Extending SCADA Networks Using Wireless Communications

Steve T. Watt, Henry Loehner, Shankar V. Achanta, Andy Kivi, and Ben Rowland
Schweitzer Engineering Laboratories, Inc.

Presented at the
2nd Annual PAC World Americas Conference
Raleigh, North Carolina
September 1–3, 2015

Originally presented at the
Power and Energy Automation Conference, March 2015

Extending SCADA Networks Using Wireless Communications

Steve T. Watt, Henry Loehner, Shankar V. Achanta, Andy Kivi, and Ben Rowland,
Schweitzer Engineering Laboratories, Inc.

Abstract—**With the deployment of intelligent electronic devices (IEDs) in the substation yard, there is a need to integrate the IED measurements into existing supervisory control and data acquisition (SCADA) systems. Typical SCADA networks used within a substation control house consist of a copper or fiber communications infrastructure using serial or Ethernet protocols. When extending SCADA networks to remotely located IEDs, engineers have the following options: copper cables, fiber cables, or wireless. Extending copper cables outside of the control house is not advisable because of electrical interference resulting in unreliable communications links or even equipment damage. Fiber-optic cables are an extremely reliable means of transporting information between remotely located IEDs. For greenfield IED installations or for installations where high-availability communications links are required, fiber is the practical design approach. However, for local-area network (LAN) extension of existing SCADA networks, wireless communication is a lower-cost alternative that is worth consideration.**

This paper explores technology options for extending LANs to devices in a substation yard by using wireless technology and addresses the following:

- **SCADA requirements for wireless networks.**
- **Different types of wireless technology.**
- **Considerations for additional applications.**

I. Introduction

This paper explores technology options for extending local-area networks (LANs) to devices in a substation yard by using wireless technology.

When intelligent electronic devices (IEDs) are upgraded in substation yards, there is a need to add supervisory control and data acquisition (SCADA) communication to these new, more intelligent devices. Fiber-optic cables are an extremely reliable means of transporting information between remotely located IEDs. Fiber-optic cable has the following advantages over copper cables: isolation from ground potential rise, prevention of induced electrical noise, and elimination of signal ground loops. Cable costs are about $100 plus $1.50 to $4 per yard for a duplex cable with variation based on the ruggedness of the cable.

However, for local-area SCADA network extension in existing substation yards, fiber-optic cabling installation can be expensive and slow. Trenching in existing substation yards is complex and time-consuming. Installation costs vary by geography, but a common estimate for installing a single run of fiber in a substation yard can exceed $25,000.

Wireless networking offers a cost-effective alternative to running fiber-optic cable in existing substation yards. Wireless networking can provide up to 90 percent savings versus installing fiber-optic cabling, with greatly expedited implementation. Before we outline the various wireless networking options, let us define in greater detail the requirements for SCADA communication.

II. SCADA Requirements for Wireless Networks

A SCADA system provides the monitoring and control of remote devices through a communications network. In their early stages, SCADA systems were designed as telemetry systems with little to no control because of communications bandwidth constraints. Today, SCADA networks consist of many remote terminal units (RTUs) that communicate back to a central computer using standard Modbus® or DNP3 communications protocols. These SCADA system protocols use polling schemes to gather information from each end device and report the data back to a central SCADA master. The system can then automate control decisions based on the data received. Because SCADA networks are developed around low-speed communications, the throughput and latency requirements within the communications network are not demanding and allow for large implementations of networked devices.

Fig. 1 shows the interactions between various domains through communications for smart grid solutions [1].

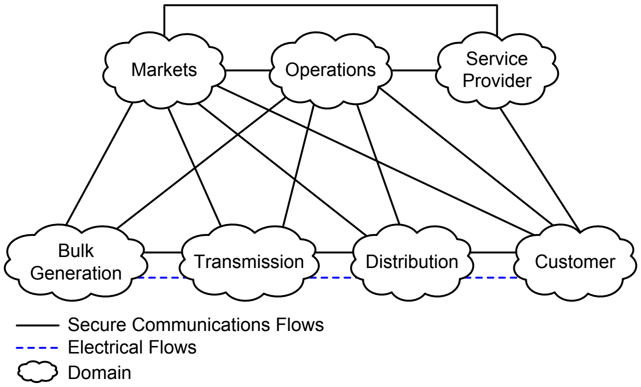

Fig. 1. National Institute of Standards and Technology (NIST) Smart Grid Framework

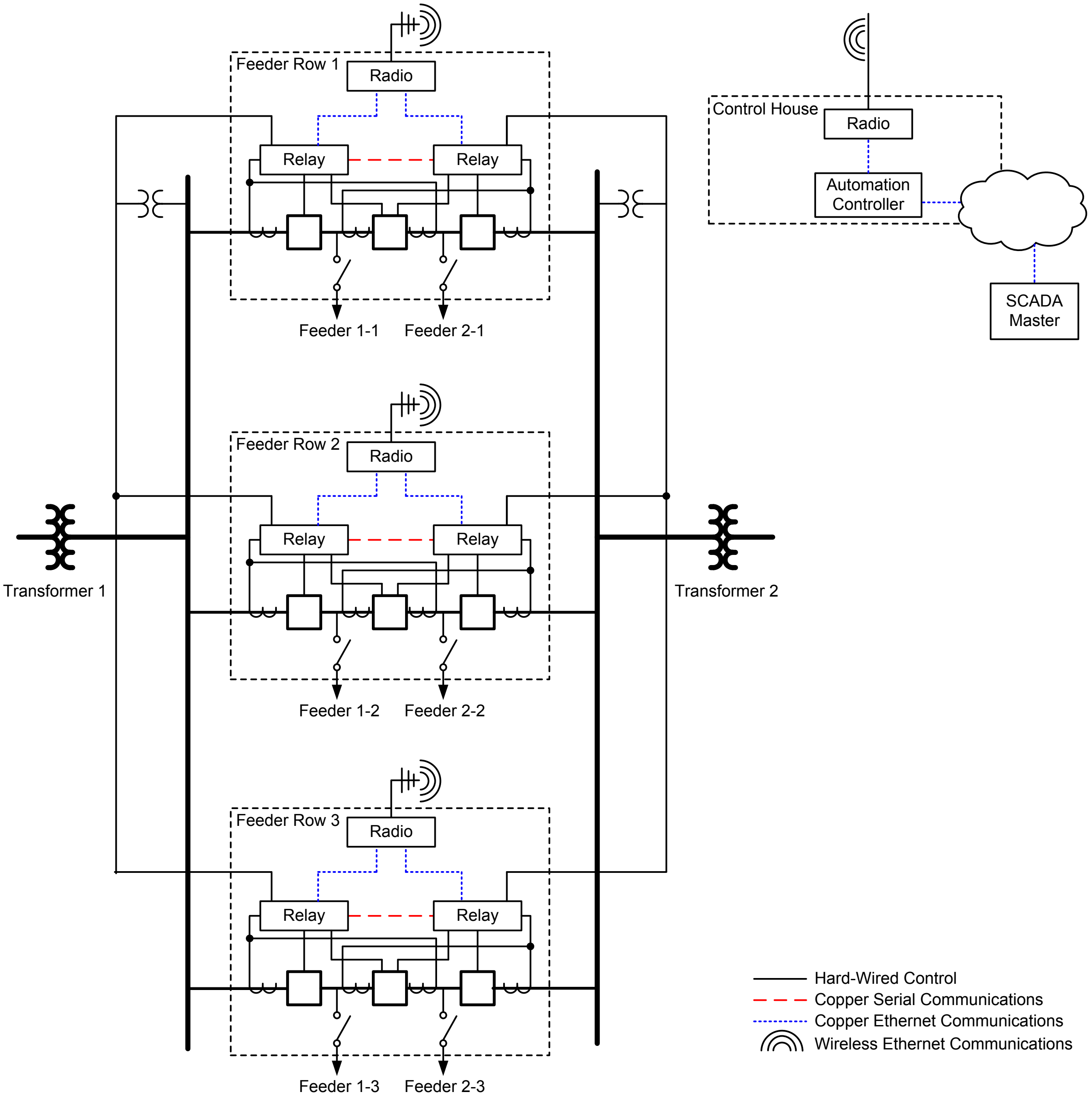

Fig. 2. Schematic of Three Communications Links to Three Feeder Rows in a Substation Yard

Interdomain communications usually occur via wide-area network backhaul communications. Devices that are in the operations domain use the backhaul communications links to gather information for SCADA applications. However, for intradomain communications (e.g., communications in a distribution substation between the control house and a cabinet in a yard), there are several options available, including fiber for greenfield installations and short-range wireless for existing installations. There are instances where information collected via these short-range links is transported to the SCADA master in the operations domain via backhaul communications links. Fig. 2 shows a scheme for such communications. Fig. 3 shows wireless communications links in a substation yard.

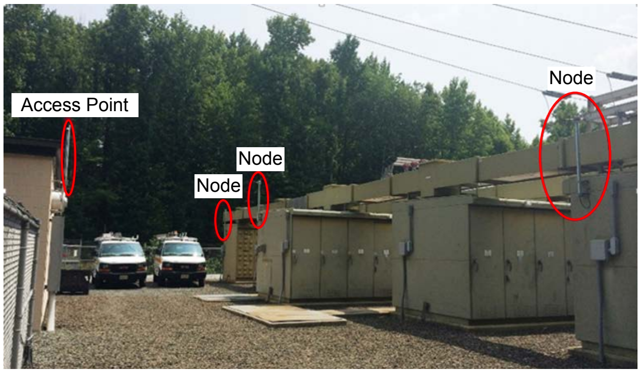

Fig. 3. Access Point and Communications Nodes in a Substation Yard

SCADA traffic is commonly sent using Transmission Control Protocol/Internet Protocol (TCP/IP) over Ethernet, which provides guaranteed delivery of messages to the application through message acknowledgements. At the wireless link layer, radio systems generally acknowledge all wireless data transfers and re-send those that are lost (at least once). With these two mechanisms in place, wireless links can provide a high level of communications reliability for SCADA data collection. This is true even in the face of burst errors due to interference or fading effects on the wireless link.

For short-range SCADA data collection within a substation or utility site yard, wireless link distances might range from tens of feet to 1,000 yards at a large site. For most wireless technologies, these distances do not pose a problem. However, because of the presence of the metal infrastructure common in a substation, there are opportunities for multipath reflections and obtaining a clear line of sight may be difficult. In these conditions, systems operating at lower frequencies will provide better performance due to more favorable radio propagation characteristics.

SCADA data collection applications (DNP3 and Modbus) were originally designed for use with low-bandwidth serial data communications links and as such are tolerant of long communications latencies. In SCADA-over-IP applications, the higher data rates associated with wireless IP data links, or wired Ethernet networks, allow for lower communications latency. Latency requirements for a specific SCADA scheme depend on how many devices are being polled and the rate at which they need to be polled relative to control system response time requirements. The user can trade off wireless network size to achieve a desired response time for a given wireless network data rate. Wireless systems with higher throughput rates allow more flexibility with respect to network size and polling rates. For SCADA communication in a substation yard, 20 to 25 end devices are typical for a system.

SCADA polling and response messages will typically range from less than 100 bytes to around 350 bytes in length. SCADA polling rates can vary widely but are not usually faster than once a second or once every other second. This results in an approximate upper bound on network loading of 100 to 350 bytes per second (800 to 2,800 bits per second [bps]) per device being polled. This does not account for wireless link protocol overhead and inefficiency in channel access, which may be equivalent to doubling the amount of data sent across the link, resulting in a total wireless network burden of about 1.6 to 5.6 kbps per SCADA device polling once per second. For less frequent polling intervals, the network load can be as much as ten times less than this upper bound.

From this analysis, it is easy to see that very low data rate wireless systems with throughput on the order of 10 kbps would be able to support only a relatively small number of devices with a fast polling cycle but support more devices with less frequent polling intervals. Wireless systems with throughput around 100 kbps would be able to handle a moderate number of devices with a fast polling rate and a large number of devices with a slower polling rate. Higher speed wireless networks with throughput around 1 Mbps or higher would be able to handle a large number of devices regardless of polling rate.

III. Different Types of Wireless Networking

The application of wireless technology for substation SCADA data collection includes a number of options with respect to network topologies, frequency bands, and devices. A number of these are outlined in this section, and the attributes of the technology as they relate to the requirements of SCADA data collection are explored.

A. Network Topologies

1) Point to Point

A point-to-point network contains only two devices. This is the simplest wireless network topology. In some circumstances, multiple point-to-point networks can be set up in a single geographic area to provide a pseudo point-to-multipoint network.

2) Point to Multipoint

In a point-to-multipoint network, multiple terminal devices communicate through a base station or access point. This type of network is useful for data collection and general wireless communication with multiple devices.

3) Mesh

In a mesh network, each device communicates with more than one other device in the network. If two devices can communicate directly, they will do so. If they cannot, they will use intermediary devices to relay messages to their final destination.

The presence of redundant links in the network prevents the loss of communication if a single link is compromised. Mesh can be a good topology in hilly terrain or around tall buildings, where nodes do not have line-of-sight to the access point and can connect through a nearby node.

However, mesh has tradeoffs—increased system overhead associated with routing messages, resulting in lower throughput and longer latency, and a greater density of devices is required to provide path redundancy.

B. Industrial, Scientific, and Medical (ISM) Bands

The ISM radio bands in the United States consist of three separate frequency allocations. The first is between 902 and 928 MHz, the second is from 2,400 to 2,483.5 MHz, and the last is between 5,725 and 5,875 MHz. The first of these bands is unique to the Americas, while the other two are recognized as ISM bands worldwide. These bands are commonly referred to as license-free bands because users do not need a license to operate a radio in these bands. The downside of license-free bands is that use in any particular geographical area is shared among many potential users.

Being a license-free band does not mean there are no rules for use of this spectrum. On the contrary, the U.S. Federal Communications Commission (FCC) has defined very specific rules to allow shared use among many different entities. At the same time, the rules allow a relatively wide range of technologies to be deployed in these bands, from relatively narrow-band frequency-hopping radios to high-bandwidth Wi-Fi® devices. The breadth of technology options in these bands is explored in subsequent paragraphs, but first, the general characteristics of the bands are described along with some general advantages and disadvantages of using them.

Each of the ISM bands provides a relatively broad spectrum allocation (26 MHz for the 900 MHz band, 80 MHz for the 2.4 GHz band, and 150 MHz for the 5.8 GHz band). As such, they provide the bandwidth needed for broadband, high-data-rate data services. This is a distinct advantage not shared by the narrow-band ultra-high frequency (UHF) licensed bands described later in this paper. The fact that there are no licensing requirements means that it is easy for a utility or other user to deploy and operate a radio network.

There is a disadvantage to these bands being shared because there can be background interference from other users that can limit the ability to receive low-level signals and limit the link range. The interference environment is constantly changing as new users come online in one area or another. Crowding and interference can be especially problematic in the 2.4 GHz ISM band, which is widely used for Wi-Fi services worldwide.

The FCC and other international regulatory bodies have defined specific rules for operation of devices in the ISM bands to mitigate the impact of interference from multiple users. Each country generally creates its own regulations for ISM band devices, but for the most part, these country-specific rules are modeled after either the FCC regulations (in the case of many Central and South American countries) or European Union (EU) regulations (in the case of many African and Asian countries). Individual countries sometimes have exceptions to the base FCC or EU rules to account for differences in device usage and/or frequency band allocations. The FCC regulations for the three ISM bands discussed previously are contained in the Code of Federal Regulations Section 47 Part 15.247. The EU regulations for the 2.4 GHz ISM band are contained in EN 300 328, while the EU regulations for the 5.8 GHz band are contained in EN 302 502 [2]. The following lists outline some of the more significant FCC and EU regulations for these ISM bands.

The rules of operation for the 900 MHz band (FCC) are as follows:

- Maximum radio transmit power of 30 dBm.
- Maximum Equivalent Isotropically Radiated Power (EIRP) (transmit power out of the antenna) of 36 dBm.
- Frequency hopping for devices with channel bandwidths of less than 500 kHz.
- Digital modulation for devices with channel bandwidths greater than 500 kHz.

The rules of operation for the 2.4 GHz band (FCC) are as follows:

- Maximum radio transmit power of 30 dBm.
- For EIRP point-to-point links, maximum antenna gain of 6 dBi plus 3 dBi for every 1 dBm that the radio transmit power is below 30 dBm.

The rules of operation for the 5.8 GHz band (FCC) are as follows:

- Maximum radio transmit power of 30 dBm.
- Unlimited EIRP for point to point links, with no required reduction in radio transmit power for high-gain antennas.

The rules of operation for the 2.4 GHz band (EU) are as follows:

- Allowance of frequency hopping and digital modulation devices.
- For Wi-Fi and similar adaptive (listen-before-talk) systems, maximum EIRP of 20 dBm.
- For non-adaptive systems with EIRP greater than 10 dBm, limited duty cycle (transmitter 3.5 to 10 milliseconds maximum on and 3.5 to 10 milliseconds minimum off) and channel use (10 percent).
- For nonadaptive systems with a maximum EIRP of less than 10 dBm, no duty cycle or channel use restrictions.
- Channel occupancy time of 1 to 10 milliseconds.

The rules of operation for the 5.8 GHz band (EU) are as follows:

- Nominal occupied bandwidth of 10 or 20 MHz.
- Radio transmit power of 27/30 dBm for 10/20 MHz channels.
- EIRP of 33/36 dBm for 10/20 MHz channels.
- Power spectral density of 23 dBm/MHz.
- Required channel availability check to avoid radar interference.

C. ISM Band Device Technologies

Devices operating in the ISM bands can be proprietary designs with unique attributes tailored to a specific application or market need, designs that strictly adhere to a specific industry standard, or hybrids that incorporate elements of a standard but also include some proprietary design aspects.

1) Standards-Based ISM Devices

There are several industry standards that define specifications for devices operating in the ISM bands. These include IEEE 802.15.1 (Bluetooth®), IEEE 802.15.4 (ZigBee®), and IEEE 802.11 (Wi-Fi). Devices that adhere to these standards are widely available. Bluetooth is the most popular standard for low-power short-range communications for applications like wireless audio. ZigBee is widely used for low-power industrial data communications, including automated meter reading. Wi-Fi is the standard for consumer wireless LAN solutions. The main attributes of these systems are listed in the following subsections.

2) *IEEE 802.15.1 (Bluetooth)*

Bluetooth is a short-range wireless technology based on the IEEE 802.15.1 standard originally developed to replace serial data cables. Communication is point-to-point only. Bluetooth uses the 2.4 GHz ISM band with frequency-hopping spread-spectrum technology with 1 MHz channels between 2.4 and 2.4835 GHz. Bluetooth transmission hops from one frequency to another in a predetermined pseudo-random fashion, and if the data transmitted over one channel are lost due to interference, the data are retransmitted at a later time on a different channel. Bluetooth devices are grouped into three classes based on their transmit power. Bluetooth technology can support communications distances up to 300 feet. The main application of Bluetooth devices for power utilities is serial port extension over wireless for device commissioning and event collection and also cable replacement over a short range between IEDs. Bluetooth communications have the following features:

- 2.4 GHz (United States and international) designs.
- Frequency hopping that mitigates impact on narrow-band interference.
- 2.1 Mbps bandwidth (but can be limited by bandwidth of serial interface [115 kbps]).
- Up to 300-foot range.
- Battery-power for portable devices.
- Improved pairing security with Version 2.1.
- Utility-grade serial-to-Bluetooth adapters that cost $100 to $300.

Advantages of Bluetooth include the following:

- Simple plug-and-play operation.
- Cable replacement for EIA-232 cables over short ranges.
- Support for portable electronics such as laptops, smart phones, and so on.

Disadvantages of Bluetooth include the following:

- Point-to-point communication only.
- Limited distance (up to 300 feet).
- 2.4 GHz band interference.
- Security concerns prior to Version 2.1.

3) *IEEE 802.15.4 (ZigBee)*

IEEE 802.15.4 wireless is commonly used for lighting, traffic management systems, industrial sensors, and meter reading applications. This standard supports low-to-moderate data throughput systems. Devices are available for both the 900 MHz and the 2.4 GHz ISM bands. A primary focus of the IEEE 802.15.4 standard has been simple, low-power connectivity. Industrial radios based on this standard should have the capacity to handle SCADA data collection on moderate-to-large networks at relatively high polling rates. Industrial ZigBee devices cost in the range of $200 to $400 and have the following features:

- 900 MHz (U.S.) or 2.4 GHz (U.S. and international) ISM bands.
- Medium channel bandwidth (1.5 MHz).
- Medium signaling rate (250 kbps).
- Capability for a 1-mile range (but low-powered devices typically only reach 300 feet).
- Low power consumption (battery operation).

Advantages of ZigBee include the following:

- Support for point-to-point, point-to-multipoint, and mesh networks.
- Capability for battery operation.
- Device interoperability.

Disadvantages of ZigBee include the following:

- Limited device offering for electric utilities.
- 2.4 GHz primary band interference issues.
- Poor security (off by default).
- Mesh network requirements for long distances.

4) *IEEE 802.11 (Wi-Fi)*

Industrial Wi-Fi devices are relatively common. These devices provide broadband communications access, which is equally desirable for both industry and consumer applications. For short-range SCADA data collection, Wi-Fi devices are a possible option. Link range is typically 300 feet outdoors but can be extended up to 1,000 yards with high-gain directional antennas, though it is likely to limit system throughput. Widespread use of Wi-Fi in business and consumer sectors can cause interference from adjacent networks sharing the same spectrum. The throughput of the system should support a relatively large number of devices for SCADA polling. The characteristics of Wi-Fi are as follows:

- 2.4 GHz and 5.8 GHz (U.S. and international) ISM bands.
- Hybrid systems designed to operate in 900 MHz ISM band.
- Broadband channel (5, 10, and 20 MHz).
- Adaptive modulation and coding rates.
- High wireless signaling rate (1 to 54 Mbps).
- Short range (300 feet typically).
- Wireless security via wired equivalent privacy (WEP) and Wi-Fi protected access (WPA) (most commonly).
- Access point and client cost of about $1,500 for designs most suitable to substations.

Advantages of Wi-Fi include the following:

- High throughput.
- Device interoperability (Wi-Fi is built into most laptop computers).
- Ability to incorporate wireless LAN and SCADA data collection on the same system.

Disadvantages of Wi-Fi include the following:

- Lots of interference in 2.4 GHz band.
- Poor propagation characteristics on 5.8 GHz band.
- Limited range.
- Reliability (devices are generally not substation hardened).
- Required client (most substation IEDs do not offer a Wi-Fi card option).
- Weak WEP security.

5) *Manufacturer-specific ISM Devices*

Manufacturer-specific devices use proprietary radio frequency technology that does not conform to any industry standard. This gives developers flexibility to better tune designs to specific applications. Manufacturer-specific ISM radio systems come in many varieties, ranging from low-bandwidth mesh systems for residential metering to mid-bandwidth solutions for distribution automation and high-bandwidth products for backhaul.

For substation SCADA data collection, the distribution automation products provide the best fit. These products typically offer data rates ranging from 100 kbps to 1 Mbps and support point-to-point or point-to-multipoint configurations. Characteristics of manufacturer-specific ISM devices are as follows:

- 900 MHz (U.S.) and 2.4 GHz (U.S. and international) designs.
- 100 kbps to 1 Mbps and 1- to 20-mile range (typically offered by distribution automation products).
- AES 128- or 256-bit encryption.
- Access point and client cost of $1,500.

Advantages of manufacturer-specific ISM devices include the following:

- Lots of product choices and tuned to applications.
- Good balance of distance and data rate.
- Device ruggedness for harsh environments.
- Low latency.

Disadvantages include the following:

- No device interoperability.
- May have interference in any ISM band.

D. Very High Frequency (VHF)/Ultra-High Frequency (UHF) Land Mobile Radio (LMR) Band Devices

LMR devices are fundamentally different from the ISM band radios described previously because of the rules governing the spectrum in which they operate. These radios are an evolution of analog frequency modulation (FM) voice radios and the rules governing usage of these radio bands were first established to provide voice communications for business and public safety agencies (fire, police, and so on). For analog FM voice communications channels, bandwidths of 25 kHz were adopted and were in place for many years. As the popularity of these types of devices increased, competition for licenses increased and channel coordination became increasingly difficult. This caused regulatory agencies to look at changes to make more efficient use of the spectrum available for this type of radio system. With the advent of audio synthesis techniques and digital communications, it became possible to provide acceptable quality voice communications in a narrower channel, and so most UHF bands were converted to 12.5 kHz channels in the first decade of the 21st century. The 12.5 kHz channel spacing is now standard, but some bands still allow a user to obtain a license for a 25 kHz channel if the equipment meets certain spectral efficiency requirements. This change, called refarming or narrowbanding by the FCC, allowed twice as many individual channels in the same band as had previously existed, easing the pressure on license application and channel coordination. The narrow channel bandwidth limits throughput and therefore is a better fit with serial devices rather than higher bandwidth Ethernet.

Even prior to the change to the narrower channels, licensees were using UHF licensed band radios for data communications as well as voice. In many instances, the same radio would provide both capabilities. Because the radios used FM for analog voice communications, it was relatively easy to convert them to use frequency-shift keying (FSK) modulation to provide digital voice and data communications. Handheld portable UHF radios are available for voice communications, and dedicated industrial UHF radios are available for data communications. Recent device developments include the use of higher order modulation in dedicated data radios to provide higher system throughput as well as improved spectral efficiency.

The narrow channel bandwidth of these devices allows a large number of channels in relatively modest band allocations. There are a number of UHF bands allocated between 150 MHz and 1 GHz, with many of them being 5 MHz or less. Across all of these bands there are thousands of separate channels available, making it relatively easy to obtain a license within most geographic areas for one or multiple channels in any particular band.

The main attributes of these narrow-band UHF radios are as follows:

- 12.5 kHz channel.
- Proprietary designs.
- Favorable radio frequency band propagation characteristics.
- Up to 10-watt transmit power.
- Receive sensitivity of typically −110 dBm.
- Various possible modulation types and rates (FSK, phase-shift keying [PSK], and quadrature amplitude modulation [QAM]).
- Low date rates (10 to 60 kbps) that align with serial interfaces.
- Long possible link range (20 to 40 miles).
- AES 128- or 256-bit encryption.
- Access point and client cost of $1,800.

Advantages include the following:

- Licensed channels that avoid interference from other users.
- Long link distance with narrow channels and higher allowable transmit power.
- Devices usually hardened for harsh environments.

Disadvantages include the following:

- Low system throughput.
- Increased latency in contention-based networks.
- No device interoperability.
- Licensing costs.

E. WiMAX Devices

WiMAX refers to implementations of IEEE 802.16, a broadband wireless standard designed to provide up to 40 Mbps data rates and provide some level of interoperability. WiMAX was originally designed to provide high-speed broadband Internet connectivity to fixed and mobile devices over long distances. Where Wi-Fi can provide wireless access for a building, a WiMAX system can provide access for a city or campus. WiMAX is also used as a wireless backhaul technology for cellular networks.

Although often compared to Wi-Fi, WiMAX is a cellular-like technology, with base stations and network infrastructure to allow mobility across multiple base station service areas. WiMAX also supports multiple services that allow devices to negotiate bandwidth and quality of service levels with the base station to meet the throughput and latency needs of a variety of applications. WiMAX supports multiple devices actively communicating with a base station simultaneously. It uses a time division multiple access (TDMA) frame structure with a 5-milliseconds frame and dynamic resource allocation on a frame-by-frame basis. The base station controls access to the wireless channel through a scheduling mechanism that takes into account the throughput and latency requirements of all attached devices. WiMAX supports multiple channel bandwidths from 1.5 to 28 MHz. It uses orthogonal frequency-division multiplexing (OFDM) modulation and fractional subcarrier allocations to provide improved performance for individual devices in the face of multipath fading.

All of this capability comes at a price of considerable system complexity and cost for base stations and associated network switching and control infrastructure. WiMAX system deployments can be expensive and would not generally be cost effective for isolated or small-scale wireless communications systems. They are more suited to large-scale utility-wide systems providing multiple types of communications services.

The WiMAX Forum is the industry group promoting WiMAX use. This group has created a document called "System Profile Requirements for Smart Grid Applications (WiGRID)" that defines the parameters of a WiMAX system that addresses the wireless communications requirements of electric utilities [3]. This system profile defines the attributes of WiMAX systems tailored to the specific latency, throughput, connectivity, and security needs of electric utility applications.

In terms of frequency bands, WiMAX devices can use licensed bands such as 2.3, 2.5, and 3.5 GHz subleased from Internet service providers or can use unlicensed 2.4 and 5.8 GHz ISM bands. They can also operate in the 3.65 GHz shared-license band.

The WiMAX standard addresses several aspects of security: user authentication, device authentication, wireless encryption, and key management.

A majority of mobile operators in the United States have chosen long-term evolution (LTE) over WiMAX as their 4G service (fourth generation of mobile Internet access technology) largely due to compatibility with previous mobile technologies. However, WiMAX is a viable choice for private industrial networks.

Base stations can cost $4,000 to $6,000 or more, while nodes are $900 to $1,800, based on design.

Advantages of WiMAX include the following:

- High data speeds (up to 30 to 40 Mbps).
- Adjustable modulation algorithm (based on physical link attributes).
- Longer link range.
- Quality of service capabilities.

Disadvantages of WiMAX include the following:

- WiMAX is far less popular than cellular.
- Expensive access point and base station cost from $4,000 to $6,000.
- More base stations are required to support operation in higher frequency and higher bandwidth applications.

F. Cellular

Cellular communication is also an option for wireless SCADA communication. In a cellular network, a given area is separated into individual cells, with each cell establishing its connection to a wireless transceiver. These cells are interconnected to cover long distances. Cellular networks have become the dominant mode of communication for consumer mobile devices, and they have the potential to work for short range SCADA as well. Cellular has many distinct advantages over other forms of wireless data communication as well as some crucial disadvantages that make it a poor fit for the short-range application.

A cellular communications network and base station infrastructure is in place worldwide, allowing greater system access while providing easy scalability. With high data speeds and low initial costs, it seems as if cellular communications would be great for any application.

On the other hand, many of the advantages of the cellular solution are not applicable to short-range SCADA. For example, cellular communications customers get a built-in network that expands across the globe. The range of the wireless link is effectively unlimited. This is a wonderful advantage for many applications, but it does not add any value for short-range SCADA because that sort of range is not a requirement.

The typical cost of a cellular modem is $600 to $1,000. However, providers also charge by the month for cellular data. Previously in the paper, we calculated that a typical SCADA device might have a network burden in the 1.6 to 5.6 kbps range. This comes out to roughly 0.5 to 2 GB per month for each device. Transferring 1 GB of data from machine to machine costs around $60 per month, although typically, as you commit to purchasing more data, the price per byte of data can decrease. Additionally, if users exceed their planned data usage, overage charges can be very expensive.

Advantages of cellular communications include the following:

- High data speeds (average rate of 5 to 30 Mbps download and 3 to 6 Mbps upload).
- Longer link range when using existing networks.
- Easily scalable (just pay for more data).
- Reduced efforts and costs associated with mounting antennas.
- Low-cost modem ($600 and up).

Disadvantages of cellular communications include the following:

- Ongoing operating expenses.
- Data overages.

- Network controlled by providers (customers have no control over the provider coverage area policies or prices).
- Data are nondeterministic and not guaranteed.

IV. Wireless Networking Options Summarized

Wireless networking is a viable alternative to fiber-optic cabling when adding SCADA communication to devices in the yard of existing substations. The cost of wireless can be 90 percent lower and installation is significantly faster. This is a new and emerging wireless application, and there are no devices specifically designed for SCADA in the substation yard, but there are several technologies that provide a good fit and should be considered.

Table I shows the communications requirements for SCADA in substation yards, and Table II is a simplified summary of wireless options. Results will vary based on substation attributes and device implementations. The following are aspects of the application to consider when selecting a communications method:

- Network topology. All of the technologies support point-to-multipoint or mesh networks except Bluetooth, which only supports point-to-point networks.
- Data rate. Using a data rate of 5.6 kbps per device with a 1-second polling rate, all of the technologies should provide adequate throughput with the exception of VHF/UHF. It would be possible to use VHF/UHF at a lower polling rate.
- Range. If the longest required link is less than 300 feet, all of the wireless technologies will provide sufficient range. If longer links are required, Bluetooth, low-power ZigBee, and Wi-Fi may not be acceptable choices.

Table I
Substation Yard SCADA Application Requirements

	Network Topology	**Data Rate**	**Distance**	**Security**	**Substation Ruggedness**	**Cost**
Requirements for SCADA in Substation Yards	Point to multipoint or mesh	140 kbps for 25 IEDs with 1-second polling	1,000 yards	Modern wireless encryption	–40 to +85°C, immunity from electrostatic discharge (ESD), surge, and radiated emissions	Must be significantly lower than installation of fiber-optic cabling

Table II
Wireless Technology Options

Wireless Technology	**Network Topology**	**Data Rate**	**Distance**	**Security**	**Substation Ruggedness**	**Cost**
Bluetooth	Point to point only	115 kbps for serial to Bluetooth	300 feet	Concerns prior to Version 2.1	Commercial or industrial	~$200 per device
ZigBee	Point to multipoint or mesh for longer distances	250 kbps	Low-power implementations reduce range to 300 feet	Some implementations default to no security	Industrial	~$300 per device
Wi-Fi	Point to multipoint	1 to 54 Mbps	300 feet to 1,000 yards	Older Wi-Fi WEP should be avoided	Commercial or industrial	~$1,350 per device
Manufacturer-specific ISM	Point to multipoint or mesh	100 kbps to 1 Mbps	20 miles	AES 128 or 256 bit	Substation hardened	~$1,350 per device
VHF/UHF	Point to multipoint	10 to 60 kbps	40 miles	AES 128 or 256 bit	Substation hardened	~$1,800 per device plus licensing fees
WiMAX	Point to multipoint	5 to 15 Mbps typical	1 to 5 miles to base station	IEEE 802.16 addresses security	Commercial or industrial	Base station costs of ~$5,000 and may require licensing fees
Cellular	Point to multipoint	5 to 30 Mbps download, 3 to 6 Mbps upload	1 to 5 miles to base station	3G and 4G encryption	Commercial or industrial	$600 for modem and ongoing monthly costs

- Security. With Bluetooth, ZigBee, Wi-Fi, and cellular, security should be analyzed based on device implementation. Older implementations of these standards suffered from security vulnerabilities (i.e., Wi-Fi WEP weaknesses). ZigBee devices default to no security but may allow the user to force encryption and message authentication. Up-to-date implementations of manufacturer-specific ISM, VHF/UHF, WiMAX, and cellular devices should offer sufficient encryption and message authentication. manufacturer-specific ISM and UHF/VHF are generally a less attractive target for attackers.
- Substation ruggedness. In this category, it is important to consider the target application for the devices. Generally, only manufacturer-specific ISM and UHF/VHF radios are primarily designed for electric utilities for distribution automation applications. They have broader operating temperature ranges and stronger immunity from electrostatic discharge, surge, and radiated emissions. Products in the other technology categories should be scrutinized for ruggedness. Some may provide acceptable reliability based on the implementation, but many will not.
- Cost. Bluetooth and ZigBee offer the lowest device costs at $100 to $400 per device. Cellular offers a lower device cost for each modem at $600 to $1,000 but requires an ongoing monthly cost for usage that scales up with data usage. Manufacturer-specific ISM radios and Wi-Fi devices are considered mid-tier from a cost perspective, averaging about $1,500 for a suitable device. UHF/VHF radios typically have a similar price tag, plus there is a cost to license the required frequency bands. WiMAX is the most expensive option because of the base station that ranges from $4,000 to $6,000. Also, to take full advantage of WiMAX, a licensed band is required.

V. Additional Consideration – Surveillance Video

Another application that may be added to existing substation yards is surveillance video.

The bandwidth requirements for a video application restrict its use to the higher-rate wireless systems with 1 Mbps or higher system throughput. If the goal is to address both SCADA and surveillance video with a wireless network, Wi-Fi, cellular, and ISM band radios with higher data rates are viable options and WiMAX solutions become more attractive.

VI. Conclusion

All seven wireless technologies have the potential to work for short-range SCADA in a substation yard. Wireless networking for short-range SCADA in substation yards is a new idea. When considering wireless technology for an implementation, it is best to evaluate several alternatives. Manufacturer-specific ISM radios are arguably the best fit, so they should be considered as one alternative.

VII. References

[1] NIST Special Publication 1108R2, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, February 2012. Available: http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.

[2] U.S. Government Publishing Office, *Electronic Code of Federal Regulations*, Title 47, Chapter 1, Subchapter A, Part 15, December 2014.

[3] WiMAX Forum, “WiMAX Forum® System Profile Requirements for Smart Grid Applications: Requirements for WiGRID,” WMF-T31-002-R010v01, February 2013.

VIII. Biographies

Steve T. Watt received his B.S. in mechanical engineering from Virginia Polytechnic Institute and State University. He worked in the information technology industry for over 20 years at Hewlett Packard before joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2012. Steve is currently the lead product manager for precise timing and wireless networking products at SEL.

Henry Loehner received his B.S. in electronic engineering from Cal Poly San Luis Obispo in 1983. He worked at Hewlett Packard and Agilent Technologies for 25 years as a radio frequency design engineer and research and development project manager, developing test and measurement equipment for the cellular telephone industry. While working for Hewlett Packard, Henry received a patent for an electronic step attenuator design. He joined Schweitzer Engineering Laboratories, Inc. in 2010 and is currently working as a lead radio frequency design engineer.

Shankar V. Achanta received his M.S. in electrical engineering from Arizona State University in 2002. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2002 as a hardware engineer, developing electronics for communications devices, data acquisition circuits, and switch mode power supplies. Shankar received a patent for a self-calibrating time code generator while working at SEL, and he is an inventor on several patents that are pending in the field of precise timing and wireless communications. He currently holds the position of research and development manager for the precise time and wireless communications group at SEL.

Andy Kivi received two B.S. degrees, one in operations management and one in information systems, from the University of Idaho. In 2004, he joined Dell Computers as an enterprise support technician, and in 2008, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as a desktop system administrator and data security technician. In 2010, he transferred to the research and development division of SEL as a project manager, and in 2013, he transferred to an application engineer position in the communications division of SEL.

Ben Rowland received his B.S. in engineering management with an emphasis in electrical engineering from Gonzaga University in May of 2014. During his time at Gonzaga, he began working as an intern at Schweitzer Engineering Laboratories, Inc. (SEL). After graduation, he started working full time at SEL. He currently holds the position of associate application engineer for the SEL precise timing and wireless products.

20150123 • TP6680-01