Joseph Watson, Jr. Esq.
Director
Federal Government Affairs

Telephone 202.347.7500
Fax 202.347.7501
www.exeloncorp.com

Exelon Corporation
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001

July 12, 2010

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

ATTN: NBP RFI: Communications Requirements:

Re: DOE Request for Information – Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid Policy

Exelon Corporation (Exelon) hereby submits the following comments in response to the Request for Information ("RFI")[1] by the Department of Energy ("Department" or "DOE") regarding the current and future communications requirements of utilities, including, but not limited to, the requirements of the Smart Grid in an effort to implement certain recommendations of the National Broadband Plan. Exelon Corporation is a holding company, located at 10 South Dearborn Street, Chicago, Illinois. Exelon Corporation owns Commonwealth Edison Company (ComEd) and PECO Energy Company (PECO). Together ComEd and PECO own transmission and distribution systems and serve over five million retail electric customers in northern Illinois and the

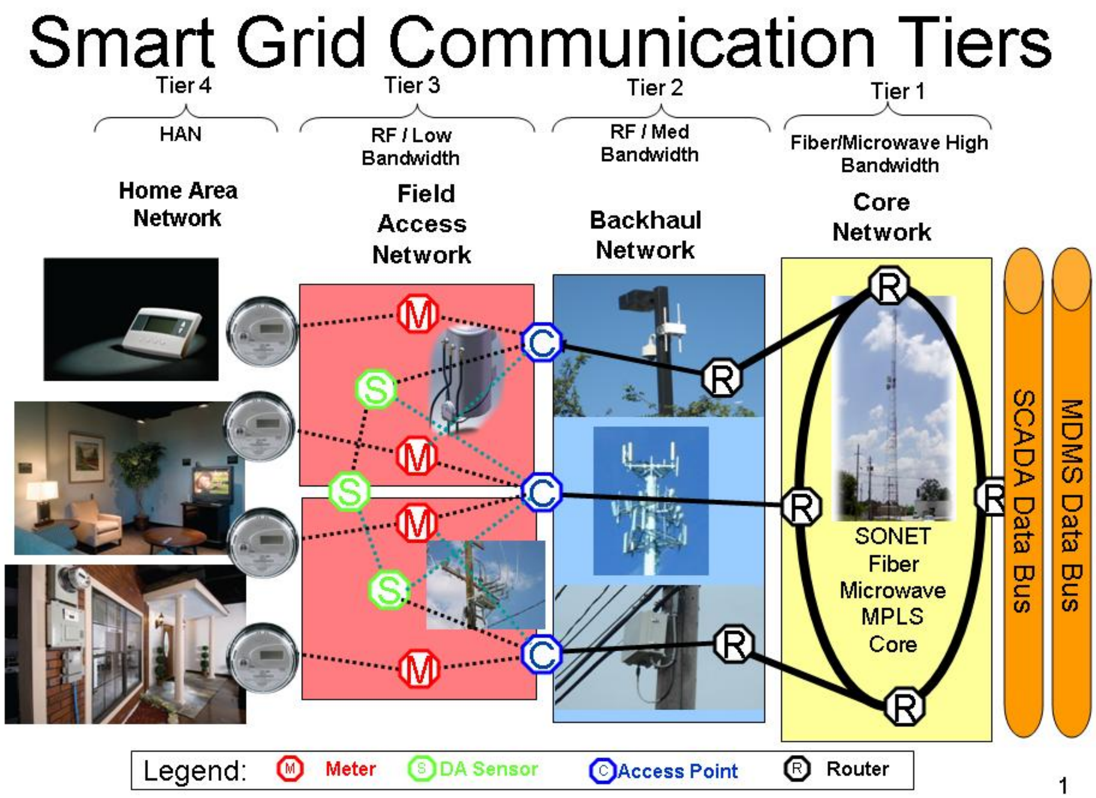
[1] *Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid* Policy, Department of Energy, 75 Fed. Reg. 26206 (May 11, 2010).

Philadelphia area. Exelon Corporation also owns Exelon Generation, LLC (ExGen), which owns or controls approximately 33,000 MW of generating facilities.

COMMENTS

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?

Exelon, including ComEd and PECO over the past two years developed a detailed Smart Grid strategy including identifying the application portfolio to represent the Smart Grid and the associated communication infrastructure required to make it a success. The development of the communications strategy established multiple use cases as described below and the team evaluated multiple communication options and technologies to meet the requirements of the application portfolio. Additionally the strategy embodies a number of fundamental principles enumerated below to ensure the adequacy of the communications solution. The 4 tier model provides the foundation of Smart Grid communications and is architected in such a way to deliver appropriate capacity to the various Smart Grid applications.



The Smart Grid Communications Vision is to provide a secure tiered, robust and deterministic communications architecture with adequate capacity to meet the current and foreseeable future capacity and performance requirements of the Smart Grid Application portfolio.

Fundamental Design Principles

- ✓ **Security**
  - Robust end-to-end, aligned with industry best practices
- ✓ **Converged Communications**
  - Smart Grid applications will share a converged communications infrastructure but will be logically isolated (tunneled).
- ✓ **Interoperable**
  - Industry standard open protocols will be utilized preferentially end-to-end.
  - Avoid use of proprietary protocols
- ✓ **Privately owned communications**
  - Enables Exelon to maintain governance and control over all aspects of the technology.
- ✓ **No Unanalyzed Single Points of Failure** (Self Healing)
  - The communication architecture will be designed with no unanalyzed single points of failure.
  - Consistent with the deterministic philosophy, failure modes and backup schemes shall be incorporated to form a “self healing” architecture.
- ✓ **Maintenance Management & Monitoring**
  - Inherent to the communications Architecture will be Communications Maintenance Management & Monitoring, i.e. the ability to maintain, monitor and control network devices.
- ✓ **Defined Standards**
  - Architectural Design Standards will exist to embody & enumerate the details of the Fundamental Design Principles

Note that the following discussion addresses what Smart Grid technologies are being deployed now and in the near future. This does not imply that current communication technologies in use provide adequate reliability, performance and capacity to accommodate a full Smart Grid integrated deployment.

- ➢ Current Technologies
  - ➢ Communications are needed to support the following existing technology applications: SCADA Telemetry, Power System Protection (Relaying/Tele-protection), Phasor Measurement Units, Smart Meters (AMI), Distribution Automation, , Demand Response (AC cycling (e-mail, voice, paging, work management, distribution operations, customer billing and operations).

    - Outside of the Smart Grid environment, there are other Business use cases to support the need for high reliability communications including Nuclear; specifically the Emergency Response Field Teams need to transmit field survey telemetry across the territory in accordance with emergency response plans up to a 50 mile radius from the nuclear facility.

- Future

    - Mobile dispatch, Radio Communications with Field Personnel, Infrastructure Security Systems (video surveillance, and personnel access)
    - EV charging stations, in-home devices (e.g. smart appliances), web presentment, real-time rates will be added in accordance with strategic and regulatory requirements.

- How are these needs being met?

    - They are being met by a combination of utility owned communications systems and leased communications systems. Many of these systems today are legacy analog technology with limited monitoring capability and a poor operational performance record. Future systems identified in our strategy will be digital IP based, or otherwise standards based, and are built to support scalability and interoperability as the Smart Grid application portfolio grows.
    - The most critical application to Utilities is System (relay) Protection or Tele-protection. System Protection ensures that fault conditions do not impact transformers and otherwise protects those assets from harm. It is this application that in large measure justifies the deployment of a fiber backbone throughout the Utility territory. The reliability of this communication channel needs to be on the order of 99.9999% or higher. System Protection drives the amount of backup required as well, which needs to be on the order of 48 hours or longer.

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?

See chart below.

	Security	Bandwidth	Frequency of occurrence	Reliability	Coverage	Latency	Backup
Power System Protection	High (NERC)	Low	Low	High (no outages during fault events)	Company Wide. All substations	Low (fast – Millisecond)	Dual un-switched Path
SCADA	High (NERC)	Medium	Continuous	High (auto-recovery during fault events)	Company Wide. All substations	Medium (Sub-second)	(typically on same path as protection) Dual switched headend
AMI	Medium (High sec imbedded in native protocol)	Medium	Continuous	Low	Company Wide. All customers.	High and variable can be tolerated	None
DA	High (High sec imbedded in native protocol. Must resist denial of service)	Medium	Continuous	High (independence from AMI "last gasps"	Company Wide. All poles and substations	Medium (Sub-second)	
Land Mobile Radio	Medium	Medium	Continuous	High	Company Wide. Entire area.	High and variable can be tolerated	Coverage Overlap and multiple simultaneous frequencies
Mobile Dispatch	Low (High sec imbedded in native protocol)	Low	Continuous	Medium	Company Wide. Entire area	High and variable can be tolerated	Coverage Overlap and multiple simultaneous frequencies
Security Video	High (High sec imbedded in native protocol. Must resist denial of service)	High	Continuous	High	Company Wide. All substations, offices and storage locations	High. Must support streaming video	Dual switched headend
Security Access Systems	High (High sec imbedded in native protocol. Must resist denial of service)	High	Continuous	High	Company Wide. All substations, offices and storage locations	High and variable can be tolerated.	Dual switched headend
Enterprise	Low (High sec is imbedded in the native protocol)	High	Continuous	Medium	Company Wide	Medium	Dual switched path

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

- Public versus Private

  - It is a challenge for utilities to use public carrier systems in more rural areas because of limited or reduced coverage/availability and throughput requirements, since reliability, bandwidth and latency are the same in all locations for the electric utility
  - Electric utility ownership of communications systems helps ensure higher reliability, since public systems may not be adequately designed, operated and maintained to support the high level of reliability required by electric utilities. They have long term viability and will not be phased out by public carrier.

- Urban area challenges

  - Difficult to operate microwave systems in dense urban areas
  - Higher interference with RF systems
  - In-home devices more challenging to communicate with in high-rise buildings

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

- See response to question 1, for Smart Grid application portfolio and associated matrix in question 2.

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

- There are various technology choices depending on the specific application and there may be multiple communication technologies integrated into a single smart grid solution, i.e. see the 4 tier SG communication model. For example, smart meters may use a wireless mesh network that uses a fiber optic backbone for its communications.

  - Example technologies include but are not limited to the following:

    1. Tier 1
       a. Fiber Options
       b. Analog or Digital Microwave
       c. Leased or Owned digital point to point circuits
       d. MPLS (multi-protocol label switching)
       e. Frame Relay
    2. Tier 2

    a. Point to multipoint RF technologies (e.g. WiMax)
    b. Power Line Carrier
    c. Cellular (data and voice)
    d. Satellite
3. Tier 3
    a. Land mobile radio
    b. Wireless RF P-2-P network
    c. Wireless radio frequency mesh network
    d. One-way and Two-way paging
    e. Satellite
4. Tier 4
    a. ZigBee
    b. Home plug
    c. U-Snap
    d. Internet

- System Protection drives the need for fiber optic deployments and can be best managed by the Utility to ensure reliable performance. Therefore it is available to leverage other Smart Grid communication application requirements.

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 communication system needs for electric utilities increase significantly to support smart grid applications (bandwidth, reliability, security and latency), electric utilities need reliable, upgradeable communication options that will be available during challenging events when other forms of communication are not available. The reliability of power delivery is directly related to the reliability of related communication systems. This includes a strong backbone, dedicated Utility spectrum and system ownership to support customer needs.
- Long term availability of parts, components and networks

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

- Commercial wired and wireless networks meet some of today's utility needs specifically in areas where good service is adequate, i.e. 98-99% availability. However, experience has shown that these systems are inadequate to meet reliability, latency and bandwidth requirements for many utility applications that are necessary to maintain the stability of the grid and support customer restoration activities during a storm event.

- Utilities have had significant history with the use of Public Carrier Communications and the Carrier's have demonstrated time and again an inability to meet Utility requirements in reliability and sustainability.
- Commitment to long term network availability

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

    - Commercial networks need to be hardened to improve reliability and availability of services including prioritization of data and voice services in times of emergencies and power system protection and automation communications. Additionally, there needs to be SLA improvements and shared consequential damages in the event performance levels are not met that in turn cause damage to either the Utilities or customers property. This includes a minimum of 48 hour backup for communication facilities under loss of power and a reduction of mean-time-to-repair to provide upwards of 99.99999% availability.
    - Commercial networks do and will continue to play a role in the Utility communication technology portfolio, however, each Utility must be positioned to choose what technology is applicable to meet its needs and ultimately the customer's needs.
    - Commercial networks should provide pervasive coverage in both wired and wireless technologies in rural regions regardless of the business case.

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?

    - Utilities will need to provide pervasive communications system coverage and adequate capacity to meet the requirements of the smart grid application portfolio as presently defined and envisioned to support future growth. There will be multiple technologies required to support this need as enumerated above and there will be no single solution that satisfies all the requirements. These systems will be designed to be secure, interoperable and scalable and meet existing and future standards such as NIST and NERC. New applications yet to be defined within the Smart Grid portfolio will require significant additional capacity including video surveillance and thermographs.

Conclusion

Exelon respectfully requests that the Department consider these comments and ensure that any DOE action recommended regarding the communications requirements of electric utilities is consistent with them.

Respectfully submitted,

/s/ Joseph Watson, Jr.

Joseph Watson, Jr.
Director, Federal Government Affairs

Exelon Corporation
101 Constitution Avenue, N.W.
Suite 400 East
Washington D.C. 20001
(202) 347-7500 (telephone)
(202) 347-7501 (facsimile)
joseph.watson@exeloncorp.com

Douglas M. McGinnis
Principal IT Architect
Exelon Corporation
2301 Market St.
Philadelphia, PA 19103
(215) 841-6478 (telephone)
doug.mcginnis@exeloncorp.com

Daniel C. Hill
Senior Vice President and
Chief Information Officer
Exelon Corporation
10 S. Dearborn St.
Chicago, IL 60603
(312) 394-3598
daniel.hill@exeloncorp.com

Dated: July 12, 2010