Smart Wireless Communications for Smart Devices

John "Jake" Rasweiler, MSEE, MBA, P.E., PMP
Vice President: IT, Engineering & Network Operations

Arcadian Networks, Inc.
400 Columbus Ave, Suite 210E
Valhalla, NY 10595

Jake.Rasweiler@arcadiannetworks.com

Keywords: Smart Grid, spectrum, broadband, wireless, communications, Last Mile, Rural, 700 MHz, SCADA, AMI

ABSTRACT

In the context of the "Smart Grid", interoperable systems are those that promote and enhance end-to-end functionality across systems and organizations interacting with the grid itself.

The author will discuss the Wireless Communication Infrastructure interoperability issues for Utility's Smart Grid deployments and also identify the key technical and business barriers. By relating interoperability benefits, principles, and the GridWise context-setting framework, the reader will better understand the technical and business drivers critical infrastructure companies such as Electric, Water and Gas Utilities and Oil and Gas Companies must consider when adopting licensed, broadband wireless solutions for their fixed and mobile; voice and data field communications.

Rural last-mile architectures, applications and devices will be discussed.

INTRODUCTION

The "Smart-Grid" opportunity

Electric, Water and Gas Utilities and Oil and Gas companies have well understood that their field network infrastructure is the "eyes" and "ears" of their operations – connecting remote devices and field professionals in an effort to reduce the cycle time to detect problems, dispatch technicians and increase the overall security, throughput and resilience of their multi-billion dollar production assets.

Over time these industries spent millions of dollars building specialized networks for each asset and application in the field. Often, communications have been built for specific applications (SCADA, substation automation, etc.). With the growth of higher data rate applications such as automatic meter reading (AMR) and video surveillance, some specialized field communication networks no longer effectively serve the needs of the emerging "Smart" energy-efficient world. Communications needs, capabilities and deployment is evolving from serving voice demand with intermittent data collection, to system requiring constant information flow with voice as a adjunct to the data requirements. The key to untangling the communication knot rests in architects' ability to converge field communication needs to create true interoperability among people and machines.

Interoperability in the modern "smart-grid" encompasses seamless end-to-end compatibility of hardware devices and data flows from the customer application or equipment, through the distribution and transmission network, back to the ultimate power source. The rationale for interoperability is greater efficiency and decreased service interruptions through a better coordination of energy sources and uses (see Figure 1). This paper will focus on identifying and selecting "smart wireless" solutions that promote interoperability and enable the Smart-grid.

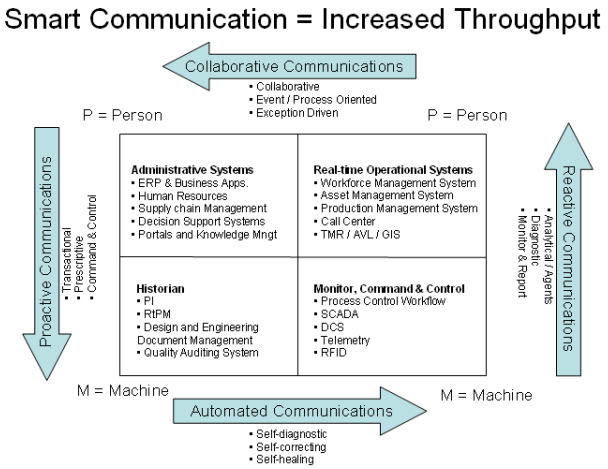


Figure 1: Benefits of smart-grid interoperability

Today, modern technology has the potential to connect the grid, increase energy savings, reduce peak power demand, and offset or avoid large generating investments. In order to achieve these benefits, the industry must shift from supply to demand response and drive exponential growth in the number of connected intelligent devices including distribution automation, substation automation, asset management, AMR, micro-grid coordination, distributed generation and appliance control beyond the meter. This technology, however, must connect the grid in a fashion that advances interoperability.

Wireless' proliferation to close the communications gap

Critical infrastructure industries still have a significant number of critical assets (substations, reclosers, C&I establishments, water lift stations, pipelines, etc.) planned for connection or left unconnected.[i] It is important to note that other critical infrastructure industries make extensive use of wireless solutions for asset connectivity. Wireless technologies by definition use spectrum which by its nature has no affinity to industry. When examining the growth in deployment the numbers are staggering.

While the electrical critical infrastructure ecosystem numbers just over 1 million assets[ii], the number expands to over 3 million when other critical infrastructure industries are considered.

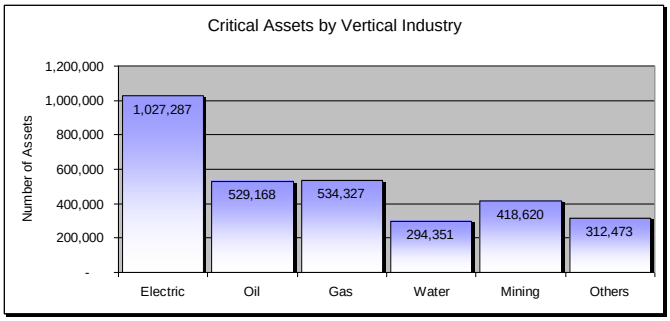


Figure 2: CII Assets by industry

These number become dwarfed by plans to deploy RF based AMI systems as outlined in the 2007 FERC report on Demand Response and Advanced Metering[iii]. The number of meters selected to be served by RF systems exceeds 19 million. When factoring in the deployments with as of yet undeclared technology choices the potential number increases to over 43 million meters (see Table 1).

GridWise helps in making the "smart" wireless choice

The demand for greater connectivity to end points creates opportunity as well as confusion for technologists charged with cost effectively and reliably engineering solutions through the enterprise and local ecosystem. In order to assist with this process, the Gridwise Architecture Council prepared a useful template for decision makers to use when reviewing interoperability of technologies being considered for use within the smart grid. In light of this framework, communications selected must be flexible to support and promote interoperability among a wide spectrum of entrenched legacy communication options, scale with the number of connections, intelligently interleave multiple traffic flows and provide data security.

Utility	AMI type	Meters	Year	Status
Kansas City Power and Light	Fixed RF	473,863.00	1996	Contracted
Puget Sound Energy	Fixed RF	1,325,000.00	1997	Contracted
Exelon (PECO)	Fixed RF	2,100,000.00	1999	Contracted
United Illuminating (CT)	Fixed RF	320,000.00	1999	Contracted
Austin Energy	Fixed RF	125,864.00	2002	Contracted
WE Energies (WI)	Fixed RF	1,000,000.00	2002	Contracted
Colorado Springs	Fixed RF	400,000.00	2005	Contracted
Chathum Kent	Fixed RF	100,000.00	2006	Contracted
City of Seattle	Fixed RF	400,000.00	2006	Contracted
Southern Company	Fixed RF	35,000.00	2006	Contracted
Arizona Public Service	Fixed RF	800,000.00	2007	Utility plans
Austin Energy	Fixed RF	230,000.00	2007	Contracted
Consumers Energy	Fixed RF	1,700,000.00	2007	Utility plans
Duke Energy in Kentucky	Fixed RF	250,000.00	2007	Utility plans
Florida Power and Light	Fixed RF	100,000.00	2007	Contracted
Hawaiian Electric Company	Fixed RF	3,000.00	2007	Contracted
Northeast Utilities	Fixed RF	1,181,880.00	2007	Filed AMI plan
Southern California Edison	Fixed RF	4,475,000.00	2007	Filed AMI plan
WE Energies (WI)	Fixed RF	100,000.00	2007	Contracted
Xcel Energy	Fixed RF	710,000.00	2007	Contracted
Anaheim Utilities	Fixed RF	110,635.00	2008	Utility plans
Pepco Holdings	Fixed RF	1,830,000.00	2008	Filed AMI plan
CenterPoint	Fixed RF and BPL	1,900,000.00	2006	Contracted
Total RF		19,670,242.00		
BGE	TBD	1,000,000.00	2007	Filed AMI plan
DTE Energy	TBD	1,300,000.00	2007	Utility plans
Tallahassee city of	TBD	107,780.00	2007	Utility plans
Utilities active in market	TBD	3,960,000.00	2007	Market Activity
American Electric Power	TBD	4,730,000.00	2008	Utility plans
Consolidated Edison	TBD	1,900,000.00	2008	Utility plans
CPS Energy	TBD	627,210.00	2008	Utility plans
Duke Energy in NC	TBD	2,200,000.00	2008	Filed AMI plan
Energy East	TBD	1,229,788.00	2008	Filed AMI plan
Florida Power and Light	TBD	3,900,000.00	2008	Pilot Ongoing
Hawaiian Electric Company	TBD	291,580.00	2008	Pilot Ongoing
Portland General	TBD	775,000.00	2008	Filed AMI plan
San Diego Gas and Electric	TBD	1,300,000.00	2008	Filed AMI plan
Central Vermont Public Service	TBD	175,000.00	2010	Utility plans
Total RF and TBD		43,166,600.00		

Table 1: Meters served or potentially served by RF systems

Communications in the smart grid can be grouped by range, quantity and capacity. For the purposes of this discussion the groupings include[iv]:

- Backhaul: MPLS/Ethernet over Fiber, Microwave, etc.
- Mid-haul: Broadband over Power Lines, 3rd Generation wireless, 4th Generation Wireless (IP Wireless, WiMAX), Licensed and Unlicensed Radio
- Last mile: 3rd/4th Generation (3G/4G), licensed spectrum carrier services, MAS radio, Zigbee / WiFi, POTS
- Home or Personal Area Network: Zigbee, Bluetooth, Serial, Ethernet, WiFi, POTS

Wireless communication options are diverse and provide a viable choice for use in the smart grid – often in the mid-haul and last mile segments.

There are a number of factors to be considered for any choice of wireless communication. The GridWise Contextual Framework provides a thorough context to review interoperability as shown in Figure 3[v]. We will use the framework to discuss the interoperability issues for wireless technologies considered for use in a utility's Smart Grid deployment and identify the key technical and business barriers to acceptance. GridWise groups interoperability into three broad categories[vi]:

- technical interoperability
- informational interoperability
- organizational interoperability

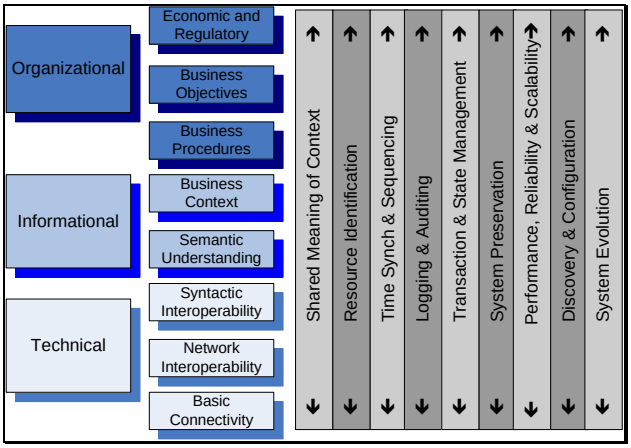


Figure 3: GridWise Interoperability Framework Design

This paper's scope will be limited to considering the interoperability aspects specifically relating to the selection of smart wireless solutions for the smart grid.

GRIDWISE FRAMEWORK: WIRELESS INTEROPERABILITY

Technical interoperability

Technical interoperability concerns the communication and physical connections between wireless infrastructure and the connected smart devices. Technically interoperable wireless infrastructure enhances end-to-end information flow.

Spectrum

Depending on the type of organization, access to licensed spectrum may involve additional cost to the overall solution. The proliferation of wireless communication deployments will necessarily increase the utilization of available spectrum potentially to the point of congestion if not properly engineered. Much of the spectrum used in the critical infrastructure space can be grouped into several holdings:

- Utility (e.g. microwave, T/LMR, MAS, etc.)

- Private/Public Carrier (Fixed Wireless, MMDS, PCS, Cellular, etc)
- Secondary Use (various)
- ISM/Unlicensed bands (900 MHz, 2.4 GHz, 5.8 GHz, etc.)

Selection of spectrum is a critical factor affecting to the level of utility, control, protection and reliability the operator enjoys on the RF link over the intended lifetime of its use.

Licensed Vs. Unlicensed:
Licensed spectrum designation identifies user priority if any for the band. Rules for each band include acceptable technologies, uses, user groups, data rate and power limitations. Licensed spectrum cost and maintenance is analogous to land rights - it is an investment asset easement in the air.

In considering such an investment, one should explore the cost benefit tradeoffs of licensed versus unlicensed spectrum. Some considerations include the economic and legal penalties associated with the networks' monitoring and reporting failure on the performance of the end device or application versus the cost of the spectrum, over the expected lifetime of the project (typically 5 years or longer). Second, consider the expected noise floor for the geography being covered by the wireless system. Organizations such as the American Petroleum Institute, the Utilities Telecom Council and the Association of American Railroads warned that if the FCC failed to take steps to transform how unlicensed (900MHz) spectrum is currently managed there would be a significant risks to the band and the hundreds of millions of devices that use it every day as interference continues to rise[vii].

Spectrum band characteristics:
Each spectrum band possesses unique physical characteristics. Several are considered below:

Selected Frequency Bands (f):

- f<30 MHz:
  - Ionospheric effects
- 30<f<300 MHz:
  - LOS space wave
  - f<10 MHz ground wave is predominant
  - Ionosphere is transparent
- 300<f<3 GHz:
  - Reflection by ground and buildings
  - Troposphere refraction
  - Diffraction over hill tops and buildings
  - Multipath effects because of trees and buildings
- 3<f<30 GHz:
  - Atmospheric absorption
  - Diffraction by precipitation

When choosing an operating band, one must match the spectrum characteristics to the desired network design. Lower operating frequencies tend to have improved long range and non line of sight (NLOS) characteristics and well as extended propagation under certain environmental conditions. Higher frequencies tend to require line of sight conditions (LOS) and exhibit signal attenuation with precipitation.

Licensing spectrum does incur a level of cost and maintenance that must be considered. It is inherently more secure than ISM bands due to reserved use by licensed operations as well as the limitation on equipment sales to licensed operators. A licensed solution gives the technologist a degree of control and predictability over the use of spectrum during the life of the deployment. Very often the licensing choice weighs the management and expectation of risk in the band against the level of assurance provided by the licensing right afforded to and mandated by the project(s) under consideration.

IP as the Interoperability standard

Due to the proliferation of wireless technologies and availability of Internet Protocol (IP) enabled devices, IP via Ethernet is quickly becoming the communication standard deeper into the grid. IP provides numerous advantages including faster polling times, flexible addressing and scalability, cyber security (encryption, RADIUS authentication, VLAN tagging, MAC filtering, etc.) and support for automatic re-routing in the event of an emergency.

IP provides a common method for networks and devices to communicate. Most legacy communications (serial, MODBUS, etc.) can be accommodated on a IP link providing a convergence advantage where more than one application can be accommodated by one IP connection – all enjoying the benefits or routing, security and often economies of scale.

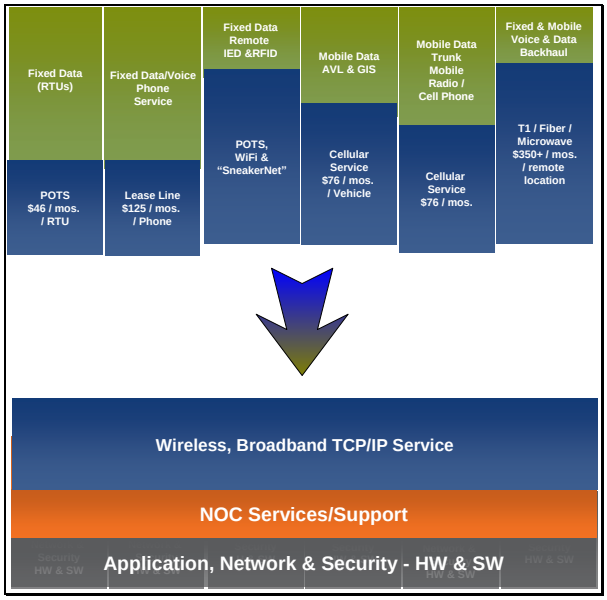


Figure 4: Convergence to integrated IP solutions

Physical connections: Power, type, path and quantity of communications interfaces (e.g. AC/DC, serial, IP)

Designed Reliability

Deployment decisions must consider the impact of the supporting infrastructure - whether it is a standalone unit or OEM device - to the expected reliability.

As a reference, consider the reliability tier definitions of the Uptime Institute which defines connection and supporting infrastructure necessary for each level of expected reliability[viii]. Factors include data distribution path redundancy, power and fault tolerance.

Tier Rquirement	Tier I	Tier II	Tier III	Tier IV
Component Redundancy	N	N+1	N+1	N+1 minimum
Distribution Paths	1	1	1 Active + 1 Alternate	2 simultaneous
Fault Tolerant	no	no	no	yes
Availability (data Center)	99.67%	99.75%	99.98%	99.99%

Table 2: Designed availability tiers

In the case of commercial wireless carriers, many have backup power; however, the available duration may be insufficient. As indicated in the independent panel review following hurricane Katrina, the FCC is only now requiring that cell sites maintain eight hours emergency backup power.[ix]

Supporting Infrastructure and Network Interoperability

When considering deployment, factors include the feasibility of supporting the infrastructure with the available power, space, and structural elements. Many backhaul and mid-haul technologies require the use of tower mounted antennas, which must be among the factors considered

Wireless communications are beneficial only if they provide communications and are available in the locations where smart devices are deployed. The FCC licenses spectrum by geographic areas or locations (e.g. major economic areas MEAs). The boundaries may or may not coincide with the utility operators' exact area of interest.

Wireless Infrastructure Viability

Traditional utility investments have long depreciable lives usually in excess of 20 years. Smart grid applications are; however, under consideration for information technology designation with a 5-year depreciable life[x]. Under either scenario, wireless infrastructure selection must consider the vendor platform stability, commitment and roadmap to ensure long term product support and availability over the expected life of the project. For illustration purposes, consider:

- Wi-Fi was invented in 1991 and first established as a standard in 1997 with several versions A, B, G released
- 1997: GSM service launched domestically with EDGE upgrades in 2003 and migration to HSDPA begun in 2006

INFORMATIONAL INTEROPERABILITY

Smart Wireless Performance

Selection of wireless infrastructure must consider the requirements of the supported applications. Specifications include:

- Data rate capability: certain technologies (e.g. CDMA) have asymmetrical throughput from tower to remote. Selection must consider the predominant direction of traffic flow and ensure the available data rate is sufficient for applications
- Latency: when encapsulating serial data on IP technology, the added TCP/IP overhead may deliver inconsistent or excessive latency (> 100 ms range) which may be problematic for serial SCADA masters and protocols[xi]. UDP provides an alternate choice to improve consistent packet latency.
- Quality of service (QOS): QOS provides a mechanism to mark and classify data-streams,

ensuring appropriate prioritization by the routing infrastructure – especially important during periods of wireless system loading. Data priority (QOS) is rapidly becoming adopted and ubiquitous in the backhaul and mid-haul network segments. Many smart wireless communications options provide compatible QOS options capable of extending QOS capability though the wireless segment.

Network health & status

To maximize network resilience and response time as well as differentiate communications health from grid health, many utilities have telecommunications Network Monitoring Systems (NMS). While state-of-the art wireless technologies are available with element or network management packages, most are SNMP V1, V2 or V3 compliant allowing for integration with commercially available 3rd party NMS packages. Commercial wireless carriers rarely provide such network access – even in premium service arrangements.

ORGANIZATIONAL INTEROPERABILITY

Cyber security implementation considerations

Wireless communications are often mistakenly associated with Wi-Fi enabled cyber hacking. A properly engineered security plan will be largely independent of the physical connection type – wired or wireless. Adding these elements requires additional maintenance and IT knowledge from the utility. The whole area of cyber security requires a number of highly skilled IT staff in order to design, implement and maintain the entire security domain and policy. Traditionally, utilities have had two choices to modernize their field infrastructure, they could:

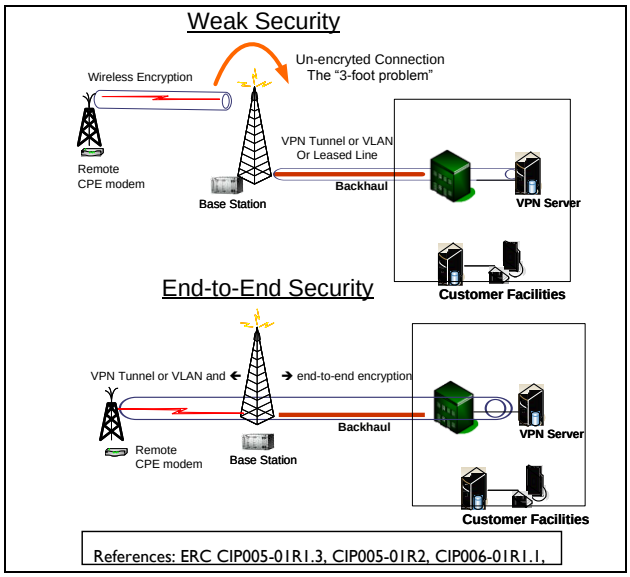
1) either build and maintain their communication infrastructure, which not only is capital intensive, but also non-core to the business of producing energy, or delivering water or gas service, or
2) partner with a consumer-oriented carriers who typically are challenged to provide last-mile and rural communication services or an SLA security and performance guarantee that meets or exceeds utility specifications.

Emerging alternatives focused on critical infrastructure, machine-to-machine and remote communications offer economies of scale associated with a consumer-oriented carrier, combined with the mission-critical security and performance requirements and flexibility of control required by today's public safety, utility and oil and gas companies. Hopefully, as the need for licensed spectrum, increased security and "smart" integrated solutions continues to grow, additional alternatives will become available to critical infrastructure companies.

Cyber security and NERC CIP ESPs

Equipment and technology are critical factors to the extent that they enable interoperability with the purchasers' security practices and NERC Critical Infrastructure Protection (CIP) standards[xii], CIP-002 to CIP-009. These CIP requirements describe proper management of secure network devices. In particular, the key concern for CIP-005, is creation of an Electronic Security Perimeter (ESP). This requires implementation of a security device at the network boundary between the substation and the external WAN environment. Currently available technologies blur the line between radio function, security function and software-based security/firewall agents present in the wireless devices themselves (encryption, IPSEC VPN, SSL, HTTPS, etc).

Careful consideration must be made when factoring cyber security in concert with physical access control at the facility. Many wireless options today provide air-link encryption compliant to NERC. It is not uncommon for multiple electrical utility entities to co-locate communications in facilities owned by one party. NERC CIP-006 requires physical security be closely managed for areas within the ESP. When CIP-005 and CIP-006 are considered in tandem however, wireless deployments using only air-link encryption may leave the link vulnerable in the facility. Firewall (VPN) functionality between the remote location and the head office minimizes cyber vulnerability at intermediate connections. Moreover, legacy systems migrated to communication links secured by VPNs, retrofits security without having to upgrade the application itself.



In order to manage compliance with intrusion detection and password management, RADIUS authentication compatibility (or equivalent) is a necessity and mandatory in selected technologies interacting at or near the ESP. Fulfillment of cyber-security needs by wireless infrastructure provides functionality capable of advancing interoperability in the smart grid while minimizing overall security risk.

Change Control and Maintenance Schedules

Selection of smart wireless options involves considering the tradeoffs of going outside the enterprise for assistance which may include risk or cost mitigation, outsourcing services, service providers, private carrier tailored solutions compatible with the smart device plans, or as a source of staff augmentation. When connecting critical infrastructure smart devices, operators should strive for maximum control over wireless network change and maintenance notification so as to minimize conflict with ISO notification, peak demand or other critical smart-grid operating periods and maximize interoperability with the System Operations requirements for the utility operator.

Financing and Ownership

Wireless communication investments require significant financial commitment. Funding profiles often differ based on the ownership structure of each utility (e.g. IOU, municipal, Coop, etc.). Infrastructure vendor selection may hinge on the financial flexibility afforded in the procurement process. Commercial carriers may sell or lease the subscriber device, whereas equipment providers often sell or finance equipment. System integrators or private carriers may have greater flexibility in offering a wide spectrum of options.

SUMMARY

This paper reviewed the interoperability issues (technical, informational, organizational) for the selection of Wireless Communication Infrastructure for Utility's Smart Grid deployments and also identified the key technical and business factors by relating aspects associated with interoperability benefits, principles, and the GridWise context-setting framework. Specifically, the paper discussed technical and business drivers critical infrastructure companies such as Electric, Water and Gas Utilities and Oil and Gas Companies must consider when adopting broadband, licensed, wireless communication networking infrastructure to converge their fixed and mobile; voice and data field communications.

ABOUT THE AUTHOR

John "Jake" Rasweiler is the Vice President of Engineering and Network Operations at Arcadian Networks, Inc. John's telecommunications career includes work at CellularOne, AT&T Wireless Services and most recently Sprint Nextel where he held positions including Senior Director RF Engineering and Market Director. His background and experience include fixed and wireless network design, site development, field and network operations, and construction. In addition, John presented at international conferences on the topics of machine-to-machine communications, the digital oil field, microcell and urban network design. He holds BA, MSEE and MBA degrees as well as two patents, is a licensed professional engineer (P.E.) and a project management professional (PMP). His current responsibilities include managing the design of custom, broadband, wireless communication services for the energy industry (electric, water, and gas utilities and oil and gas companies) using private licensed 700 MHz spectrum and converged IP platforms to improve operating efficiencies and promote future initiatives.

APPENDIX: APPLICATION OF THE GRIDWISE EVALUATION CHECKLIST FOR WIRELESS INFRASTRUCTURE ALTERNATIVES

The GridWise Architecture Council proposes a reference checklist[1] to be used by decision makers selecting smart grid component decisions targeted at advancing interoperability on the smart grid. The interoperability checklist, for the purposes of this paper, was adapted to enable initial evaluation of wireless infrastructure options and its ability advance interoperability within the smart grid.

1. Does the wireless solution specify the point of interface, whether this part of the system interacts with other elements:
   - Grid equipment
   - Software
   - The market
   - Other business organizations
   - Users/operators
2. Does the wireless solution make use of publicly known open architecture?
3. Is the Wireless solution technologically neutral?
   - Capability and performance are defined while allowing technological innovation
4. Are multiple vendor sourcing options are available to avoid being held captive by one vendor?
5. Does the wireless infrastructure rely on open and published standards for connection to network elements?
6. Does the wireless solution allow vendor and communication interface flexibility and diversity?
   - To connect with various types of communications
7. Does the wireless system use standard communication protocols capable of supporting common electric utility protocols including:
   - Modbus, DNP3, IEC 61850
   - common information models
8. Does the wireless option provide improved access and availability of data to the targeted information users including:
   - Interval data
   - Grid health
   - Operational commands
9. Does the wireless option enable efficient expansion and scalability resulting in improved efficiency and response time?
10. Does the wireless option provide cyber-security compliant with NERC CIP standards and privacy best practices?
11. In the case of mission critical electricity systems and user well-being, is adequate redundancy and protection designed into the overall wireless solution sufficient to mitigate harm to the user or system?
12. Can the wireless system software be upgraded and remotely configured?
13. Is the solution backwardly compatible to earlier generations of wireless infrastructure?
14. Do wireless options allow collaborator or users to make independent decisions through the use of authorization levels and permission?

BIBLIOGRAPHY

1. Rick Schmidt, *Automation Communications Alternatives, New Communications Technology Solutions* , can be found at: http://www.powersystem.org/publications/papers/papers.aspx
2. Office of Senator Maria Cantwell, *Overview of the "Reducing Demand through Electricity Grid Intelligence" Act*, April 25, 2007
3. EICTA,, EICTA White Paper on Standardisation and Interoperability, November 2006, can be found at: http://www.eicta.org/fileadmin/user_upload/document/document1166544474.pdf
4. Robert J. Landman, "Section 10, Power System Components, 10.7 Supervisory Control and Data Acquisition Systems", *Standard Handbook for Electrical Engineers by Donald G. Fink and H. Wayne Beaty*, pp 10-147 to 10-168, can be found at: http://www.sandc.com/edocs_pdfs/EDOC_001914.pdf
5. SAIC Smart Grid Team, *San Diego Smart Grid Study: Final Report*, October 2006, can be found at: http://www.gridwise.org/pdf/061017_SDSmartGridStudyFINAL.pdf
6. Sarah Poole , "Wireless in the Smart Grid Advanced Metering Infrastructure", *UTCJOURNAL* • 1ST.Q2007, can be found at: http://www.journal.utc.org/file_depot/0-10000000/0-10000/3389/conman/Wireless+Smart+Grid+1-07.pdf

[i] Massoud Amin and Phillip F. Schewe, "Preventing Blackouts", *Scientific American*, May 2007, Vol. 296, no. 5, can be found at: http://www.math.uwaterloo.ca/~yhao/scientific_american/Scientific.American.2007.05.May.pdf

[ii] Frost & Sullivan report for Arcadian Networks, Inc.

[iii] FERC, *Assessment of Demand Response & Advanced Metering*: Staff Report, Docket No. AD06-2, August 7, 2006, available at: http://www.ferc.gov/industries/electric/indus-act/demand-response.asp

[iv] SAIC Smart Grid Team, *San Diego Smart Grid Study: Final Report*, October 2006, can be found at: http://www.gridwise.org/pdf/061017_SDSmartGridStudyFINAL.pdf

[v] GridWise Interoperability Context-Setting Framework – Draft, January 2007 available at: http://www.gridwiseac.org/pdfs/interopframework_v05%20070129.pdf

[vi] GridWise Architecture Council, Decision-maker's interoperability checklist draft version 1.0, April 2007 available at: http://www.gridwiseac.org/pdfs/gwac_decisionmakerchecklist.pdf

[vii] "UTC,API Back 'Spectrum Etiquette' for 900 MHz Unlicensed Band", UTC Industry Intelligence, October 18, 2007, Volume 5 Issue 40, can be found at: http://www.utc.org/page/admin/?cd_v=disp&cbr_v=dcb&nt=true&cbr_eid=53813&ct=contentbrowser

[viii] W. Pitt Turner IV, P.E., John H Seader, P.E., and Kenneth G. Brill, "Tier Classifications Define Site Infrastructure Performance", *Uptime Institute White Paper*, can be found at: http://www.iswest.com/colocation/TierClassification.pdf

[ix] Federal Communications Commission, FCC 07-10, In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, Released: June 8, 2007, section 77, p25. can be found at: http://www.cpeworld.org/files/fk/file/FCC-07-107A1.pdf

[x] Office of Senator Maria Cantwell, Overview of the "Reducing Demand through Electricity Grid Intelligence" Act, April 25, 2007

[xi] John M. Shaw, "Evolving to a Strategic Substation Network Architecture", *Electric Energy T&D Magazine*, January-February 2007, Issue 1, Vol. 7, can be found at http://www.garrettcom.com/techsupport/papers/electric_energy_shaw.pdf

[xii] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf