Michael T. McMenamin
Global Govt & Public Affairs

1100 New York Avenue, NW
Suite 640 West
Washington, DC 20005
Phone +1 202 312 5916
Fax +1 202 312 5904
mcmenamin@alcatel- lucent.com

12 July 2010

VIA ELECTRONIC FILING

U.S. Department of Energy
Office of the General Counsel
1000 Independence Avenue, SW
Room 6A245
Washington, DC 20585

Re: *Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid Policy*

Alcatel-Lucent ("ALU") appreciates the opportunity to contribute to the Department of Energy's ("Department") Request for Information ("RFI")[1] to better understand the communications requirements of utilities, including the requirements of Smart Grid Technology. ALU sees smart grid as one of several solutions offered by the technological advances and widespread deployment of broadband networks. While in its comments ALU addresses the narrow issues raised specifically in the Department's RFI, these comments also convey broader policy recommendations for the Federal Government, including the Federal Communications Commission ("Commission"), to consider.

ALU has been a provider of telecommunications solutions to the US electric utility industry for decades. As an example of the range of utilities and communications solutions that we work with, ALU has provided strategic guidance and infrastructure management on Smart Grid Telecommunications to Oncor Electric Delivery ("Oncor"), a large, Investor-Owned Transmission and Distribution System Operator based in Dallas, Texas serving 3,200,000 customers over a 73,000 square mile area of northern Texas. In addition, ALU has worked with Bristol Tennessee Essential Services ("BTES"), a utility with more than 33,000 electric meters across 280 square mile area, to expand its communications capabilities over a fiber network that is used by 99 percent of its customers. Using ALU's Passive Optical Network System to achieve wide-area communications and distributed computing, BTES has made improvements in real-time energy data collection, transfer and management for current and future smart grid applications. BTES has also upgraded its efficiency by adding demand response and distribution automation, enabling it to reduce the number of customer minutes in power outages. Advanced communications capabilities have also enabled BTES to use real-time communications to improve its pricing schedules through Time-of-Use, Real-Time Pricing and Critical Peak Pricing, and to increase its responsiveness to customer service issues and better educate its consumers.

[1] *Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid Policy*, Fed Reg Vol. 75, No. 90 at 26206 (May 11, 2010).

The Oncor and BTES experiences demonstrate that as broadband capabilities are expanded and they become more widely available to electric utilities in the United States, we will come closer to achieving the important national goal of achieving energy independence. The Commission's plan for broadband should promote its role in improving energy efficiency and achieving energy independence.

ALU's View of Smart Grid

First, smart grid is not an individual application or solution, rather a collection of distinct applications that have varying degrees of latency sensitivity, market availability, interference issues, and power requirements. As a primary supplier of telecommunications solutions to the utility industry, ALU recognizes that while many utilities may prefer exclusive networks for smart grid applications, cost considerations will result in utilities using shared and/or commercial networks for many of these applications. In a shared environment, the service provider must be able to provide the resiliency and redundancy that these applications require in order to achieve the energy independence and efficiencies offered by a smart grid solution.

Second, smart grid is platform-agnostic and a wide variety of broadband platforms will be employed (e.g. wireless, wireline, etc.), but the Internet Protocol should be the end-to-end network layer. IP will enable the multiple smart grid applications to work in the collaborative and unified manner necessary for utilities to realize the potential efficiencies and control offered by smart grid.

Finally, many smart grid deployments could be better served using broadband wireless solutions, but the Department must consider whether sufficient spectrum is available to achieve these solutions as well as the broader goals of the national broadband policy. While unlicensed spectrum addresses certain parts of the smart grid solution, such as smart metering, and network technology can address reliability and interference concerns on a shared network, there is no substitute for more commercially-available licensed spectrum for all broadband solutions, including smart grid.

(1) What are the current and future communications needs of utilities, including for the deployment of new Smart Grid applications, and how are these needs being met?

It is ALU's experience that most utilities prefer exclusive ownership of their networks that would be void of interference issues caused by outside users. We believe that ownership by multiple parties of the segments of an integrated network complicates network architecture in physical and logical connectivity, routing, reliability, and security among other factors. Owning a dedicated utility network, however, may not always be possible because of the cost, availability of network assets including spectrum, and/or the need for deploying applications in an expedient manner. Moreover, owning a dedicated network would likely result in longer technology refresh cycles and issues surrounding management of the network versus sharing ownership of network segments with a service provider that will update and run the network, which could be viewed either positively or negatively, depending on the utility. Ultimately, the choice will be based on each utility's application and network requirements and those associated costs.

We believe that confusion exists today as to what Smart Grid applications and networks comprise, particularly the communications requirements of these applications. It is technically and woefully inaccurate to use Smart Grid as a generic descriptor for Smart Metering. Smart Metering is one aspect, although it is the largest Smart Grid and best known activity occurring today and directly touches the consumer. However, it is also "low-hanging" fruit in terms of relative simplicity to implement when compared to enabling dynamic power management through multiple utilities. It is also the least critical in terms of its communications requirements. If one meter fails to communicate for a few minutes or days, then its impact is negligible to the over all grid. Conversely, losing connectivity to automated substation elements could cause the grid to shut down thousands of homes in order to protect itself, which represents a much different scenario in regards to reliability requirements. As a result, current industry practice separates Smart Grid from Smart Metering when discussing capabilities and requirements. With many people interchanging the terms, it is easy to see how confusion occurs in the marketplace.

Similarly, all "utilities" are not created equally. There is a tendency to put all utilities in the same "utility" bucket, when in fact, not all are Critical Infrastructure providers. For example, a "utility" that is a market retailer has no power grid infrastructure to manage. They buy power from a wholesaler (also a utility) who likewise may not have any grid infrastructure to manage. These "utilities" clearly do not need dedicated networks to run their operations and can operate extremely well on consumer-oriented networks. Likewise, there are independent utilities that exist for the sole purpose of providing themselves with electric power. These utilities have no need for dedicated spectrum to support their Smart Grid activities. In fact, wireless access networks for Smart Grid operations are primarily needed to support Distribution and Transmission System Operators ("TDSO"). These operators tend to have widely distributed assets that cannot be cost effectively run with private Fiber Optic infrastructures and many cannot be reliably and ubiquitously served by commercial wireless carriers for their most critical grid management functions. It is the TDSO that the remainder of this response will focus on.

All utilities can and do use commercial wireless networks today to fulfill some of their less critical communications needs and ALU expects commercial networks to continue to provide and expand their services to the utilities. It is, however, ALU's experience that most TDSOs prefer exclusive ownership of "*mission critical networks"* that would be void of interference issues caused by outside users in order to insure they meet stringent safety and grid control requirements. As a matter of practice and regulation, electric TDSOs build and operate networks that will operate regardless of the state of operation of the power grid, much as public safety networks are constructed and for many of the same reasons. As an example, a fundamental concept of Smart Grid is automated control of the operation of the grid at higher capacity levels that require much finer monitoring and control of assets to maintain grid reliability. Evolving devices and sensors on the distribution grid will require continuous uninterruptable communications for these devices to function correctly. If interrupted, these devices will cause portions of the grid to shutdown in order to protect it.

As a matter of common business practice, current commercial wireless networks are built to "best effort" standards regarding availability and are sometimes not available when and where the utility needs them most during extended power outages. Nor do commercial networks provide service to all parts of a utility service territory. Focused on consumer services, they are designed to cover a vast number of consumer users under normal operating circumstances, conversely not for territorial footprint under the worst operating circumstances that a TDSO must provide service for. Simply put, today if a commercial wireless provider must wait until the utility has restored its power in order to restore service to the utility to reconnect the automated controls that operate its grid, then that is an irresolvable paradox and no one will be adequately served by the co-dependent relationship. In fact, a large and protracted electrical outage event is by definition a public safety emergency, and the communications needed to support this event must meet significantly the same hardening standards to continue operations that are required of public safety agencies. We believe that hardening commercial wireless networks for continuous off-grid power and antenna wind loading to meet utility availability requirements for core Smart Grid functions and extending coverage to all parts of a utility service territory would represent an enormously expensive undertaking for a commercial service provider that simply cannot be realistically funded as part of a consumer-focused commercial service business case.

That said, we believe that many smart grid applications being deployed today can adequately operate on current commercial communications networks, and it is our position that utilities and others will often look to commercial services for low-risk, high device capacity applications such as Smart Meters and Plug-in Hybrid Electric Vehicles. However, most utilities seek exclusive access arrangements for their mission-critical applications out of concern for quality of service and prioritization needs, and for Critical Infrastructure Protection (CIP) audit requirements that are a challenge in a shared network environment. Commercial providers will need to support utility mission critical applications and their performance, reliability, security, and auditing requirements in a shared environment of commercial networks. Priority access and priority flow management could also be an issue for critical smart grid applications, with pre-emption ability favoring the power utility applications..

Further, while Investor-Owned Utilities may face regulatory hurdles in providing services other than power delivery, we believe that the many local government and cooperative utility owners in under-served/unserved market areas could and wish to serve as a conduit or as a provider of broadband services for their under-served citizens. In that case, dedicated utility spectrum could be used to extend broadband coverage into areas that cannot be economically served by commercial carriers. However, the business case and regulatory environment for the public/private partnerships to support such activities will need to be evaluated on a case by case basis by the grid operators.

(2) What are the basic requirements, such as security, bandwidth, reliability, coverage, latency, and backup, for smart grid communications and electric utility communications systems in general—today and tomorrow? How do these requirements impact the utilities' communication needs?

One of the maxims in enterprise and commercial telecommunications is that applications always grow to fill the available network bandwidth. Smart Grid is in its infancy and much like the early Internet it is difficult to draw a direct correlation between what the bandwidth requirements of today are and what will be needed in the near future. With the first smart grid applications being rolled out today primarily around smart metering using non-real-time access to meters (measured in reads per day), it is fair to say that today's bandwidth requirements are quite low. Nonetheless, ALU believes that as more instrumentation evolves into the distribution grid and more emphasis is placed on cyber security and physical substation security, the bandwidth requirements of a smart grid control network will increase dramatically – much as the Internet has done.

As utility investments in telecommunications technologies necessarily must be for the long-term and in order for the Department to understand that future, ALU's Bell Laboratories has produced a Rough Order of Magnitude prediction of what we believe a utility can reasonably expect to see developed in regards to mission-critical wireless bandwidth requirements over the next five (5) to ten (10) years.

These bandwidth computations are at a "rough order of magnitude" level and have been developed using relatively simple models in conjunction with our experience in the market and information derived from the product plans of our application partners in the sector. Applications include new smart grid applications, legacy utility application, mobile workforce applications, and utility enterprise applications. Reasonable assumptions are made on the possibility of new smart grid applications being deployed by the utility in the near future as well as expansion of the application endpoints to much wider set of utility locations. The basic unit of computation is the bandwidth requirements for a base station. Bandwidth estimates are presented for several coverage areas and population densities covered by a base station.

Reference Architecture

Figure 1 illustrates smart grid architecture of systems and applications that can possibly send or receive data through a base station over the wireless access network.

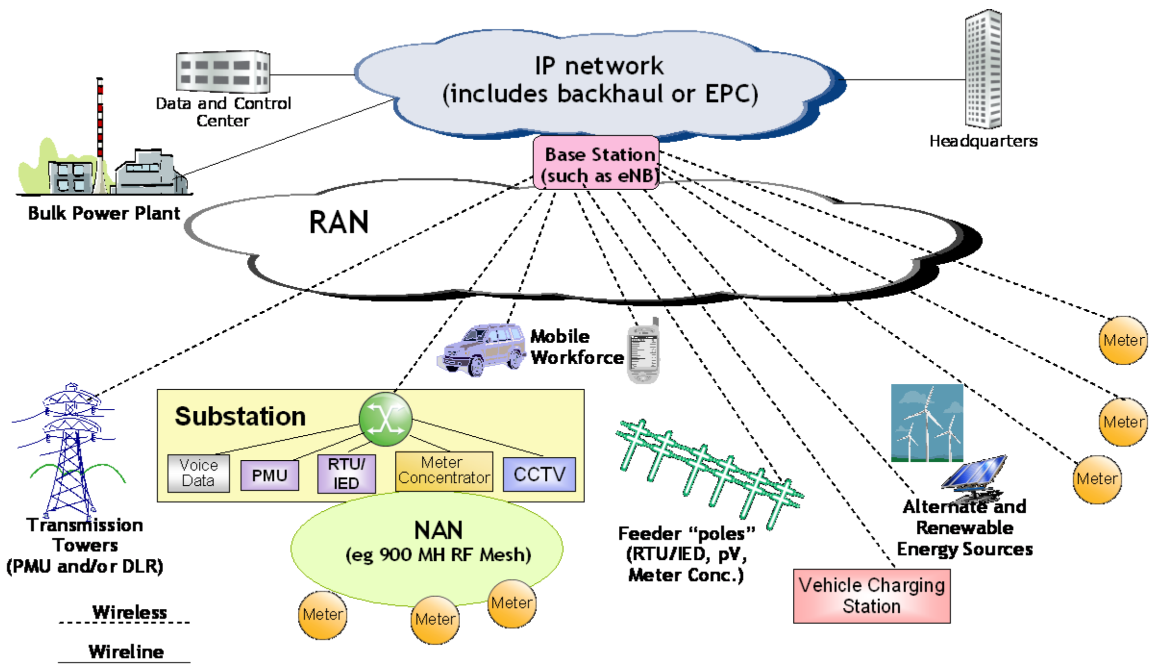

Figure 1: *Reference Architecture*

No specific broadband wireless technology is assumed in the reference architecture as well as in bandwidth computation. The only assumption is that the utility endpoints connect to a base station over radio access network (RAN). The base station connects to an IP network either directly or the base station traffic is backhauled to the core network.

For the purpose of computing the maximum bandwidth requirements, all traffic that *may* be carried over the radio access network is included in computation. Thus, traffic for all endpoints and application that are shown (in Figure 1) to connect to the base station is included in bandwidth computation, even though in many cases, some of the endpoints may not exist in a base station's coverage area or connect to the IP network over wireline connections. However, we assume that large locations such as bulk power stations, utility data and control centers, and utility enterprise offices do connect over wireline connection to the IP network.

The reference architecture is an IP data and voice (VoIP) network. For most smart grid applications, the uplink traffic bandwidth requirements are greater than the downlink traffic requirements and wireless technologies are typically "uplink limited." For peer-to-peer applications such as voice communication, the traffic requirements in each direction are the equal. Therefore, we have assumed that the total downlink bandwidth requirement is not greater than the total downlink bandwidth requirement and only the uplink traffic for each application is used for bandwidth computation.

Traffic Assumptions Based on Figure 1

Traffic is computed for each endpoint of an application, even if traffic is from multiple applications, for some the endpoint may be aggregated at a substation (router). Based on our experience in the market, we have estimated the number of endpoints for each application supported by a base station. Similarly, the number of transmission towers, substations, and so forth are also assumed based on the population area. Moreover, "critical traffic" refers to the traffic that must be carried either because it essential for operations and/or required because of emergency conditions (incident).

(Traditional) Supervisory Control And Data Acquisition (SCADA):

SCADA measurements at each Remote Terminal Unit (RTU) and Intelligent Electronic Device (IED) are included, irrespective of whether the IED measurements are aggregated at an RTU. It is expected in the near future that RTUs/IEDs will be deployed at many feeder locations in addition to their traditional deployment at substations.

Most of the bandwidth requirement is necessitated by periodic SCADA measurements. Bandwidth is computed using DNP packet specifications. An overhead is added to allow for other SCADA traffic.

Critical Traffic: Traffic for only the periodic measurements is considered critical.

Synchrophasors:

Synchrophasors are Phasor Measurement Units (PMUs) that provide voltage/current phasor measurements with time stamps synchronized to a common clock. In addition to the substations, it is assumed that PMUs *may* be deployed at a few transmission towers in the future.

In addition to the traffic measurements for periodic Class A measurements (60 per second), an overhead is allowed for other PMU traffic including the Class C traffic.

Critical Traffic: Traffic for only the Class A measurements is considered critical.

Closed Circuit Television (CCTV):

CCTV helps in surveillance of the substations for security and could be used in the future for field repair and/or outage prevention. There may be more than one CCTV camera at a substation. During normal operation, it is assumed that video feeds from all cameras are transmitted at a speed required for low resolution.

Critical Traffic: During an incident (at a substation), it is assumed that the video feed for one of the cameras is transmitted at higher speed for better resolution whereas all other cameras transmit at the lower normal speed. Further, it is assumed that only one substation in the base station coverage area is involved in that incident.

Mobile Workforce:

During normal operation, it is assumed that only one push-to-talk talk group is active in the base station coverage area, and that there is no real-time video capture. It is assumed that all voice and video traffic is IP.

Critical Traffic: During an incident, it is assumed that there are multiple talk groups active in the coverage area and that there is one real-time video capture stream (in uplink direction) at data rate required for high resolution.

Automated Metering Infrastructure (AMI):

Two classes of smart metering technologies are considered.

1. Meter concentrator located at a substation collects traffic from a very large number of meters (up to a few thousand) that communicate with the concentrator over a Neighborhood Area Network (NAN) communication technology such as the 900 MHz (unlicensed spectrum). Note that this NAN is separate from the wireless broadband network under consideration. The concentrator traffic is then transmitted to the base station. In this case, the bandwidth requirement for AMI is assumed to be the same as the total of bandwidth capacity of the NAN radios used in the meter concentrator.

   Critical Traffic: Critical traffic requirement is assumed to be the same as that for the normal traffic

2. There is either no meter concentrator and the meters directly send traffic to the base station or the meter concentration is very low (collecting traffic from only a handful number of meters) and the large number of concentrators sends traffic to the base stations. For normal operation, in addition to the periodic meter measurement traffic, an overhead is added to the AMI traffic.

   Critical Traffic: After an outage, it is assumed that the traffic requirement for each meter affected by outage is equal to a large multiple of the normal measurement traffic (accounting for meter registration traffic). It is assumed that only a fraction of the meters in the coverage area are affected by outage

New Smart Grid Elements:

These include (possibly future) alternate and renewable sources of energy resources, storage elements, and electric vehicle charging stations that are in direct control of the utility. With little available information on their communication needs, it is assumed that each such new smart grid element has a number of measurement units sending measurements to the control center - similar to SCADA IEDs. Further it is assumed that the normal and critical traffic assumptions are the same as SCADA traffic assumptions.

Dynamic Line Rating (DLR):

The utilities may deploy DLR measurement units at a few of the transmission towers. Once again, with little available information, it is assumed that the normal and critical traffic assumptions for each DLR measurement unit are the same as SCADA traffic assumptions.

Enterprise Voice:

This refers to the VoIP requirements for substation personnel and mobile workforce excluding their push-to-talk traffic. The VoIP traffic is computed from average normal operations voice demand (in Erlang) with a typical wireless codec date rate.

Critical traffic: The average voice demand is assumed to be greater during incident than during the normal operations. Also note that the number of persons during an incident is more due to the increase in the mobile workforce in the coverage area as was observed earlier.

Enterprise Data:

This refers to the enterprise data traffic requirements for substation personnel and mobile workforce. The data traffic is computed using normal enterprise data requirement per enterprise user.

Critical traffic: Per user demand is assumed to be the same as that during normal operation. But note that the number of persons during an incident is more due to the increase in the mobile workforce in the coverage area as was observed earlier.

Bandwidth Requirements

As was noted earlier, the bandwidth requirements are computed on a “rough order of magnitude” basis. Further, reasonable worst cases are assumed; in particular, the total bandwidth is assumed to be the sum of the worst case computed bandwidth for each of the applications.

The estimated bandwidth requirements for four representative scenarios are presented in Table 1 below.

Table 1 - Smart Grid Bandwidth Requirements

Traffic Req. in kbps		Scenario 1 Dense Urban area **with** meter concentrators	Scenario 2 Dense Urban area **without** meter concentrators	Scenario 3 Urban area **with** meter concentrators	Scenario 4 Subarban area **with** meter concentrators
Total	**Normal**	**1,643**	**1,715**	**1,496**	**1,618**
	Critical	**3,435**	**3,421**	**3,108**	**2,930**
Total Data	**Normal**	688	760	542	680
	Critical	1,050	1,036	819	786
Total Video	**Normal**	826	826	826	826
	Critical	1,789	1,789	1,789	1,789
Total VoIP	**Normal**	129	129	129	113
	Critical	597	597	500	355
Traditional SCADA	Normal	165	165	95	140
	Critical	138	138	79	116
Synchr-ophasors	Normal	213	213	213	320
	Critical	178	178	178	266
CCTV	Normal	826	826	826	826
	Critical	1,238	1,238	1,238	1,238
Mobile WF (PTT - VoIP)	Normal	16	16	16	16
	Critical	161	161	129	81
Mobile WF (video)	Normal	0	0	0	0
	Critical	550	550	550	550
AMI	Normal	154	225	77	77
	Critical	154	140	77	77
New Smart Grid Elements	Normal	32	32	32	48
	Critical	27	27	27	40
Enterprise VoIP	Normal	113	113	113	97
	Critical	435	435	371	274
Enterprise Data	Normal	124	124	124	96
	Critical	554	554	459	287
Dynamic Line Rating	Normal	0	0	0	3
	Critical	0	0	0	3
Base Station Coverage (sq. km)		1.85	1.85	2.15	11.70
Population density (per sq. km)		30,000	30,000	15,000	2,000

Key Bandwidth Observations:

1. We believe that the bandwidth requirements for a base station are less than 5 Mbps for supporting smart grid application endpoints in its coverage area. In fact it is much less than 5 Mbps in most cases.
2. The CCTV surveillance traffic is the major contributor to the bandwidth. On the other hand, the bandwidth requirement is less sensitive to the number of endpoints or the traffic volume assumptions of other smart grid applications in the coverage area.
3. There is little Dynamic Line Rating ("DLR") traffic since we have assumed that either there are no transmission towers in dense urban areas and/or DLR is deployed at only a very small number of towers.

Latency is also a critical issue with smart grid applications. While some application latency tolerances could arguably be measured in days (smart metering) many critical functions have much lower latency tolerances. ALU submits the following table listing a few of the most important smart grid applications by category, as well as other utility applications carried over the network and their qualitative requirements.

Figure 2 - Smart Grid Application Latency

Application	Data Rate / Data Volume (at endpoint)	(One way) Latency Allowance	Reliability	Security
Smart Metering	Low/V. Low	High	Medium	High
Inter-site Rapid Response (*e.g.* tele-protection)	High/Low	V. Low	V. High	V. High
SCADA	Medium/Low	Low	High	High
Operations data	Medium/Low	Low	High	High
Distribution Automation	Low/Low	Low	High	High
Distributed Energy Management and Control (inc. ADR, Storage, PEV, PHEV)	Medium/Low	Low	High	High
Video Surveillance	High/Medium	Medium	High	High
Mobile Workforce (Push to X)	Low/Low	Low	High	High
Enterprise (corporate) data	Medium/Low	Medium	Medium	Medium
Enterprise (corporate) Voice	Low/V. Low	Low	High	Medium

ADR: Automated Demand Response

P(H)EV: Plug-in (Hybrid) Electric Vehicle

SCADA: Supervisory Control and Data Acquisition

ALU has also conducted bandwidth requirement studies at the request of various utilities. A summary of one such utility, based on its current rollout of Automated Metering Infrastructure and 5-year plans for other smart grid applications is shown in Figure 2 above and explained further below:

- Today's throughput requirements are quite low
  - AMI traffic measured by vendor at 2GB/month at each collector which translates to ~ 6kb/s at a constant data rate - peak rates are probably higher, but not by much
  - Limited SCADA, but has even lower bandwidth requirements at this time
  - Primary bandwidth user is the IP network's routing protocols
- Near-term throughput requirements are projected to increase with AMI roll-out
  - AMS traffic has been predicted by vendor to be in the order of ~700kb/s at metropolitan substations with multiple collectors - this will be the heaviest user
  - SCADA not a significant contributor at this stage
  - Mobile Data usage is expected to escalate, however, still able to be served by cellular coverage with a peak data rate of 500kb/s and very occasional usage
- Long-term requirements introduce higher throughput requirements
  - Team predicts increasing use of low-rate video surveillance at substations and other critical assets requiring 1mb/s to 2mb/s of peak throughput to be useable
  - Mobile Data usage is expected to escalate significantly to include e-mail, voice, map data, pictures, and other traffic needing 1mb/s peak throughput to be useable.
  - AMI traffic is expected to increase to over 1mb/s per sector near constant throughput in metropolitan service area
- Predicted 10-year horizon requirement is 3mb/s at a near constant bit rate with 5mb/s needed to handle peak traffic conditions

An important consideration when looking at these charts are instances where the application requirements may be different from those in the table, depending on the context. For example, in the case of smart metering application, active demand response and emergency load management will require higher reliability and lower latency as an integrated system than it does as a stand alone application.

Data volume and data rates for most smart grid control applications are not expected to be very high in and of themselves, rather it is the aggregate utilization of the network where the challenges lie. Real time monitoring of wave forms, aggregated demand response and video surveillance and some enterprise data applications will, of course, require higher data rates. Of interest is that for many smart grid applications the downlink traffic is less than the uplink traffic.

Latency requirements for smart grid and other utility applications vary from less than 10 ms for teleprotection, to about 20 ms for some synchrophasors applications, to 100-200 ms for most smart grid control, SCADA and VoIP applications, to up to several seconds for smart metering and some SCADA applications. Unlike most other data networks, support for applications with latencies less than 100 ms is required in the smart grid and can be very challenging. Other than these very low latency applications, we believe that most current wireless services can satisfy the requirements of smart grid applications with latency requirements of 150ms or greater.

(3) What are other additional considerations (*e.g.* terrain, foliage, customer density and size of service territory)?

Question 3 highlights the primary challenges utilities are facing when selecting communications solutions for smart grid deployments, regardless of whether it is a private or commercial solution. There are many combinations of these, and few utilities will share all in common, however, all are limiting factors that tend to favor one approach over another in a given geographic area and often prohibit a single physical layer technology from meeting all of a utility's wireless broadband requirements across its service territory, particularly with larger utilities. This is the primary reason that ALU favors standardization of utility networks at the network (or IP) layer, not at the physical layer.

As an example, mountainous and dense urban terrains can provide a significant challenge for wireless technologies to the point that fiber optic and other wireline solutions may provide a more cost effective alternative. Conversely, dense urban areas also attract commercial carriers and alternative wireline service providers that give the utility more options to select from, mountainous areas tend to be less densely populated, giving the utility few choices for meeting their requirements.

For wireless solutions, as you exceed 2GHz in frequency, the signal begins to fade more quickly; foliage provide reflective surfaces that quickly degrade wireless signals, buildings become impenetrable by the signal, and the cost of the deployment begins to escalate. Conversely, spectrum under 2GHz is difficult to come by and could require the utility to share network assets or enter into expensive spectrum leasing agreements that would significantly impact the operations cost and eventually the cost to the rate payer.

These variations are numerous and are just a few examples of the trade-offs utilities face. Ultimately it boils down to the business case for the utility; the cost of deployment of a given technology in a given geographic and demographic circumstance vs. the capabilities the various options provide. It is ALU's view that this business case decision will vary for each and every utility.

(4) What are the use cases for various smart grid applications and other communications needs?

See *supra* response to Question 2.

(5) What are the technology options for smart grid and other utility communications?

Most utility Transmission System Operators and Distribution System Operators have access to some licensed spectrum, primarily in narrow-band frequencies intended only to support Land Mobile Radio, but these licensed frequency assignments are not adequate for Mobile Workforce, video surveillance, or the future real-time grid control applications. There are currently very few, if any, TDSOs in the United States that currently have sufficient spectrum to support these applications.

Unlicensed spectrum networks continue to be the dominant solution for communications of wireless meter applications in the United States, not the wireless carriers, although this is clearly an application of Smart Grid that the wireless carriers do and should provide services for. These are high device density applications that need little bandwidth and have the capacity to operate well under best effort conditions. Most smart metering solutions use 900 MHz unlicensed spectrum with channels in the 902-928 MHz band with several hundred kilohertz per channel. Zigbee (2.4 GHz) is generally used in home area networks in the United States but has been used for smart metering in other countries. We also believe that the use of WiFi mesh is another possibility, along with WiMax in 3.65 the GHz space that is being deployed today. That said, ALU does not believe than any unlicensed spectrum technology is suitable for mission-critical grid control and monitoring applications, and that licensed spectrum will be required for those applications.

ALU believes that it is not possible to provide a single answer for which communications technology is best suited for smart grid applications because of the diverse applications on the market. In addition, requirements of some of the applications are dynamic and evolving *e.g.* smart metering application. Further, we believe that an application-specific individual network such as Supervisory Control and Data Acquisition ("SCADA")[2] will be far too expensive and unmanageable with many current and new smart grid applications. It is necessary that an integrated network support all applications with proper implementation of quality of service, reliability, and security for individual application traffic carried over the network.

Although there is no single answer to this question, there is a general agreement as to the technology path that the smart grid networks will take. We believe that path leads to Internet Protocol ("IP") as the overall end-to-end network layer technology of choice. The IP suite of technologies offers the needed levels of reliability, redundancy and availability, and can leverage an extensive ecosystem of products and services designed for telecommunications.[3]

IP networks must continue to support legacy systems and networks including proprietary smart metering technologies that have already been deployed. In addition, some applications and some North American Electric Reliability Corporation ("NERC") requirements may not be supported by IP connections or current implementations of the technology for some time, *e.g.* the teleprotection application between substations.[4]

These substation applications such as teleprotection and SCADA may need to be treated differently, as they have special requirements. For instance, if it is not feasible in a particular network to use IP-enabled teleprotection or SCADA, an end-to-end layer 2 network will have to be deployed. Depending on the requirements, it may be possible to tunnel these protocols through IP, using technologies such as Internet Protocol/Multiprotocol Label Switching ("IP/MPLS") Pseudowires.[5] This is a proven technology that is broadly deployed in carrier networks and is undergoing adoption by the utility industry. Low latency requirements of <10ms in Teleprotection may require connectivity over direct physical wired or wireless connection

---

[2] Supervisory Control and Data Acquisition systems are used extensively by power, water, gas and other utility companies to monitor and manage distribution facilities.

[3] It must be noted, however, that IP networks do not necessarily imply the use of the Internet.

[4] Teleprotection refers to detection of the fault at a substation remotely at another substation and then remotely taking action (such as tripping the circuit breaker) at the substation where the fault has occurred. This needs to be done within a few milliseconds.

[5] Pseudowire is point to point layer 1 or layer 2 connection over IP/MPLS. There are many protocol options between the two end points such as TDM (often called VLL-Virtual leased line), Ethernet, Frame relay, and so forth. Pseudowire basically emulates the corresponding protocol over IP/MPLS. (TDM: Time division multiplexing. Example: T1).

between substations. In order to achieve high reliability in Teleprotection it may require two or more such connections between substations.

A. Physical Network

In a typical utility network, the physical network itself will be divided into an access and a core portion. The technology choices for the access portion will require the most tailoring for individual utilities in order to meet their specific requirements. Where a utility is publicly owned, and can offer additional services, such as internet access and Internet Protocol Television ("IPTV"), they may choose to lay fiber, such as Gigabit Passive Optical Network ("GPON") systems. Where a utility is limited from offering additional services, they may choose to either use a customer's existing broadband connection or deploy a broadband wireless access infrastructure. Since it is far from certain that a customer will have or consistently maintain an existing broadband connection, due to coverage and subscription issues, in our observation, utilities prefer to own their broadband wireless access networks.

B. Core Level

The core of the smart grid network will be centered on utility-grade IP/MPLS routers, optical systems and microwave transmission equipment. The core will be fiber where it can and microwave where it does not make economic sense to lay fiber. We believe even higher capacity can be realized using wave division multiplexing ("WDM") technologies and systems.

Devices that are part of the distribution grid can be attached to the larger smart grid network using either an access-style attachment or a core-style attachment. Smaller elements, such as SCADA remote terminal units at the remote transformer will likely be attached over the access infrastructure. Large substations, on the other hand, could be connected via microwave or fiber. The specific choice will depend on the node needing attachment and the specific utilities network.

C. Access Level

ALU believes that both wireless and wireline broadband technologies can be configured to meet most of application requirements at the access level – either from the endpoints or from data concentration points concentrating traffic to/from its endpoints using proprietary technologies. It is not cost effective for most utilities to extend wired technologies to each touch point in their services territory, so wireless technologies will be the dominant solution for access networks. Examples of wireless technologies over licensed spectrum include WiMax, LTE, CDMA 2000 EvDO, and HSPA[6]. Wireline examples would include DSL, DOCSIS, and GPON and PLC ("Power Line Carrier"), including BPL.[7] In the end, we believe that the choice of access technology will mostly depend on the cost effectiveness and ability of the technology to provide suitable coverage at a reasonable cost.

---

[6] WiMax: Worldwide Interoperability for Microwave Access; LTE: Long Term Evolution, CDMA 2000 EvDO: Code Division Multiple Access 2000 Evolution Data Optimized; HSPA: High Speed Packet Access.

[7] DSL: Digital Subscriber Line; DOCSIS: Data over Cable Service Interface Specifications (for cable internet connection); GPON: Gigabit Passive Optical Network); PLC: Power Line Carrier (communication over power lines as the medium carrying digital traffic). BPL: Broadband over Power Line (broadband connection with at least the last mile over PLC).

Moreover, RF mesh over unlicensed spectrum at 900 MHz ISM[8] (wireless) and PLC (wireline) are other options as these technologies are cost effective for carrying low bit rate, low priority smart metering traffic from individual meters to their meter concentrators. Technologies like 900 MHz, however, are cost-effective only in high-density urban and suburban environments where signal coverage can take advantage of shorter hops between meters and/or numerous towers unlike rural areas. PLC becomes attractive in remote rural locations where device capacity is quite low along with the bandwidth required. It is expected that as real-time demand response begins to become a reality these low bite rate, unlicensed network systems will require migration to other technologies that support broadband communications such as WiMax and LTE. Also, as latency sensitive real-time telemetry control applications are deployed across the distribution grid, such as syncrophasor control and other real time sensors, spectrum interference in unlicensed bands or across commercial networks will inhibit the deployment and usefulness of these systems.

D. Network Technologies

There may be a choice of more than one network technology for connecting every smart grid element in the network. In addition, even within a class of network technologies, multiple choices may exist, as there are many wireless and wireline access technologies.

We expect that the utility network will be an integrated IP network that supports data traffic for smart grid applications, as well as traffic for utility enterprise voice and data applications. The network must support connectivity to legacy systems and applications by providing the necessary gateways and protocol conversion. For some time, it may not be possible to carry a few grid applications (such as teleprotection) directly over an IP connection due to their latency requirements and/or due to NERC CIP[9] compliance.

Typical smart grid architecture may include an IP core network in the metro area(s) in utility coverage. The utility data and control center, utility offices, bulk generation sites, substations in the metro areas, and market entities such as independent system operators may connect directly into the core network. The substations in remote areas, (mostly renewable and alternate) generation sites, and electric storage sites will connect to the core over broadband wireless and/or wireline access networks. The choice of access will depend on network availability and their suitability for carrying the application traffic. A substation is a natural data concentration point for communication traffic from consumer buildings (residential, industries, business), other power consumption locations, as well as for the SCADA traffic generated at the electricity distribution points on distribution "feeders" such as at utility poles. Neighborhood area networks such as the 900 MHz RF mesh or PLC are the low cost choices for connections to the substation. Over time it is also possible that the broadband wireless or wireline access networks will be used to connect these buildings and feeder locations to substations or directly to the core network.

---

[8] Mesh connections between meters and their concentrator over unlicensed 900 MHz ISM (Industrial Scientific, and Medicine) band in a neighborhood.

[9] NERC: North American Reliability Council; CIP: Critical Infrastructure Protection.

In addition to a smart meter, a building may have local generation (*e.g.* PV cell, UPS) and storage (*e.g.* PHEV) facilities. They may be connected along with the meter over a local area network ("LAN") or a Home Area Network ("HAN") for building energy management. HAN communication technologies include Zigbee and HomePlug. As buildings also gain smarter grid capabilities, their bandwidth needs will increase. This will put pressure on 900 MHz FR and PLC technologies and accelerate the need for broadband wireless or wireline connections.

The voice and data systems deployed for the utility mobile workforce will connect to the network over wireless access. Gateways will be necessary until broadband VoIP is used for mobile work force voice communication, *e.g.* push to talk.

Finally, enterprise voice and data communication will also be carried over the integrated IP network, including those from the substations.

Like most IP networks, implementing MPLS will also provide added advantages of traffic separation with MPLS virtual private networks ("VPN"), streamlined quality of service and security implementation, and virtual leased lines and virtual private LAN service implementation if necessary.

(6) What are the recommendations for meeting current and future utility requirements, based on each use case, the technology options that are available, and other considerations?

As indicated in our response to Question 2, ALU has concluded that while it is not possible to characterize an application that has not been invented yet, many utilities generally need between 3-5Mb/s of wireless throughput to meet their foreseeable smart grid needs. Of interest is that, unlike consumer applications, for many smart grid applications the downlink traffic is less than the uplink traffic.

While most utilities have access to narrowband spectrum that they use for Land Mobile Radio (LMR), narrowband LMR spectrum will not be sufficient for this level of application data throughput. With a few notable exceptions to include real-time wave-form telemetry, however, data volume and data rates per device for most smart grid control applications are not expected to be very high. Real time monitoring of wave forms, aggregated demand response, video surveillance and grid restoration activities drives the requirement for higher data rates.

Some vendors, while well known and influential but new to the utility marketplace, have erroneously advised the Commission that the utility sector does not require additional spectrum space for Smart Grid deployments. ALU believes this advice was in error, reflecting a lack of understanding of the critical utility operations functions that Smart Grid deployments must accommodate and enable. Furthermore, if followed, we believe that this advice will substantially raise the eventual cost to the consumer, delay Smart Grid deployments in the U.S., put our national electric infrastructure at risk, and will not serve the greater public interest.

We believe that the wide variety of commercial wireless carrier and unlicensed spectrum solutions in the 220MHz and 900MHz band are perfectly suitable for a utility's long-term needs for metering and other non-critical traffic. However, for grid control systems we firmly believe that many utilities will either need dedicated networks using licensed spectrum or will need to partner and share networks and spectrum with entities that have similar operational requirements, such as Public Safety.

ALU believes that there is no need for specific radio technology requirements or the need to rule out a specific band or duplexing scheme for smart grid technology. These are best driven by the market place, although caveats do exist as the current commercial networks using time division duplex ("TDD") are [biased backwards] are not engineered to meet [from the perspective of] utility application requirements. For most utility applications, the downstream traffic is substantially less than the upstream traffic, suggesting TDD ratios should either be even or [biased upstream] engineered to handle more traffic on the uplink. In addition, utilities operating in dense urban environments need building penetration, while utilities operating in rural environments need cost-effective coverage; therefore we believe that lower spectrum bands would be preferred for smart grid technology.

Currently, unlicensed spectrum is the dominant solution for private network communications of wireless meter applications in the United States. Many current smart metering solutions use 900 MHz unlicensed spectrum with channels in the 902-928 MHz band with several hundred kilohertz per channel. Zigbee (2.4 GHz) is generally used in home area networks in the United States but has been used for smart metering in other countries. We also believe that the use of WiFi mesh is another possibility, along with WiMax in 3.65 the GHz space that is being deployed today. That said, all of these unlicensed and/or regulated-unlicensed bands represent sub-optimal solutions for smart grid deployments.

Frequency interference in unlicensed spectrum, however, is a growing problem and 3.65GHz has some limitations that make it difficult to use in utility applications. While most vendors of unlicensed spectrum equipment today provide mechanisms to circumvent interference such as channel hopping or by increasing power, as more systems use these frequencies, the problem is compounded and results in a growing problem with latency that make it unsuitable for a significant number of utility applications. As real-time smart grid applications come online, this latency will pose a significant threat to grid stability and reliability.

Interference problems can be initially managed by RF studies and planning for the deployment in unlicensed bands to help offset problems with interference, however, the unlicensed RF environment is subject to change at any time as other entities add or remove equipment operating in the same band. This can ultimately affect the network performance, particularly so in urban and some suburban environments. As noted above, equipment manufacturers use different techniques to work around interference when it occurs including frequency hopping and increasing power, however, these techniques do provide additional latency that is not acceptable in some Smart Grid applications. It is for these reasons that we do not believe that unlicensed solutions are appropriate for utility control systems.

Due to the ubiquitous nature of the electric grid infrastructure that resides everywhere, the utility needs to procure communications capabilities to cover territory where other communications options may not exist. As such, the utility must currently consider the use of alternative low-bandwidth or high-cost technologies to provide themselves with service. The use of power line carrier ("PLC") and satellite communications must be considered where there are no other network access technologies. Except for short distances such as up to the secondary of the distributing transformer, PLC technology may be expensive and may not afford large data rates. But with emerging Institute of Electrical and Electronics Engineers ("IEEE") P1901 standard and new product development, higher rate PLC solutions with Orthogonal Frequency Division Multiplexing ("OFDM") will be possible. Further, satellite services are frequently used in very remote circumstances and will continue to be part of the utility infrastructure. But as new smart grid applications are deployed and technologies become available, broadband wireless and wireline technologies will provide the most suitable access options.

ALU continues to believe that a contiguous spectrum allocation completed in a timely manner providing at least 3-5 Mb/s of wireless throughput per sector or greater would rapidly speed up deployment of smart grid networks either through a utility dedicated or public/private network. While it matters in terms of cost to the rate payer what band that spectrum is allocated in, our greatest concern is not where the spectrum is allocated, but rather how long it takes to accomplish an allocation. Given the pressures on the utility industry to deploy meters and other smart grid elements, our concern is that the market place will likely commit to deploying suboptimal solutions to get started that will need replacement prior to end-of-life, burdening every citizen in the country with the additional cost of replacement.

(7) To what extent can existing commercial networks satisfy the utilities' communications needs?

Reliability requirements vary by application and will depend on the application, its relative timing in the marketplace, and the specific technology deployed to provide service for the application. Today, applications such as meter reading can reliably run over commercial wireless networks with adequate reliability for individual meter or a small distributed energy resource ("DER")[10]. In the near future, we believe that Electric Vehicles and Plug-in Hybrid Electric Vehicles (EV/PHEV) will be a primary opportunity for utility use of the commercial wireless networks, providing the opportunity for seamless "electrical usage roaming," much as we do now with cellular service roaming. We believe that commercial carrier wireless systems work best at providing what they were designed to do; provide decent coverage and availability to the greatest number of users possible under most conditions. What they do not do well is provide service under Force Majeure and other unanticipated conditions – conditions that utilities must continue to operate in.

While some commercial carriers are beginning to offer Service Level Agreements to utilities and other customers, commercial wireless networks today were built and continue to operate using the "best-effort" standard for consumer applications, so the guarantee is primarily a contractual obligation, as opposed to an operational reality for the utility. For many utility applications, commercial carriers will need to make substantial and expensive changes to their network infrastructure to meet utility requirements for service availability and performance reliability under environmental and security event conditions that they would not expect to provide to consumers. The impact of failure goes far beyond purely financial penalties levied against the service provider to potentially significant disruptions of social and economic activity.

In addition, due to safety concerns and regulatory constraints regarding the ability to manage the grid, a State PUC's electric power regulations in all likelihood will usually require on

[10] Distributed Energy Resource: These are the power generation units at consumer locations. For example, at residences they may be solar (PV-photovoltaic cells); at commercial and industrial locations they may be PV cells, wind turbines, CHP (Combined Heat and Power, UPS (Universal Power Supply)).

average 72 or more hours under “lights out” conditions. This is a regulatory requirement that was implemented to ensure the safety of utility workers and provide for the most expeditious way to restore service. By no means is this an operational “nice to have” requirement and it is expensive to build to this standard. However, in order to support core grid control applications wireless networks will need to be constructed with power systems that meet the applicable State PUC requirements of supporting communications equipment without direct power from the distribution grid, and can withstand hurricane-force winds and continue operation.

ALU believes that commercial cellular network operators are able to meet the security requirements for Smart Grid applications. It is unclear, however, whether NERC CIP accountability standards will evolve to a level that will require the utility to be accountable for end-to-end security of data, regardless of the network owner. We believe the primary issue today regarding use of commercial wireless carrier networks for mission critical smart grid applications is ultimately one of availability and reliability under the worst case conditions that the utility must operate in, not security.

(8) What, if any, improvements to the commercial networks can be made to satisfy the utilities' communications needs?

Many utility control functions operate today on commercial service provider networks. The commercial wireline networks are seldom in doubt as to their ability to meet utility communication requirements. Likewise, we also believe that many smart grid applications being deployed today can and do adequately operate on current commercial wireless communication networks without modification, and that most utilities seek exclusive access arrangements for mission-critical applications out of reasonable concern for quality of service and prioritization requirements that are a challenge in a consumer-focused wireless network environment.

Commercial wireless network providers will need to support utility mission critical applications and their performance, reliability, and security requirements in an environment currently designed for consumer services. Priority access and priority flow management will be an issue for critical smart grid applications, with pre-emption ability at the base station to insure utility service in times of significant consumer-induced congestion – such as a black-out, Force Majeure, or other significant event. Moreover, State PUC's electrical regulations require that acceptable communication network performance, security, and reliability requirements must be met during wide scale power outages and the resulting “black start” processes for restoration and should be considered by potential commercial providers and smart grid policies developed by the Commission.

These requirements represent a massive expense to the commercial wireless carrier. There may also be local regulations, such as the storage of fuel for a back-up generator on the roof of a building where a carrier base station is located, that make it difficult for the carrier to comply with extended off-grid operations requirements. It might be possible for some utilities to partner with a commercial wireless carrier on these expenses and get exceptions to local regulations, but our experience to date suggests that the carrier business case for this level of reliability and availability can not be met using consumer services revenues.

Further, while Investor-Owned Utilities may face regulatory hurdles in providing services other than power delivery, we believe that the many local government and cooperative utility owners may want to serve as a conduit or as a provider of broadband services for their under-served citizens. In that case, there may not be any regulatory conflict in network ownership and certainly opens the door for partnering with commercial carriers to extend their reach into areas they could not previously cost-effectively operate in; however, the business case and /or public/private partnerships to support such activities will need to be evaluated on a case by case basis by the grid operators and the carriers.

(9) As the Smart Grid grows and expands, how do the electric utilities foresee their communications requirements as growing and adapting along with the expansion of Smart Grid applications?

As we noted in our response to Question 2, one of the maxims in enterprise and commercial telecommunications is that applications always grow to fill the available network bandwidth. Smart Grid is in its infancy and much like the early Internet it is difficult to draw a direct correlation between what the bandwidth requirements of today are and what will be needed in the near future. With the first smart grid applications being rolled out today primarily around smart metering using non-real-time access to meters (measured in reads per day), it is fair to say that today's bandwidth requirements are quite low and do not represent what will be needed in the not to distant future. Nonetheless, ALU believes that as more instrumentation evolves into the distribution grid and more emphasis is placed on cyber security and physical substation security, the bandwidth requirements of a smart grid control network will increase dramatically – much as the Internet has done.

Conclusion

ALU's experience in the utility marketplace confirms that utilities need wireless broadband networks that are void of interference and highly available under Force Majeure conditions. Our experience with the commercial wireless carriers likewise confirms that it would be nearly impossible for a consumer-focused wireless carrier to build a profitable business case for building wireless networks to meet all utility wireless broadband requirements. While many smart grid applications being deployed today and in the future can adequately operate on current commercial communication networks, many cannot. Most Transmission and Distribution Operators will continue to seek exclusive access arrangements out of concern that quality of service and prioritization requirements that are a challenge in a consumer-focused wireless network environment. In addition, we believe that the correct technology choice for smart grid networks is IP.

Finally, the need exists for either a dedicated contiguous spectrum allocation completed in a timely manner providing at least 3-5 Mb/s of wireless throughput per sector or greater, or a sharing arrangement with an entity with similar operational requirements such as Public Safety, would rapidly speed up deployment of smart grid networks either through a utility dedicated or public/private network.

Sincerely,

____

Michael McMenamin
Andrew Delaney
Alcatel-Lucent
1100 New York Ave., NW
Suite 640
Washington, DC 20005
(202) 312-5916

Mark Madden
Regional Vice President, Americas Energy
Alcatel-Lucent
401A 18th St.
Brooklyn, NY 11215
(818) 598-6238