![Cambium Networks logo]

BENEFITS OF WIRELESS COMMUNICATIONS NETWORKS IN
Electric Utility Automation and Security

THE ELECTRIC UTILITY INDUSTRY IS UNDERGOING SIGNIFICANT CHANGE as focus increases on more flexible distribution substation topologies and the integration of renewable energy sources. Concerns over outage costs, distribution and transmission loss, and cybersecurity threats are leading to a much deeper and wider penetration of intelligent sensors and controllers in the grid. Renewable energy and distributed energy resources are increasing the size and complexity of the distribution network as new substations come on board and microgrids become more prevalent. The availability of sensors and re-closers with built-in communications enable faster fault location isolation and service restoration (FLISR), minimizing outage costs. And of course smart meters and AMI drive better analytics on managing demand variation. We also see the growing need for data capacity at the substation and field network level as field engineers need access to back-office resources and increased security requirements demand video surveillance for employee and asset security. And while the focus on this mission-critical infrastructure in most of the world is to increase efficiency and availability, it is also important to note that more than 1.3 billion people in the world still lack reliable access to electric energy and extending the grid into these areas will require low-cost efficient solutions.

This whitepaper outlines the applications for wireless connectivity in electric utility automation and then considers the benefits of a private wireless network compared to alternatives such as wireline networks for the utilization of the public 3G/4G network. It also covers the important aspects in selecting a wireless network technology.

Fixed Wireless Broadband Use Cases in Utility Infrastructure

SCADA Networks - The traditional use case considered for utility infrastructure is sensor data collection via SCADA solutions. SCADA solutions are characterized by relatively low data rates with sensors and data sources spread widely over a geographic area. As network devices become more intelligent, SCADA systems are becoming more important, not only for control and monitoring, but for end-to-end analytics applications. Security is becoming more critical and the protocols to carry SCADA traffic are increasing in the size of packets needed to carry this traffic. For example, a simple poll request consisting of an 8 byte command can expand to 70-80 bytes when sent over Ethernet using a secure DNP3 protocol. Wireless broadband solutions can handle this increased load, aggregate this SCADA data, and pass it over long distances with low latency back to centralized SCADA masters and network operations centers. System availability and security are table stakes for these applications.
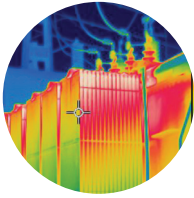
Disaster Recovery / Network Resiliency

Many electric utilities are deploying communications using wireline technologies such as fiber or copper. As these communications become more mission critical, availability becomes more visible and system outages more costly. The ability to continue operating or to restore communications after a natural disaster or man-made attack can differentiate utility companies and ensure that the public is protected. Wireless broadband is a natural fit for disaster recovery applications. Whether deployed as an always-on, real-time backup solution or kitted as a rapidly deployable tactical response system, wireless communications can be counted on for the fastest way to restore communications.

Remote Connectivity to the Home Office

As these systems become more complex and the availability of information for troubleshooting, planning, and installation increases, field engineers are in need of connectivity back to the home office as well as to the Internet. Wireless broadband can deliver Internet and Intranet access over long distances and rugged terrain to areas not covered by the public 3G/4G network or reachable by fiber. Combined with secure industrial-grade WiFi hotspots, field engineers can access the corporate

infrastructure and all the resources they would have access to while on the corporate LAN regardless of where they are in the field. All while using the tools they are already have, such as laptops and smart phones, and reducing the cost and dependency on the spotty coverage and availability of the public 3G/4G network in these remote locations.

Video Surveillance and Security at the Substation

When the substation has a broadband data connection, new personnel safety and asset security capabilities can be brought on board including perimeter security with video cameras. Whether the requirements call for local storage and on-demand access or constant streaming, wireless backhaul can deliver the bandwidth required. Additional capabilities, such as license plate readers and facial recognition for site access can provide positive confirmation of who is on site. And with thermal imaging cameras, outage and overload conditions can be monitored even with periodic snapshots of the substation equipment. Private wireless broadband solutions are especially well suited to video surveillance because cameras can be located where they are needed rather than where it is convenient to reach the wireline network, and there is no recurring expense of the bandwidth consumed.

Leased-Line Replacement

Many electric utilities are using wireline networks purchased from the local telecommunications operator. These leased-lines have recurring monthly operating costs and typically have limited capacity. Changes to increase capacity can take a long time to activate. Many of the low-capacity analog leased-lines are also being phased out by the telephone service providers in favor of more expensive digital circuits that aren't suitable for utility operations.

Why Private Wireless Networks Are Best Suited for Electric Utility Automation

Electric utility operators have three high-level options when selecting a communications infrastructure: private or leased wireline networks, public wireless networks, such as the 3G/4G mobile infrastructure, or private wireless networks. In most cases, the best answer is a combination of these, but here are some important areas to consider why a private wireless network delivers the best overall total cost of ownership.

Private wireless networks can be deployed quickly and placed exactly where the data is needed. There are no trenches to dig or cables to run, which can mean months between the time the need is identified and the network is operational. Especially important in electric utility substations is the safety concern and extra care required to trench additional cables. Wireless sectors can be installed covering broad areas over long distances, providing flexibility in remote node placement and re-use of the infrastructure. Maintenance costs and on-going OPEX are lower as there are no wires to break or be cut. With a wireless infrastructure in place, the capacity can be leveraged for many different applications, and using quality of service, the most important data can be prioritized. Private wireless broadband networks have low recurring costs especially when compared to accessing the 3G/4G mobile network or leasing lines from carriers. The 3G/4G mobile network has the benefit of existing coverage in some areas, but it is important to note that there is no provision for prioritization of mission critical traffic or even ensuring that capacity is available. Providing field engineers with 3G/4G data access is a large recurring expenditure that could be avoided.

Private wireless network operators have control over access and how the traffic gets prioritized. Combining rapid deployment, low initial cost, and virtually no recurring costs, private wireless broadband networks are clearly the total cost of ownership leader providing a rapid return on investment.

Key Considerations in Choosing a Technology for Private Wireless Networks

There are many networking technologies being deployed by electric utilities today, each with different capabilities. Here are some key considerations when discussing these different techniques.

Capacity vs. Range: Several factors impact the amount of data capacity that can be delivered at a particular distance. Those factors include spectrum, channel bandwidth, transmitter power, terrain, noise immunity and antenna size. In general, capacity comes down the longer the distance to be covered. The longest propagation would be in a low frequency narrow band channel with a high-gain antenna, while higher capacities could be had by selecting wider channels. Cambium Networks has a software tool called LINKPlanner that makes it easy to do "what-if" scenarios to select the best combination of channel size, antenna, and radio to achieve the desired capacity with the necessary availability. Cambium Networks offers capacities of more than a Gbps, and link distances from a few hundreds of meters up to 245 km.

Topologies (PTP, PMP, Rings, Mesh): Point-to-Point (PTP) topologies are best suited for delivering lots of capacity over long distances. PTP links are also great for short-range spurs connecting a single location to the wireline backbone. PTP connections cover longer distances that are less susceptible to interference as the antenna patterns are narrower so the energy can be focused in the direction of the transmission. Resiliency in a PTP link can be provided by deploying in 1+1 or 2+0 configurations with parallel sets of radios. Ring topologies are excellent for resilient operations of high-capacity links covering a large area. Mesh networks can be built using multiple PTP links or with specialized meshing protocols to enable multiple paths from point A to point B. Mesh networks have the down side of each packet traversing multiple hops so can lead to lower capacity given the infrastructure investment. Point-to-Multipoint (PMP) networks provide scale and capacity over a geographic area. PMP networks are typically deployed to cover sectors or cells. The key capability to look for in PMP networks is their ability to scale both in the number of nodes per cell but also the ability to place cells next to each other without interfering. Cambium Networks radios use synchronization techniques to ensure that adjacent PMP radios do not interfere with each other.

Licensed vs. Unlicensed

Wireless spectrum can be characterized as either licensed or unlicensed. Access to licensed spectrum is typically purchased to provide an organization exclusive access to a particular channel in a particular location. Operation in that channel should be largely free of interference from competing radios. The downside is the spectrum may be extremely scarce or expensive to access. Even when more easily accessible, it can take weeks to gain the approval to operate so licensed bands are not well suited to rapid deployments. Unlicensed spectrum is generally open and available to anybody to use with no exclusive rights granted to any particular organization or individual. The tradeoff is that competing systems may occupy the same channel at different power levels leading to interference. Unlicensed radio manufacturers include capabilities in these radios to cope with this potential interference. Cambium Networks uses features such as Dynamic Spectrum Optimization (DSO), adaptive modulation, automatic transmit power control, and out of band filtering to minimize the impact of this interference.

Line of Sight vs. Non-Line of Sight

A radio link can described as being line of sight when there is an optical path between the two radios making up the link or non-line of sight (NLoS) when there is some obstruction between the two radios. Near line of sight is simply a partial obstruction rather than a complete obstruction. In general, lower frequency solutions have better propagation than higher frequencies. In fact, above 6 GHz wireless solutions must operate in line of sight. From 1 GHz to 6 GHz, the capabilities will vary, and below 1 GHz the propagation becomes much better. Cambium Networks has many techniques in 5 GHz radios to maximum the propagation of these signals including OFDM, multipath, ARQ and radios designed to work at very low receive sensitivities.

Security

With ongoing cybersecurity threats, the security of wireless communications is growing in importance. Techniques to look for here include the ability to encrypt the over-the-air link, secure management interfaces with HTTPS and SNMPv3, and create multiple user accounts with password complexity rules. Cambium Networks radios are deployed in mission-critical infrastructure solutions around the world, including military deployments and public safety missions, so security is built in our products from start to finish. Selecting a solution with strong security features makes it easier to comply with NERC-CIP audits. For the most security, Cambium Networks also offers solutions validated to FIPS 140-2 which is a US Federal government standard for security.

Quality of Service

Operators need to make the most efficient use of available spectrum by deploying multiple services on the same channels and also making sure the most important information is transmitted with highest priority. Solutions should have multiple Quality of Service (QoS) levels and the ability to sort traffic based on both layer 2 and layer 3 standard traffic classifiers. In this way, the source of the data can mark the class of service or priority, and the end-to-end network will ensure that the traffic is delivered with the desired level of urgency and criticality.

Network Management

The ability to manage a network is a direct impact on the total cost of ownership. Systems that allow centralized management of configuration, fault detection, performance/trend monitoring, and security validation minimize the effort and also reduce the opportunities for unplanned outages. Cambium Networks radios support both local web-based interfaces as well as a centralized management system called *cn*Maestro™.

Cambium Networks has deployed more than five million wireless broadband nodes around the world. We are experienced in mission-critical communications in areas such as electric utility infrastructure, federal military deployments, digital oilfields, and public safety operations. Cambium offers the industry's most complete end-to-end set of solutions including transport, backhaul, distribution, and WiFi access, all managed from a common set of tools.