Doug Houseman Capgemini, Why Your Smart Grid Must Start with Communications, Feb. 14 2009.

[11] Jeffrey Taft and Shahid Ahmed, Networks for High Performance: The Journey to Smart Grid Communications Infrastructure, http://ww.energypulse.net/centers/article/artice_display.cfm?a_id-2156

[12] NASPInet Technical Specifications, 5/29/2009.

[13] Technology White Paper, Alcatel/Lucent, Smart Choices for the Smart Grid. Retrieved from the web. Feb. 2011.

[14] Raj Vaswani and Eric Dresselhuys, Implementing the Right Network for the Smart Grid: Critical Infrastructure Determines Long-Term Strategy, Chapter 1. Technology, White paper, www.UtilitiesProject.com

[15] Andrew K. Wright, Paul Kalv, and Rodrick Sibery, "Interoperability and Security for Converged Smart Grid Networks", Grid-Interop Forum, 2010.

Yong-Hee Jeon received the B.S degree in Electrical Engineering from Korea University in 1978 and the M.S and Ph. D degrees in Computer Engineering from North Carolina State University at Raleigh, NC, USA, in 1989 and 1992, respectively. From 1978 to 1985, he worked at Samsung and KOPEC (Korea Power Engineering Co.). Before joining the faculty at CUD (Catholic University of Daegu) in 1994, he worked at ETRI (Electronics and Telecommunications Research Institute) from 1992 to 1994. Currently, he is a Professor at the School of Computer and Information Communications Engineering in the CUD, Gyeongsan, Korea. Since January 2008, he has been a Vice-President of KIISC (Korea Institute of Information Security and Cryptology).