Evaluation of Wireless Technologies for Power Delivery Automation

Eric Sagen and Henry Loehner
Schweitzer Engineering Laboratories, Inc.

Presented at the
14th Annual Western Power Delivery Automation Conference
Spokane, Washington
March 27–29, 2012

Evaluation of Wireless Technologies for Power Delivery Automation

Eric Sagen and Henry Loehner, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper addresses the performance, reliability, security, and cost tradeoffs of wireless communications approaches for power delivery automation applications. Topics include licensed and unlicensed links, standards-based wireless protocols, and cellular radio solutions. Topologies include point-to-point, point-to-multipoint, and mesh configurations. The paper discusses the requirements for each application area, including telemetry, distribution automation, high-speed restoration, substation local-area network extension, supervisory control and data acquisition, engineering access, and wireless backhaul extension for stations that are out of reach of primary fiber-optic or microwave backhaul systems.**

The paper identifies the requirements for each of these applications, including speed, latency, throughput, bandwidth, reliability, and security, and compares the capabilities of each technology to the requirements of each application. The reader can learn from the examples and methodologies and apply this knowledge to analyze specific requirements and solutions.

I. Introduction

Radio communication is an attractive approach for many power delivery automation and monitoring applications. For links outside of the substation yard, the installed costs of wireless systems are generally lower than the cost of wires or fiber-optic links, and wireless systems can be put into service more rapidly. In some cases, it is not feasible to obtain the right of way needed for wired or fiber-optic solutions.

The cost and calendar-time advantages of wireless solutions are balanced by interference considerations. If interference causes a message to be rejected, the end equipment must be able to tolerate delays while the message is retransmitted.

Wired or wireless signals that are used for control or carry information used in control calculations need to be secured through encryption and authentication to prevent successful cyberattacks or eavesdropping.

This paper describes applications that can use wireless communication for power delivery automation and compares the requirements for these applications with the capabilities of several wireless technologies.

II. Application Areas

A. Traditional Electrical Distribution Sectionalizing and Restoration

Electrical distribution feeders are often divided into segments using small breakers or reclosers that are capable of interrupting current. The lines can be further divided into smaller sections using sectionalizers, which are switches that can be opened when there is no current flowing but are not capable of interrupting load or fault currents. Recloser controls detect an electrical fault and trip the reclosers closest to the fault, isolating the fault.

If there are remotely operable sectionalizers installed, as shown in Fig. 1, the recloser controls or a distribution automation controller can issue commands to the sectionalizers nearest the fault to open. When this process is complete, the controller commands the reclosers to close.

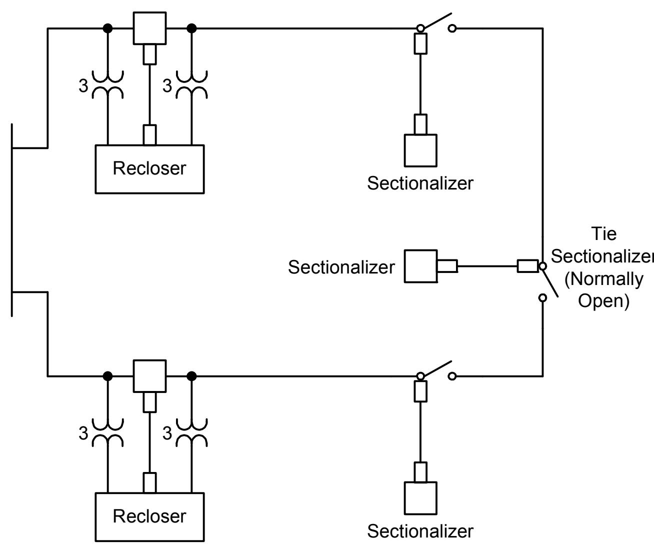

Fig. 1. Sectionalizer Scheme With Reclosers

Table I summarizes the key attributes required by traditional restoration applications.

TABLE I
TRADITIONAL RESTORATION ATTRIBUTES

Application	Speed	Traffic	Distance
Traditional restoration	Slow: seconds	Sparse: occasional commands	~10 miles

B. High-Speed Electrical Distribution Restoration

High-speed electrical distribution restoration demands operation in 50 milliseconds or less to quickly restore power to feeders supplying loads that are sensitive to power interruption. Some examples of these loads are manufacturing processes with batches of material that will harden or explode if power is lost during critical parts of the cycle or high-rise hotel and casino loads with significant revenue-per-minute losses while the power is off.

High-speed restoration schemes have the block diagram depicted in Fig. 2, but the communications links must transfer information in 50 milliseconds or less, rather than in seconds. The commands to operate the reclosers are small in size, and the frequency at which the command is issued is very low. The critical need for this channel is to maintain a very high availability. The communications channel must be available when the control is performed. In order to accomplish this, many protocols use a constant data stream, repeating the message in order to check the availability of the channel.

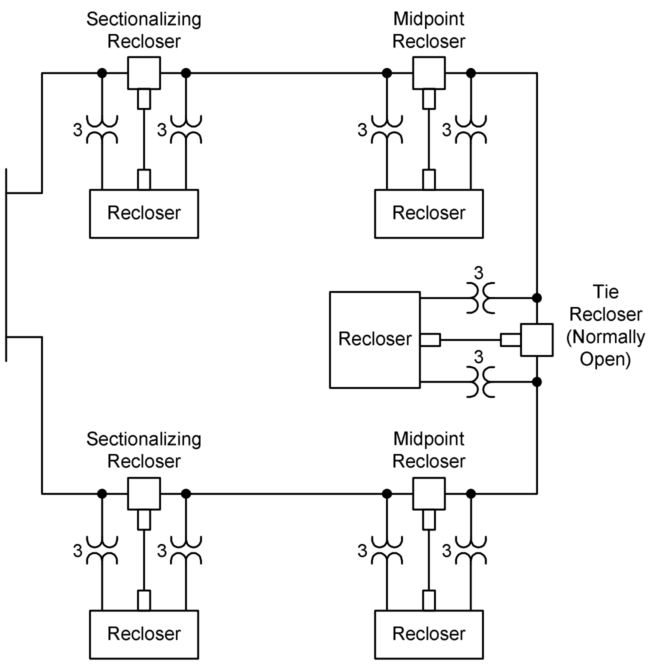

Fig. 2. Loop Scheme With High-Speed Recloser Controls

Table II summarizes the key attributes required by high-speed restoration applications.

TABLE II
HIGH-SPEED RESTORATION ATTRIBUTES

Application	Speed	Traffic	Distance
High-speed restoration	Fast: ~50 ms	Sparse: a few infrequent commands	~10 miles

C. Faulted Circuit Indication

FCIs (faulted circuit indicators) are typically overcurrent devices. They are mounted by spring clamps to overhead feeders at branches in the line and provide patrolling personnel with a visual indication of which branch sensed fault current. Additionally, fault counters and timed-reset fault indicators efficiently aid location of temporary flickering outages. Through wireless communication, FCI information is available to remote personnel or computer systems. Because an FCI is typically applied where there is no voltage transformer to provide power, its radio must be operated from batteries. The low-power battery source limits how frequently FCIs can communicate and mandates short communications links.

Table III summarizes the key attributes required by FCI applications.

TABLE III
FCI ATTRIBUTES

Application	Speed	Traffic	Distance
FCI	Slow: ~seconds	Sparse: small updates very infrequently	~2 miles

D. Supervisory Control and Data Acquisition

SCADA (supervisory control and data acquisition) communications links connect RTUs (remote terminal units) and control centers. An RTU may be a single device that includes a processing module and signal inputs and outputs connected to sensors and actuators, or the RTU functions can be distributed among multiple devices in a local network and then consolidated into a single SCADA link by a station processor or master controller. In modern SCADA systems, operational data are sent approximately every 1 to 5 seconds and include voltages, currents, and device states (Table IV). When digital inputs change state, report-by-exception messages are often used.

TABLE IV
SCADA ATTRIBUTES

Application	Speed	Traffic	Distance
Remote devices to substation	Slow: ~seconds	Steady operational data	Up to 10 miles
SCADA to control center	Slow: ~seconds	Steady operational data plus occasional large nonoperational file transfers	Wide variation

Wireless links are deployed for SCADA purposes between substation controllers and remote devices that are on connected feeders (e.g., recloser, capacitor bank, or voltage regulator controls). For links from substations to control centers, small systems sometimes use radio links. In larger systems, the SCADA links use a fiber-optic or wired WAN (wide-area network) backbone and the role of radio links is to provide a backhaul connection to the nearest WAN node for stations without a direct WAN connection.

E. Load Shedding

Load shedding is the act of tripping breakers or other switches to remove load from the power system. This can occur at a feeder level, dropping large amounts of load in response to loss of generation, or at an individual customer site for selected classes of loads, referred to as demand-side management. The role of the radio is to provide a means of shedding dispersed loads at recloser or sectionalizer points in order to minimize the affected customers in order to stabilize the power system.

Table V summarizes the key attributes required by load-shedding applications.

TABLE V
LOAD-SHEDDING ATTRIBUTES

Application	Speed	Traffic	Distance
Feeder-level load shedding	Slow: ~seconds	Occasional small messages	~2 miles
Demand-side load shedding	Slow: ~seconds	Occasional small messages	~2 miles

F. Teleprotection and Remedial Action Schemes

Teleprotection data links must provide sufficient time determinism so that protection engineers can depend on permissive, transfer trip, guard, or blocking messages to consistently be transferred in a known, stable period of time. Many applications demand end-to-end contact transfer times of under 1 electrical cycle (16.66 milliseconds in 60 Hz systems or 20 milliseconds in 50 Hz systems) or, for some applications, 2 cycles (see Table VI). IEC 61850-compliant systems require 4-millisecond transfer times between memory locations inside the end equipment to ultimately achieve these external end-to-end times [1].

TABLE VI
TELEPROTECTION ATTRIBUTES

Application	Speed	Traffic	Distance
Teleprotection	Fast: 4 to 40 ms	Smaller packets at time-deterministic rates	~20 miles

G. Voltage Control

Automatic voltage control schemes interact with voltage regulator controls and capacitor bank controls to maintain the system voltage within defined limits.

Table VII summarizes the key attributes required by voltage control applications.

TABLE VII
VOLTAGE CONTROL ATTRIBUTES

Application	Speed	Traffic	Distance
Voltage control	Seconds to minutes	Infrequent control commands or set points and ongoing voltage telemetry	~10 miles

H. Customer Meter Reading

AMR (automatic meter reading) systems collect data from customer meters at a relatively low data rate. AMI (automatic meter infrastructure) collects meter data and provides the communications mechanism for demand-side load shedding, as described in Section II, Subsection E.

Table VIII summarizes the key attributes required by AMR and AMI applications.

TABLE VIII
AMR AND AMI ATTRIBUTES

Application	Speed	Traffic	Distance
Meter reading	Minutes to hours	Small, infrequent messages from many devices	Varies

I. Technician and Engineering Access

For engineering and technician access, radio links generally transfer information from one device to another with no human included in the process. Technicians or engineers interact with devices to perform tasks that include retrieving reports for forensic analysis, changing settings, and loading new firmware.

1) Remote Personnel Access

Remote access allows a person to communicate with a device in the field from a central or office location. Often, this is achieved through the fiber-optic or wired backbone infrastructure to a site where a radio is installed to communicate the last hop to the end equipment. The interaction usually consists of short commands and responses and occasional file transfers of data or settings from the remote device or settings or firmware to the remote device.

Table IX summarizes the key attributes required for remote personnel access.

TABLE IX
REMOTE ACCESS ATTRIBUTES

Application	Speed	Traffic	Distance
Remote personnel access	Slow: ~seconds	Command interaction and occasional large file transfers	~10 miles

2) Local Personnel Access

Personnel access has been accomplished with local cables to handheld or laptop devices, but electric utility personnel elect to use wireless links instead of cables for the following variety of reasons:

- In a substation or plant, the area near panels and switchgear has a lot of human traffic, especially during commissioning or outages. By using a short-range temporary wireless link to a nearby desk or table, a person can interact with devices without being an impediment to foot traffic and without the tripping hazard of a cable.
- The technician or engineer can use temporary wireless links to interact with devices that are in unsafe or uncomfortable locations from a safer, more comfortable place.
- Radio frequency devices can be installed permanently on device ports to allow personnel to interact with the device when they are in the general vicinity using compatible handheld or laptop equipment. Examples include the following:
  - Securely interact with controllers, including recloser controls, capacitor bank controls, and voltage regulator controls, from the safety and comfort of the truck. This avoids opening the door of the control cabinet and allowing precipitation or contaminants to enter the cabinet and avoids diverting traffic and traversing hazardous areas.
  - Securely interact with substation automation controllers without entering the substation yard to retrieve data or perform other tasks. This allows

personnel who are not trained to safely enter substations to perform tasks without additional personnel or exposure to substation hazards, avoids snow removal to open substation gates, and reduces the likelihood of a physical security breach by tailgating or coercion.
- Securely interact with devices located in arc-flash hazard areas (or other hazardous areas) to avoid exposure to the hazard and prevent suiting up in personal protective equipment.

Table X summarizes the key attributes required for local personnel access.

TABLE X
LOCAL ACCESS ATTRIBUTES

Application	Speed	Traffic	Distance
Local personnel access	Slow: ~seconds	Command interaction and occasional large file transfers	5 to 300 feet

J. Hybrid Applications

When a single radio link serves multiple functions, the speed and bandwidth requirements for all functions should be aggregated to determine the radio link requirements. Further data stream analysis is required to determine if a class of messages needs to have a transmission priority greater than that of another class of messages. For example, if the same radio link is transferring nonoperational data, operational SCADA data, and high-speed control messages, either the bandwidth must be available and allocated so that all messages arrive in sufficient time regardless of other traffic or the transmission priorities must be assigned as follows:

1. High-speed control messages
2. Operational SCADA data
3. Nonoperational report and engineering access

III. WIRELESS TECHNOLOGIES

A relatively wide range of choices is available to users selecting a wireless technology for power delivery automation. These choices include using public or private networks, licensed or unlicensed bands, standards-based or proprietary systems, and packet-based or TDM (time-division multiplexing) access technologies. All of these choices provide benefits, and all have limitations. Making the right choice for a particular power delivery automation need is a matter of matching the capabilities of the technology to the requirements of the application. The following sections summarize some of the key attributes of various wireless technology choices.

A. Public Networks (Cellular)

Cellular phone networks are ubiquitous in urban, suburban, and many rural areas. They are designed to handle large volumes of voice and data traffic and have a steady evolution in capability that is likely to continue moving forward. The popularity and design of cellular services ensure, in most instances, that a user is in range of more than one cellular tower for any one system and that multiple cellular carriers serve an area. Being in range of multiple cellular towers provides a user with a certain level of redundancy, while the presence of multiple carriers gives the user an opportunity to find the price and capability to address specific needs.

So why use cellular? From a power delivery automation communications network deployment perspective, cellular systems offer the benefit of a built-in network infrastructure. The user only has to deploy relatively inexpensive end devices to create a functioning network. This benefit is offset to some extent because use of cellular networks incurs a monthly service fee that varies depending on usage. In the past, cellular plan rates have made these monthly service fees prohibitively expensive, but cellular operators are making an effort to attract more machine-to-machine customers, offering attractive service policies for customers based on aggregate monthly usage. Still, cellular network access can be expensive if the overall traffic levels are high and is best suited for applications where sparse communication is needed or where the steady-state operational data rate per device is relatively low.

Cellular networks also offer relatively robust network security, especially at the wireless interface level. There is also some level of physical security for the base stations themselves, which, in many cases, includes backup power to keep the network running in case of power failure. Localized power outages may have limited or no effect on a cellular network, given the redundancy of multiple base stations and local power backup. Cellular networks also support virtual private network services to insulate corporate data traffic from wider Internet traffic.

Cellular networks operate on a variety of bands, which include UHF bands (700, 800, and 900 MHz) with favorable radio propagation and structure penetration characteristics that can be especially advantageous in areas where the distance between the end-user site and the base station is long. Many rural and suburban networks operate in these lower frequency bands to allow longer distances between cellular sites (commensurate with the density of users in the area). In higher population density areas, it is often advantageous for cellular carriers to utilize higher frequency bands (1800, 1900, and 2100 to 2300 MHz) because it allows them to increase the density of base stations in an area without excessive cellular-to-cellular interference to provide network capacity that matches the needs of a larger number of customers. For the same reason, digital cellular technologies employ advanced power control algorithms to limit interference between users and base stations, which help maximize system performance.

There is an array of cellular access technologies available for machine-to-machine systems. These technologies are categorized by the industry as 2G, 2.5G, 3G, and 4G (for second generation, second generation data, third generation, and fourth generation wireless digital technology standards), with a variety of access technologies in each category. From a user perspective, the progression to newer generations of digital cellular technology is most evident in regard to the data rates possible, progressing from around 10 kbps in 2G devices to claims of up to 100 Mbps in 4G devices. These data rate claims are often made under conditions that do not pertain to the real world, and as such, real-world performance is typically a fraction of what can be achieved under test conditions.

For the user of a cellular network, it is important to understand what the end device is capable of, but it is equally important to understand the capabilities of the network to which it is connected. The 2.5G-capable digital networks (the base stations to which the cellular devices connect) are ubiquitous around the world, 3G-capable networks are widespread, and 4G networks are in the process of being built.

With the advent of 3G and 4G data rates, cellular carriers have to pay serious attention to their wire line and microwave backhaul capacity from base stations to the switching network so that aspect of the system does not become a bottleneck to system data capacity. The data rate actually available to any one user is a function of the entire network and loading from all sources. Heavy public use of cellular networks can result in a high level of data traffic, which may limit both network availability and data rates. On the other hand, cellular users do benefit from the fact that each base station is a separate entry point into a high-speed wired network and provides a network capacity multiplier that may not be available with a local private network.

The 2G cellular technologies encompass GSM (Global System for Mobile Communications), GPRS (General Packet Radio Service), and cdmaOne™ wireless technologies. This was the first generation of digital cellular devices introduced in the 1990s and is capable of providing data rates from 10 to 14 kbps. The 2.5G cellular technologies, including EDGE (Enhanced Data for GSM Evolution) and CDMA 1xRTT (Code Division Multiple Access Single-Carrier Radio Transmission Technology), were extensions of these initial digital systems capable of data rates between 150 and 384 kbps. Currently, available 2.5G devices are multimode and support the higher end of this range of data rates. The 3G cellular technologies include CDMA EV-DO (CDMA Evolution-Data Optimized) and W-CDMA (Wideband CDMA), which are both capable of between 1 and 3 Mbps data rates. The 4G technologies include HSPA (High Speed Packet Access), WiMAX (Worldwide Interoperability for Microwave Access), and LTE (Long Term Evolution), with throughput rates claimed to be from 5 to 100 Mbps. It is unlikely that a user in a real-world scenario will experience anything close to the upper end of this range unless the user is right next to a base station and the only person using the network at the time, but even so, 4G networks provide significant data throughput improvements over previous generations of devices.

Besides throughput, data networks for power delivery automation need to be concerned with latency and availability. Machine-to-machine latency in a cellular network is higher than many small private networks are capable of delivering. This is especially true if a call must be originated each time a device accesses the network. Even when this is not the case (as when using beaconing or control channels for intermittent data transmissions like SMS [short message service]), cellular network latency can be on the order of 200 milliseconds. This level of latency is not appropriate for teleprotection or high-speed restoration schemes but is acceptable for many other types of monitoring and control applications.

The availability of cellular networks is service dependent. The cellular networks do have quality of service and bandwidth usage controls. Usually, this service is not offered to the end user. This higher level of service normally comes as a premium on top of regular service. The regular cellular service provided can experience service degradation based upon the current usage of the cellular tower and the backhaul speed of the network. Any area supported by cellular systems that has a large congregation of people, like sporting events, can have drastic degradation of service.

B. Private Networks

Private networks for power delivery automation are entities unto themselves and only carry automation system data. They require the equivalent of both base station and end device infrastructure deployed by the user but can often be simpler and smaller than public cellular networks. A private company has the ability to design a network to meet its specific needs rather than using an established public network that may not be tuned to company requirements. Deployment of a private network has higher equipment and startup costs and requires expertise in the deployment of a radio system in order to ensure that the network is both robust and efficient. Private networks also have no monthly usage fees, making them suitable for both high and low traffic rate needs.

A private network may utilize a range of wireless technologies for different purposes. Likewise, multiple radio frequency bands are available for use, including unlicensed ISM (industrial, scientific, and medical) bands, as well as licensed bands. Private networks may be based on wireless telecom standards or on proprietary protocols developed by radio manufacturers to provide specific capabilities to users.

1) Standards-Based Networks

Standards-based radio networks include Wi-Fi® [2], ZigBee® (IEEE 802.15.4) [3], WiMAX [4], and Bluetooth® [5]. These systems generally allow interoperability between devices from different manufacturers. Each of these standards was devised to address a specific need. As long as network requirements fit the need for which these standards were developed, they provide a good solution. If requirements fall outside the scope for which these standard technologies were designed, they may not be as good a fit.

Wi-Fi provides a wireless packet access technology that can support a relatively large number of users over a relatively short range indoors. It utilizes a 5 to 16.67 MHz wide channel with a variety of modulation modes that provide scalable data rates advertised to be from 1 to 54 Mbps. Actual Wi-Fi data throughput is less than half of this because of channel contention from multiple devices and packet address and acknowledgment overhead. Wi-Fi operates in the 2.4 to 2.5 GHz radio band, and typical system link budgets limit the available range of Wi-Fi devices indoors to something on the order of hundreds of feet and outdoors to less than a mile. Because Wi-Fi employs scalable modulation modes, data rates can be traded off for link distance. Wi-Fi provides relatively robust security for data passed across the wireless link. In a Wi-Fi network, an access point provides the point of contact for the wireless network with the wired world; all devices in the network link to the wired world through the access point. Many manufacturers provide Wi-Fi-based systems with additional proprietary protocols to enable mesh networks for industrial and corporate use. Wi-Fi allows the transmission of an entire local-area network frame in one wireless transmission; data transmission latency depends on network loading, the amount of data being passed, and the modulation mode being employed and can vary widely from 5 to 50 milliseconds or more.

ZigBee provides a wireless packet access technology with a low data rate for short-range personal area networks. ZigBee devices can operate in the 863 to 870 MHz ISM band, the 902 to 928 MHz ISM band, or the 2.4 to 2.5 GHz ISM band. Effective network data rates are in the range of tens of kilobits per second. ZigBee was intended to provide low-power, simple, low-cost communication with a low data rate between a range of devices over short indoor or outdoor distances. ZigBee devices have a channel bandwidth of around 2.5 MHz and are usable over approximately the same range as Wi-Fi both indoors and outdoors. ZigBee also offers data encryption at the link level, similar to Wi-Fi. Because data rates are low latency for ZigBee, networks can be high when network loading is high or the amount of data being passed is large. ZigBee-compliant networks are best for short-range applications with low data rates where latency is not critical.

WiMAX is considered a 4G wireless technology and was originally developed as an alternative to 4G cellular technologies. As such, it has been deployed in both public and private networks. It provides a high data rate and uses a wide channel (20 to 40 MHz), very similar to LTE with many of the same attributes. The bandwidth of the WiMAX channel has limited deployment to frequency bands above 2.1 GHz, with 3.6 GHz being a specific band used for this technology. Propagation characteristics are not great at this frequency, so this technology is best used for point-to-point backhaul where high-gain antennas can be used to extend the range of the link.

Bluetooth is an alternative personal area networking standard that was intended for very short-range communications between devices, while providing high data rates (up to 2 Mbps). Bluetooth devices and networks were intended to be very low cost and an alternative to infrared communications devices. The typical range for a Bluetooth device is tens of feet, but there are higher-power devices that can have a range of up to 100 meters. Bluetooth devices also operate in the 2.4 to 2.5 GHz ISM band. For power system automation usage, Bluetooth devices are best suited for local personal access.

2) Proprietary Networks

Proprietary networks are systems using a custom protocol, hardware, or both to provide a network with some specific capability that may not be available from a standards-based device. There is a wide range of proprietary wireless technologies available. In general, these technologies are not interoperable (hence the name) with equipment from other manufacturers. The degree of proprietary network customization can vary, and many leverage or expand on the capabilities of a standard, such as Wi-Fi. A typical example is a long-range wireless bridge based on the Wi-Fi protocol. In other cases, the proprietary wireless network technology is more unique to address a specific need. Most microwave backhaul wireless systems are proprietary, as are TDM serial wireless systems. Link range, data rates, frequency bands, and latency are all areas where proprietary systems attempt to address user needs in a way not available from standards-based systems. The scope of proprietary systems can range from systems with very high link budgets and low data rates to microwave systems with very high data rates.

3) Licensed Networks

Systems that use licensed bands offer users the ability to have a slice of spectrum exclusively for their own use. This can be a big advantage in that the user does not have to worry about other users interfering with his or her communications network. Also, the transmit power levels permitted in licensed bands are generally higher than in the unlicensed bands, which helps with link budgets and propagation distance. The downside of licensed bands is that there are many users competing to acquire even small slices of spectrum and the costs associated with acquisition can be high or spectrum may simply not be available. In addition to the cost, the time to obtain license approval may introduce long calendar delays into a project.

4) Unlicensed Networks

Unlicensed bands for industrial use are available in Europe at 863 to 870 MHz and in North America at 902 to 928 MHz and 2.4 to 2.5 GHz; these are the ISM bands. Worldwide, the 2.4 to 2.5 GHz band is set aside for this same use. The benefit of using these bands is that the user does not need a license to use the band; the downside is that all usage is shared, and the user does not have exclusive rights to use the band. ISM bands are popular and tend to be heavily utilized. This does not preclude their use for power automation communications systems, but it does mean that interference and background noise need to be taken into account in any system deployment.

C. Access Technologies

There are two basic types of access technologies, TDM and packet. TDM systems have a deterministic, repetitive transmission protocol and specific capacity assigned to specific users, data, or channels. Their primary benefits are determinism in the bandwidth available to a channel and the latency of the transmission. TDM systems were the mainstay of wired telecoms for a long time and are still in use today. Their downside is that they are not very efficient users of spectrum when the data throughput needed by a specific user or channel is variable. Because each channel is assigned a fixed amount of the overall system capacity, the user must partition system resources based on peak channel throughput needs. If the channel does not require peak throughput all the time, then system capacity is wasted. In the context of wireless communication for power system automation, a serial link is an example of a TDM access technology. Generally, serial wireless links support one or a few serial data channels and have a defined maximum data rate for each channel. System capacity cannot be dynamically allocated to varying channel needs or shared between channels.

Ethernet is the epitome of packet access technologies. In a packet system, data are sent as a series of packets, multiple users have access to the same channel, and users have access to the entire channel for the period of their transmission. Packet data transmission is generally a more efficient use of a channel when variable rates of data transfer are needed and there are multiple users or devices accessing a shared channel. Wi-Fi and all of the other standards-based technologies previously described are packet access technologies. These technologies are popular specifically because they allow efficient use of a scarce resource (the wireless channel). The downside of packet-based systems is that they are not as deterministic as TDM systems and their latency can be higher and highly variable, which is the price paid for channel efficiency.

IV. Radio Technology Fitted for Application

The common radio application areas listed in Section III naturally fall into three classes of applications, matching different radio technologies, including the following:

- **Class 1**. High data reliability, variable latency (seconds to minutes), low bandwidth (hundreds of kilobits).
- **Class 2**. High data reliability, medium latency (hundreds of milliseconds to seconds), high bandwidth (2 to 20 MB).
- **Class 3**. High data availability, low latency (milliseconds), medium bandwidth (1 MB).

The three classes meet certain application requirements and present a natural dividing line in the radio technology that is available today.

The three classes of applications applied to the power delivery automation examples indicate which radio technologies best match those applications.

Table XI provides a list of the preferred radio class to use for each type of application. If a radio link must serve a mix of applications, then the speed, bandwidth, priority, and distance requirements for each application must be evaluated. The end user needs to make a decision as to which radio class best meets overall requirements.

Table XI
Power Delivery Automation Areas Defined With Radio Classes

Application	Speed	Traffic	Distance	Radio Class
Traditional restoration	Slow: seconds	Sparse: occasional commands	~10 miles	2
High-speed restoration	Fast: ~50 ms	Sparse: a few infrequent commands	~10 miles	3
FCI	Slow: ~seconds	Sparse: small updates very infrequently	~2 miles	1
Remote devices to substation	Slow: ~seconds	Steady operational data	Up to 10 miles	1
SCADA to control center	Slow: ~seconds	Steady operational data plus occasional large nonoperational file transfers	Wide variation	1
Feeder-level load shedding	Slow: ~seconds	Occasional small messages	~2 miles	2
Demand-side load shedding	Slow: ~seconds	Occasional small messages	~2 miles	2
Teleprotection	Fast: 4 to 40 ms	Smaller packets at time-deterministic rates	~20 miles	3
Voltage control	Seconds to minutes	Infrequent control commands or set points and ongoing voltage telemetry	~10 miles	2
Meter reading	Minutes to hours	Small, infrequent messages from many devices	Varies	1
Remote personnel access	Slow: ~seconds	Command interaction and occasional large file transfers	~10 miles	2
Local personnel access	Slow: ~seconds	Command interaction and occasional large file transfers	5 to 300 feet	2

A. Class 1 Radio

A Class 1 radio is defined as a radio that is designed to pass small amounts of data with a variable latency but with high data reliability. There are many wireless technologies well suited for this class of radios, which can be used on large wireless networks spanning a large network area. Class 1 radios are also used when connecting a few devices over a short distance.

The cellular infrastructure is a great choice for transporting these types of data with many benefits. The initial cost to the end user is much less than a private network. The monthly cost of sending data over cellular networks has dropped dramatically, and the availability of multiple cellular sites for one endpoint is very high. Newer endpoint hardware allows using one endpoint device on different cellular networks. This helps drive down the monthly service cost because the cellular network operators directly compete for business. The downside for this system is the reliability of the cellular company, their outage System Average Interruption Duration Index numbers, and the ability to get help when there are network issues.

The short-distance private network Class 1 radios use ZigBee and Bluetooth technology for distances up to 300 feet. Typically, Bluetooth is used as a cable replacement or serial-to-wireless replacement. ZigBee is used more as a private network, where manufacturers use the standard as a starting point and modify it to meet performance requirements.

For longer-distance Class 1 radio performance, the mesh radio networks provide low-cost connectivity and low-speed failover. Mesh networks have been designed to allow simple setup and automatic determination of the best path between points in the network. Another advantage of mesh radios is rapid deployment. The ZigBee standard, or a modified version of the ZigBee standard, is often used in these types of applications. Most mesh networks are proprietary and are not compatible with multiple manufacturers.

B. Class 2 Radio

Class 2 radios are becoming more popular for short- and medium-distance applications. The additional bandwidth of Class 2 radios allows customers to push more data over a wireless network. Wi-Fi is the protocol of choice for high-bandwidth links over short distances. Security, bandwidth, and networking capabilities have made Wi-Fi the wireless networking technology of choice for these applications.

Class 2 radio devices used for links of several miles or longer have been deployed in areas needing higher bandwidth for pictures or video feeds. These systems consist of a base station that services an area, similar to how a cellular network is designed. The most deployed standard-based technology in this class is WiMAX. WiMAX offers high throughput, relatively low latency per hop, and the ability to stream video and backhaul data over longer distances. The biggest problem with WiMAX is competition with LTE for market share among integrated circuit manufacturers. WiMAX was an early entrant in the 4G market, but most new network deployments are being made using LTE. Lower market share will eventually drive the cost of WiMAX up and push many of the chip manufacturers to stop investing development in this technology and possibly stop developing WiMAX chips at all.

A hybrid use of Class 2 radios for medium distances is a radio that uses multiple transceivers (in one device) operating at different frequencies to poll data at one frequency and backhaul the data at a higher frequency. Radios with dual transceivers typically use Wi-Fi at 2.4 GHz on a proprietary network for one of their links. This wireless interface is used to poll meters or other telemetry devices. The second transceiver is a Wi-Fi device operating at 5.8 GHz for the backhaul. The throughput can be substantial, but links are limited to half-mile to one-mile distances. The latency of these devices adds up quickly when a number of hops are involved to get the data to their destination.

C. Class 3 Radio

Class 3 radios are used when latency is of the highest importance. Achieving low latency requires specific topology and technology designs. The best performing radios in this class use a time-deterministic approach and point-to-point topology [6]. This allows the link to use high-gain directional antennas, allocated bandwidth, and directed traffic in lieu of the contention of multiple devices trying to send data at the same time.

Other approaches with point-to-multipoint or mesh topologies can meet the requirements of this class of devices but require careful system design. In a point-to-multipoint or mesh design network, bandwidth is divided across all units in the network. Network channel 1 Mbps capacity can easily be reduced to tens of kilobits per device when a network includes a dozen devices all needing to talk with one another. The per-device bandwidth is lower than that given by simply dividing the network bandwidth by the number of devices because contention between all of the radios competing to talk reduces the efficiency of channel usage. To make these systems work properly, they should be split up into smaller networks of around 15 devices. The smaller networks perform better and minimize the number of hops needed, which directly affects latency and throughput.

Class 3 radios come in licensed and unlicensed versions, and the choice between the two comes down to what the customer is comfortable using, the cost, and the network location. The licensed radios have a fee, but in more urban areas, it is becoming very difficult to obtain rights to licensed spectrum. Unlicensed radios on the market in this category are typically 900 MHz or 2.4 GHz. The propagation characteristics are better for 900 MHz, allowing longer link distance, while the 2.4 GHz allows more bandwidth. Worldwide, 2.4 GHz is accepted in most countries with power restrictions. Unlicensed 900 MHz radios are only allowed in North America and parts of South America.

V. Failover and Redundancy

These three radio classes may require a failover or redundancy method to increase the reliability of the network. Radios may have a failover mechanism designed to find either the best alternative path, a specific backup path, or a redundant radio to prevent single points of failure. There are three types of failover used for power delivery automation applications, including the following:

- Low-speed failover = metering and SCADA.
- High-speed failover = restoration and control.
- No failover = backup is provided by other means.

A. Low-Speed Failover

Low-speed failover is found in Class 1 radios. These networks are designed either as a point-to-multipoint network with repeater capability or a mesh topology consisting of hundreds, or even thousands, of devices. The need in this application is to have automatic failover for any single failed unit. Mesh networks are designed to find alternate paths, and all nodes have the capability of healing. This healing capability is very attractive for Class 1 radio applications. The biggest setback for this technology is that it can take from seconds to minutes to heal. The healing time is determined by the size of the network. Point-to-multipoint networks with repeater capability do not have the complete healing capabilities of a mesh network, but they can have failover capabilities for the access point and repeater. Because the failover mechanism is defined, failover times in point-to-multipoint systems are typically much faster.

B. High-Speed Failover

High-speed failover can be a requirement for Class 3 radios. The failover times required for this device class are less than 1 second. In order to achieve these faster failover times, more overhead is required to ensure that every device on the system is accounted for and check that each device is communicating. There are some mesh radios that come close to these times, but they are heavily dependent on the number of devices in the network. More hops and devices on a mesh network increase the failover times. A better system, consisting of point-to-multipoint networks with repeaters, can provide faster failover times because these networks are set up with directed traffic from the start. If the device cannot communicate to the network, it will immediately fail over to a preset radio. This point-to-multipoint failover mechanism is always faster than a mesh. The mesh must rediscover and heal as more nodes are added, so it will take longer to complete the failover process.

The other factor to consider with failover is bandwidth. Depending on which device fails and how the failover mechanism is set up, the failover unit may not be able to handle the increased number of units and may prevent the system from operating in a timely manner.

The fastest failover network is the point-to-point network. In this topology, each end has a secondary radio waiting in a hot standby mode. If either end of the link fails, the standby radio automatically takes over. The failover times in this scenario are hundreds of milliseconds or less.

C. No Failover

High-speed protection schemes may choose to have no radio failover for communications. This is typically due to the communications channel used to assist in speeding up protection. The backup mechanism is built into the protective relay to operate without the communications channel with a slight delay in operation speed. Having no radio failover is common in Class 3 radios. No failover helps to simplify the network and reduce the cost of redundant radios. In these applications, there is always a wired or timed backup operation already in place. The end user is using radios in this application either for faster operation times or as the backup to an existing wired or fiber-optic system.

VI. Conclusion

A wide selection of radios is available to meet power delivery automation needs. When determining the right radio for an application, there will always be tradeoffs involving bandwidth, latency, distance, and cost. This paper categorizes the requirements of power delivery automation applications and defines radio classes that address the different performance requirements of these applications. The discussion of the capabilities and limitations of each class of radio helps clarify the differences between the classes and provides insight into which radio technologies are available and usable for each class. Table XI shows the applications that are used with radios today, and the radio classification provides guidelines for choosing the best class of radio for the application.

VII. References

[1] E. O. Schweitzer, III, D. Finney, and M. V. Mynam, “Applying Radio Communication in Distribution Generation Teleprotection Schemes,” proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[2] IEEE 802.11-2007, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[3] IEEE 802.15.4-2011, IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), 2011.

[4] IEEE 802.16-2009, IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, 2009.

[5] IEEE 802.15.1-2005, IEEE Standard for Information Technology – Local and Metropolitan Area Networks – Specific Requirements – Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2005.

[6] S. V. Achanta, B. MacLeod, E. Sagen, and H. Loehner, “Apply Radios to Improve the Operation of Electrical Protection,” proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

VIII. Biographies

Eric Sagen received his BS in electrical engineering from Washington State University in 1997. He joined General Electric in Pennsylvania as a product engineer. In 1999, Eric was employed by Schweitzer Engineering Laboratories, Inc. as a distribution product engineer. Shortly after, he was promoted to lead distribution product engineer. Eric transferred to the time and communications group in 2006 and is currently a lead product engineer. He is certified in Washington as an Engineer in Training (EIT).

Henry Loehner received his BS 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.

20120221 • TP6536-01